

La firma digitale: implicazioni e novità del nuovo strumento

di Maurizio Sala - avvocato in Milano

e-mail maurizio@sala.it

La diffusione e l'utilizzo degli strumenti informatici e lo sviluppo dei sistemi di comunicazione tra computers hanno imposto di trovare soluzione ai problemi connessi al passaggio dal sistema tradizionale, basato sulla documentazione cartacea, a quello nuovo "elettronico".

Il legislatore ha inserito nell'ordinamento italiano la disciplina del documento informatico in tre fasi successive:

- dapprima con l'art. 15 comma 2 della legge 15 marzo 1997 n. 59 che ha introdotto il principio secondo il quale: « *Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. ...* », demandando ad un successivo specifico regolamento « *i criteri e le modalità di applicazione del presente comma* »;
- quindi con il D.P.R. 10 novembre 1997 n. 513 contenente il « *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, comma 2, della L. 15 marzo 1997, n. 59* » che ha rinviato ad un successivo « *decreto del Presidente del Consiglio dei Ministri, da emanare entro centottanta giorni dalla data di entrata in vigore del (predetto) regolamento, sentita l'Autorità per l'informatica nella pubblica amministrazione (il compito) di fissa(re) le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione,*

- anche temporale, dei documenti informatici.»* (art. 3 comma 1 D.P.R. 513/97);
- infine con il Decreto del Presidente del Consiglio dei Ministri - approvato il giorno 11 febbraio 1999, trasmesso lo stesso giorno alla Corte dei Conti per la registrazione - di attuazione del D.P.R. 10.11.1997 n.513 contenente le *«Regole tecniche per la formazione, la trasmissione, la conservazione la duplicazione, la riproduzione, la validazione, anche temporale, dei documenti informatici ai sensi dell' art. 3 comma 1»* del citato D.P.R..

Concluso il processo di formazione della disciplina giuridica del documento elettronico, l'Italia é uno dei pochi paesi al mondo ad avere recepito nel proprio ordinamento una così importante innovazione tecnologica, introducendo il concetto e le specifiche della firma digitale, tramite la quale viene conferita validità giuridica del documento elettronico.

La firma digitale non é qualcosa di riconducibile ad un elemento materiale immediatamente percepibile - così come la firma tradizionale - essendo invece un sistema di cifratura e decifratura a chiavi asimmetriche (detto anche a chiave pubblica) per garantire la sicurezza della genuinità e della provenienza dei documenti informatici.

Il D.P.R. 513 10 novembre 1997 n. 513 ha equiparato la firma digitale a quella tradizionale disponendo che:

- *« Il documento informatico sottoscritto con firma digitale ai sensi dell'art. 10, ha efficacia di scrittura privata ai sensi dell' art. 2702 del codice civile »* (art. 5 comma 1);
- *« l'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo »* (art. 10 comma 2).

Inoltre:

- *«I contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente regolamento sono validi e rilevanti a tutti gli effetti di legge.» (art. 11)*

Stante l'equivalenza, sul piano giuridico, della firma digitale a quella tradizionale e dei particolari effetti che ciò comporta é logico domandarsi come la prima possa assolvere alle funzioni attribuite dalla dottrina alla seconda e precisamente:

- funzione indicativa dell' autore del documento, consistente nella possibilità di risalire con certezza all'identità del sottoscrittore;
- funzione dichiarativa di approvazione del contenuto del documento da parte del sottoscrittore e di assunzione della paternità delle dichiarazioni in esso rese (il documento potrebbe, infatti, essere stato redatto da altri ma é solo colui che lo sottoscrive che si assume la responsabilità delle dichiarazioni in esso contenute come manifestazione della propria volontà);
- funzione probatoria che é il risultato dell'insieme delle due funzioni precedenti e cioè di mezzo di prova della provenienza delle dichiarazioni contenute nel documento da chi l'ha sottoscritto.

Per rispondere al quesito é necessario, a questo punto, spiegare, nel modo più semplice e meno tecnico possibile, il sistema crittografico alla base la firma digitale.

Facciamo un esempio.

Supponiamo che A debba trasmettere a B un documento che non vuole che altri possano leggere.

La strada da seguire é quella della crittografia, vale a dire di quella tecnica che

applicando un algoritmo matematico ad una serie di caratteri alfanumerici intellegibili a chiunque, li rende incomprensibili.

Naturalmente il processo di crittografia deve essere reversibile e consentire, quindi, di rendere intellegibile un documento precedentemente criptato.

L'elemento che consente di criptare e decriptare un documento é chiamato "chiave".

I sistemi di crittografia sono di due tipi: quello *simmetrico*, detto anche a *chiavesegreta* e quello *asimmetrico*, chiamato anche a *chiave pubblica* .

Nel sistema simmetrico si usa la medesima chiave sia per criptare che per decriptare; ecco la ragione per la quale la chiave deve essere segreta.

L'uso di questo sistema importa alcune controindicazioni e problemi quali:

- la necessità di trasmettere al destinatario la chiave segreta necessaria per decriptare il documento e, conseguentemente, della sicurezza della trasmissione di tale chiave, che se entrasse in possesso di terzi annullerebbe gli effetti della crittografia e non consentirebbe di considerare segreto il documento cifrato;
- l'impossibilità di assicurare, nei rapporti tra mittente e destinatario, la genuinità del documento che potrebbe subire alterazioni, ad esempio, da parte del destinatario che, disponendo della chiave segreta, sarebbe in condizioni di manomettere il documento originario per poi ricifrarlo ed utilizzarlo come se fosse autentico;
- l'oggettiva difficoltà di possedere, gestire e trasmettere una pluralità di chiavi segrete nell'ipotesi di comunicazioni riservate con più destinatari.

Tali problemi non si pongono nel sistema asimmetrico o a chiave pubblica .

In tale sistema, infatti, per la cifratura e la decifratura dei documenti sono necessarie due chiavi, diverse tra loro, delle quali una rimane segreta ed é conosciuta solo dal suo titolare mentre la seconda é, per l' appunto, pubblica e, quindi, conosciuta ovvero

conoscibile da chiunque perché annotata in appositi registri tenuti da uno specifico ente certificatore che garantisce l'identità del soggetto titolare di tale chiave.

Per cui, nell' esempio proposto di invio di un documento da A a B, il mittente A cifrerà il documento con la propria chiave privata (segreta) e lo trasmetterà al destinatario B che utilizzerà la chiave pubblica di A per decifrarlo.

Così operando A non dovrà mai trasmettere la propria chiave privata che, quindi, rimarrà segreta.

B, a sua volta, dopo aver decifrato il documento ricevuto utilizzando la chiave pubblica di A, avrà la certezza che il documento è genuino e che proviene da A.

In altre parole: un documento cifrato con una determinata chiave privata potrà essere decifrato solo con la corrispondente chiave pubblica.

Vale, evidentemente, anche la regola inversa per cui un documento decifrato con una determinata chiave pubblica non potrà essere stato generato che dal titolare della corrispondente chiave privata.

Il sistema delle chiavi asimmetriche assicura - quindi - la paternità del documento, vale a dire l' identità del mittente, e l' integrità del documento, vale a dire la non ripudiabilità dello stesso.

Rimane - però - il problema della segretezza.

Infatti, se per la decifratura di un messaggio crittografato con una chiave privata è necessaria e sufficiente la chiave pubblica accessibile a chiunque, il documento cifrato è, per definizione, esso stesso pubblico o, quantomeno, può essere reso intelleggibile da tutti.

Il sistema a chiavi asimmetriche offre la soluzione al problema essendo sufficiente invertire l'uso delle chiavi sopra indicato, di modo che il mittente A cifrerà il messaggio

utilizzando la chiave pubblica del destinatario B che sarà l'unico in grado di leggerlo perché titolare della corrispondente chiave privata.

Riassumendo: per assicurare l'identità del mittente e la genuinità del documento il mittente cifrerà con la propria chiave privata mentre il destinatario decifrerà con la corrispondente chiave pubblica, per assicurare la segretezza del documento il mittente cifrerà con la chiave pubblica del destinatario che decifrerà con la propria chiave privata.

Le due funzioni possono - poi - essere combinate per assicurare tanto la paternità e genuinità del documento quanto la sua riservatezza.

Per ottenere tale risultato sarà necessaria una doppia crittazione per cui il mittente A cifrerà il documento utilizzando la propria chiave privata e - poi - lo cifrerà una seconda volta impiegando la chiave pubblica di B.

B, da parte sua, decifrerà il messaggio dapprima con la propria chiave privata e, subito dopo, con la chiave pubblica di A.

Sin qui abbiamo illustrato il sistema di criptografia dell'intero messaggio utilizzato per la trasmissione riservata di un documento.

La firma digitale, pur basandosi sullo stesso principio, è qualcosa di diverso.

La cifratura di un intero documento richiede però molto tempo e potrebbe non interessarci, magari perché non abbiamo bisogno di trasmettere un messaggio riservato ma solo di garantire al destinatario B la genuinità e la paternità del nostro documento.

In tale condizione soccorre la firma digitale, che funziona nel seguente modo:

- a. dopo avere redatto (rectius digitato) un testo, gli si applica una particolare funzione, detta di hash, che ha, quale unico scopo, di ridurre l'intero documento ad una specie di riassunto estremamente sintetico (tecnicamente: una stringa binaria di lunghezza

costante di 160 bit corrispondente a 20 byte, vale a dire 20 caratteri alfanumerici corrispondenti a mezza riga di foglio uso bollo) che rappresenta l'«impronta» del documento.

L'importanza della funzione di hash é data dal fatto che la sua applicazione assicura l'unicità dell'«impronta» generata, nel senso che se al testo originario modificassimo anche un solo carattere il risultato della funzione di hash sarebbe un'impronta diversa.

b. Applichiamo all'impronta la nostra chiave privata ed otterremo la firma digitale del documento.

L'utilità dell'uso dell'impronta é di tutta evidenza: ci consente di generare la firma digitale senza necessità di criptare l'intero documento.

L'impronta rappresenta - poi - il mezzo per ottenerne l'autenticazione da parte di un terzo mantenendo riservato il contenuto del documento che l'ha generata, ma di ciò ci occuperemo più avanti quando parleremo della validazione ovvero marcatura temporanea.

La firma digitale, per come abbiamo illustrato, non cripta il documento - che, quindi, rimarrà intellegibile a tutti, vale a dire "in chiaro" - ma ne assicurerà esclusivamente la non alterazione del testo e la provenienza da un soggetto determinato.

La criptazione del testo potrà - invece - essere effettuata a meri fini di segretezza utilizzando la chiave pubblica del destinatario B, come spiegato nell'esempio fatto sopra.

Nel sistema a chiavi asimmetriche sin qui illustrato le coppie di chiavi (privata e pubblica) sono - quindi - due: una prima coppia, detta di firma, destinata alla criptazione/decriptazione dell'impronta del documento al fine di generare la firma

digitale ed una seconda coppia, detta di trasmissione, utilizzata per la criptazione/decriptazione del testo di un documento per la successiva trasmissione riservata.

Arrivati a questo punto apparirà - ci auguriamo - più comprensibile la definizione di firma digitale data dal D.P.R. 513/97 secondo il quale essa é « *il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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* » (art. 1 lett. b).

L'impiego del sistema a chiavi asimmetriche sin qui esposto lascia tuttavia irrisolto il problema di come sia possibile assicurare al destinatario di un messaggio con firma digitale che una chiave pubblica appartenga ad un determinato soggetto.

Senza dilungarci più di tanto in spiegazioni tecniche che appesantirebbero il discorso, basti sapere che la soluzione al problema risiede nella certificazione, che consiste in un documento elettronico rilasciato da una Autorità di Certificazione che attribuisce alle chiavi pubblica l'identità, precedentemente accertata, del soggetto titolare delle corrispondenti chiavi private.

Dal punto di vista pratico la cosa funziona così: chi desiderasse utilizzare il sistema di crittografia asimmetrico sin qui descritto dovrà farsi, preventivamente identificare da un apposito ente denominato Autorità di Registrazione (le cui funzioni potrebbero essere svolte, ad esempio, tramite gli addetti agli sportelli bancari piuttosto che agli uffici postali) che trasmetterà, per via elettronica, i dati acquisiti all' Autorità di Certificazione

consegnando, nel contempo, al richiedente una smart card (una specie di carta bancomat dotata di microchip) ed un software che, insieme, consentiranno di generare, con l'aiuto di un personal computer, le chiavi pubbliche (di firma e di trasmissione), rimanendo quelle private (segrete) nella smart card.

A questo punto il richiedente invierà le chiavi pubbliche appena generate all'Autorità di Certificazione che, ricevuti i dati identificativi del titolare e verificata la loro coincidenza con i dati pervenuti dall'Autorità di Registrazione, inserirà le chiavi pubbliche nel directorio (il registro delle chiavi pubbliche) «marcandole», vale a dire applicando alle stesse la data e l'ora di registrazione, ed emetterà il certificato elettronico di - diciamo così - attribuzione di paternità della coppia di chiavi pubbliche che, quindi, trasmetterà al richiedente che, da quel momento sarà abilitato all'utilizzo delle chiavi elettroniche.

Qui giunti si impone una breve enunciazione di tre concetti fondamentali:

- firma (digitale) o, meglio, firmare significa sottoscrivere con un procedimento elettronico di crittografia un documento;
- criptografia è il processo mediante il quale un testo viene secretato o, se preferite, reso riservato;
- integrità dei dati vuol dire che nessuno può modificare il documento.

Dalle definizioni sopra enunciate e dalla comprensione del sistema crittografico a chiavi asimmetriche possiamo desumere le sostanziali differenze tra la firma digitale e la firma tradizionale.

Secondo la concezione tradizionale l'integrità di un documento è inscindibilmente connessa a quella del supporto sul quale è stata fissata, ad esempio, una manifestazione di pensiero, di modo che l'alterazione di esso sia riconducibile alla riconoscibilità di

cancellature o altre modifiche.

L'imputazione del contenuto del documento ad un determinato soggetto é assicurata - quindi - dalla firma di colui che se ne vuole assumere la paternità e che appone il suo segno grafico in calce al supporto (normalmente cartaceo) sul quale é stato realizzato il documento.

La firma digitale - secondo la definizione offerta all' art. 1 lett. b del D.P.R. 513/97 - realizza da sola il risultato dell' integrità del documento e dell'imputazione dello stesso.

Essendo la firma digitale il risultato di una procedura crittografica a duplice chiave, una delle quali privata, essa é intrinsecamente e inscindibilmente collegata al contenuto del documento di modo che se venisse cambiato anche un solo carattere del documento originario il risultato dell'applicazione (a tale documento modificato) della firma digitale darebbe un risultato diverso da quello ottenuto dal documento genuino.

La conseguenza di ciò é che a testi differenti corrispondono firme (digitali) diverse (non dimentichiamoci mai che la firma digitale non é un segno grafico praticato con strumenti elettronici ma, giova ripeterlo, il risultato di una cifratura).

La firma digitale é - quindi - unica e non può essere trasferita da un testo ad un altro come, invece, potrebbe avvenire con la firma tradizionale, ad esempio nel caso di falsificazione.

Arrivati a questo punto possiamo dare risposta alla domanda che ci eravamo posti all'inizio circa l'assolvimento da parte della firma digitale alle tre funzioni tipiche della sottoscrizione: indicativa, dichiarativa e probatoria.

Quanto alla prima soccorre l'art.10 comma 7 del D.P.R. 513/97 secondo il quale:
« *Attraverso la firma digitale devono potersi rilevare, nei modi e con le tecniche definiti*

maurizio sala

**La firma digitale: implicazioni e novità del nuovo strumento
pubblicato in *Archivio Civile*, 1999, p. 681 ss.**

con il decreto di cui all'articolo 3, gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione. ». A voler essere precisi va osservato che per "titolarità della firma" si deve intendere quella della coppia di chiavi, privata e pubblica, che, insieme, consentono di attivare il processo di cifratura e decifratura di un documento.

Quindi una volta che - secondo quanto previsto dai regolamenti attuativi e tecnici dell'art. 15 comma 2 della legge 15 marzo 1997 n. 59 - l'ente certificatore abbia certificato e pubblicato una determinata chiave pubblica e questa sia stata utilizzata per decrittare un documento si può identificarne con assoluta certezza l'autore.

In realtà perché tale effetto si produca è necessario che il destinatario abbia verificato nell'apposito registro tenuto dall'autorità di certificazione che la chiave pubblica attribuita al mittente non sia scaduta ovvero non sia stata revocata o sospesa (ad esempio a seguito di segnalazione da parte del mittente stesso della perdita della segretezza della chiave privata).

Quanto alla funzione dichiarativa - di assunzione della paternità del contenuto di un documento -, essa è conseguenza dell'equiparazione del documento informatico alla scrittura privata (artt. 5 comma 1 e 10 comma 2 D.P.R. 513/97) per la quale opera la presunzione che colui che sottoscrive un documento ne sia l'autore.

In altre parole: una volta risaliti, attraverso il certificatore, al "titolare della firma" (nel senso sopra precisato) si può ritenere che tale soggetto abbia approvato ed accettato le dichiarazioni sottoscritte con la firma digitale, potendosi escludere con certezza - ed allo stato attuale delle cognizioni tecniche - la possibilità di alterazione del documento successiva all'apposizione della firma digitale.

Quanto - infine - alla funzione probatoria essa è il risultato, come per la firma

tradizionale, dell'unione delle due precedenti funzioni (indicativa e dichiarativa) costituendo il documento informatico la prova - salvo dimostrazione del contrario - della provenienza delle dichiarazioni in esso contenute dal soggetto individuato come titolare della chiave pubblica e legittimo utilizzatore di quella privata ad essa abbinata.

Possiamo -quindi - concludere che la firma digitale assolve alle tre funzioni tipiche della firma tradizionale e che - anzi - per le particolari caratteristiche della firma digitale tali funzioni sono rafforzate.

Sul piano processualcivilistico l' applicazione della firma digitale esclude, a nostro avviso, la possibilità di invocare l'art. 214 cpc che prevede la possibilità, per colui contro il quale é prodotta in giudizio una determinata scrittura privata, di disconoscerla « nega(ndo) formalmente la propria scrittura o la propria sottoscrizione ».

Non é difficile, peraltro, prevedere che il problema si sposterà sulla prova che dovrà offrire il "titolare della firma digitale" (rectius delle chiavi) della violazione della propria chiave privata prima dell' apposizione sul documento elettronico e sulla tutela dei terzi ai quali tale violazione non potrà essere opposta se non conosciuta o conoscibile per intervenuta pubblicazione della sospensione o della revoca della chiave pubblica negli appositi registri tenuti dall'autorità di certificazione.

Sul punto é utile ricordare che:

- ai sensi dell' art. 9, comma 1 del D.P.R. 513/97 « *Chiunque intenda utilizzare un sistema di chiavi asimmetriche o della firma digitale, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.* »,
- ai sensi dell' art. 10, comma 5 del D.P.R. 513/97 « *L'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa 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. » ,

- ai sensi dell' art. 8 n. 4 del decreto del Presidente del Consiglio dei Ministri approvato l' 11 febbraio 1999 « *Il titolare delle chiavi deve:*
 - a. conservare con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;*
 - b. conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;*
 - c. richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi. » .*

Le norme appena citate costituiscono applicazione di due principi fondamentali:

- il principio dell'affidamento, secondo il quale non é opponibile ai terzi l'abuso della firma digitale (vale a dire l'uso da parte di persona non autorizzata) fino a quando non é stata pubblicata la sospensione ovvero la revoca della chiave pubblica negli appositi registri tenuti dall'Autorità di Certificazione emittente;
- il principio della responsabilità del titolare della chiave privata di denunciare alla competente autorità la violazione o lo smarrimento della chiave privata e, in difetto, dell'assunzione in capo al predetto titolare di tutte le conseguenze di tale negligenza, prima fra tutte la paternità del documento firmato con firma digitale apposta con chiave segreta violata.

Tralasciando altri aspetti - pur interessanti - ma prettamente tecnici, vanno spese poche parole sulla data del documento elettronico che, pur non rientrando specificamente nel

tema oggetto di discussione, riteniamo indispensabile approfondire.

Com'è noto dalla data di un documento, in particolare dal fatto che esso sia stato formato prima o dopo un determinato evento o un altro documento, discendono importanti conseguenze giuridiche.

Normalmente chi forma e sottoscrive un documento tradizionale, destinato ad essere esteriorizzato, indica anche il luogo e la data in cui esso è stato formato.

Tale data non è però "certa", vale a dire non può essere opposta ai terzi, salvo che non si verifichi una delle condizioni previste dall' art. 2704 cod. civ. secondo il quale: « *La data della scrittura privata della quale non è autenticata la sottoscrizione non è certa e computabile riguardo ai terzi se non dal giorno in cui la scrittura è stata registrata o dal giorno della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta o dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici o, infine, dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento ...* »

Orbene la data del documento elettronico non può essere certificata dalla firma digitale che, quand'anche potesse essere desumibile e riferibile al momento di completamento del processo di cifratura del documento, non sarebbe, comunque, opponibile ai terzi.

A risolvere il problema soccorre la procedura di "validazione temporanea" definita all' art. 1 lett i del D.P.R. 513/97 « *nel risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi* »

In estrema sintesi la procedura è la seguente:

- il soggetto mittente di un documento al quale vuole venga attribuita una data certa, trasmette l'"impronta del documento" (consistente in una specie di riassunto molto

compreso del documento stesso, che si ottiene mediante l'applicazione di una funzione di hash, e che impedisce a chi riceve tale "impronta" di conoscere il documento dal quale tale impronta é stata generata senza compromettere, quindi, la confidenzialità del documento stesso) ad un servizio di marcatura affidato ad una terza parte, normalmente un' autorità di certificazione;

- il servizio di marcatura aggiunge all' impronta ricevuta la data e l' ora ottenendo un'"impronta marcata";
- l'impronta marcata viene crittata con la chiave privata del servizio di marcatura ottenendo la marcatura temporanea che viene, quindi, trasmessa al richiedente il quale la allega al documento da trasmettere al destinatario.

Da ultimo va detto che il D.P.R. 10 novembre 1997 n. 513 ha altresì previsto la possibilità di autenticazione della firma digitale.

La norma specifica é contenuta all' art. 16 che, non richiedendo particolare interpretazione, riportiamo testualmente:

« *Firma digitale autenticata.*

1. *Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato.*
2. *L'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, primo comma, numero 17, della legge 16 febbraio 1913, n. 89 (6).*

3. *L'apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.*
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 6 del presente regolamento.*
5. *Ai fini e per gli effetti dell'articolo 3, comma 11, della legge 15 maggio 1997, n. 127 (7), si considera apposta in presenza del dipendente addetto la firma digitale inserita nel documento informatico presentato o depositato presso pubbliche amministrazioni.*
6. *La presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione sono validi a tutti gli effetti di legge se vi sono apposte la firma digitale e la validazione temporale a norma del presente regolamento. »*

La realizzazione, da parte del legislatore, di una articolata e, per certi aspetti, coraggiosa disciplina del documento elettronico e della firma digitale fa ben sperare nella rapida diffusione di tali nuovi sistemi che, nelle previsioni, dovrebbe ridurre i tempi della burocrazia ed il carico degli archivi, pubblici e privati, a condizione che, ora che tutte le norme dovrebbero essere state emanate, se ne dia celere attuazione.

Milano 23 febbraio 1999

Articolo 1 Regolamento di cui al D.P.R. 10.11.1997 n. 513

Definizioni - 1. ai fini del presente regolamento si intende:

- a) per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- b) per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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;
- c) per sistema di validazione, il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità;
- d) per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici;
- e) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica;
- f) per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi;
- g) per chiave biometrica, la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente;
- h) per certificazione, il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni;

- i) per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;
- l) per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;
- m) per certificatore, il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;
- n) per revoca del certificato, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;
- o) per sospensione del certificato, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo;
- p) per validità del certificato, l'efficacia, e l'opponibilità al titolare della chiave pubblica, dei dati in esso contenuti;
- q) per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.