Il Codice dell'Amministrazione Digitale

IL DOCUMENTO INFORMATICO

Prefettura di Reggio Calabria

23-25 novembre 2010

www.vincenzocalabro.it

Definizione di documento

Il documento deve avere le seguenti caratteristiche:

1) Essere di natura materiale (carta, nastro magnetico)
2) Avere contenuto materiale (voce) o immateriale (segni espressivi che rappresentano un'idea)
3) Essere intelligibile (deve essere in grado di essere percepito dagli altri)
4) Avere la capacità di rappresentare in modo permanente un atto/fatto giuridico

Documento cartaceo

- Nel caso di un documento cartaceo c'è un legame diretto tra le informazioni contenute nel documento e il supporto atto a contenerle: il tipo di carta o di inchiostro utilizzato costituiscono proprietà distintive di un documento;
- l'identificazione dell'autore è affidata alla firma autografa: la calligrafia, infatti, è tradizionalmente considerata un elemento identificativo della persona, anche se lascia uno spazio notevole alle falsificazioni.

Documento informatico

Il cambiamento di supporto produce una differenza evidente:

- un documento informatico è riproducibile indefinitamente e modificabile con estrema facilità;
- non si può distinguere tra un documento originale e le corrispondenti copie;
- qualunque computer è infatti in grado di generare lo stesso documento.

Nel documento elettronico viene quindi a cadere il legame diretto tra informazione e relativo supporto, legame che, come è stato detto, caratterizza in qualche modo il documento cartaceo

Dematerializzazione

l termine dematerializzazione indica il progressivo incremento della gestione documentale informatizzata - all'interno delle strutture amministrative pubbliche e private - e la conseguente sostituzione dei supporti tradizionali della documentazione amministrativa in favore del documento informatico, a cui la normativa statale, fin dal 1997 riconosce pieno valore giuridico.

Definizione di documento informatico

PENALE	AMMINISTRATIVO
Articolo 491-bis c.p.: supporto che contiene dati o informazioni aventi efficacia probatoria o programmi destinati ad elaborarli	Articolo 2, D.P.R. 513/97: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (D.P.R. 513/97).

Sottoscrizione

La sottoscrizione autografa

La sottoscrizione autografa consiste nella scrittura di pugno del patronimico (nome e cognome) in calce ad un documento. La sottoscrizione svolge tre funzioni fondamentali:

1) Funzione **indicativa**: identificare l'autore del documento
2) Funzione **dichiarativa**: permette di affermare che il documento a cui la sottoscrizione è stata apposta è stato formato per conto di chi sottoscrive
3) Funzione **probatoria**: consente di provare l'identità del firmatario

La sottoscrizione del documento informatico

Il D.P.R. 513/97 conferisce formale riconoscimento della firma digitale quale strumento per la sottoscrizione di documenti informatici.

L'Italia, è stato uno dei primi paesi europei ad introdurre una disciplina organica in tema di firma digitale e documento informatico, preceduta solo dalla Germania

ITALIA: Attenzione al riconoscimento giuridico

GERMANIA ed altri: Attenzione alla sicurezza e all'uniformità tecnologica

Evoluzione normativa della firma elettronica

1	Legge 15 marzo 1997, n. 59 (Legge "Bassanini"):	Documenti creati con strumenti informatici sono validi a tutti gli effetti di legge
2	D.P.R. 10 novembre 1997, n. 513	Definizione di documento informatico e firma digitale
3	D.P.C.M. 8 febbraio 1999	Regole tecniche dei documenti informatici
4	D.P.R. 28 dicembre 2000, n. 445	Testo unico in materia di documentazione amministrativa
5	D.Lgs. 23 gennaio 2002, n. 10	Definizione di firma elettronica
6	D.Lgs. 7 marzo 2006, n. 82	Codice dell'Amministrazione Digitale
7	D.Lgs. 4 aprile 2006, n. 159	Modifiche al Codice dell'Amministrazione Digitale

Codice Amministrazione Digitale

Dopo un lungo e contraddittorio iter legislativo l'articolo 1 del Codice dell'Amministrazione Digitale individua tre differenti tipologie di firma elettronica:

1. Firma elettronica semplice
2. Firma elettronica qualificata
3. Firma digitale

Firma elettronica semplice

Firma elettronica “semplice”: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica

- Si riferisce a metodi di autenticazione aventi scarsi requisiti di sicurezza (PIN o password)
- Non viene considerata come procedura di sottoscrizione, ma al massimo come strumento di autenticazione

Firma elettronica qualificata

Firma elettronica qualificata: è quella ottenuta attraverso una procedura informatica che garantisca:

- la connessione univoca al firmatario
- la sua univoca autenticazione informatica
- la presenza di un certificato qualificato
- la sua creazione mediante un dispositivo sicuro per la creazione della firma

Firma digitale

Firma digitale: è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

La firma digitale

La caratteristica innovativa della firma digitale è che essa è intrinsecamente legata al testo a cui è apposta.

Testo e firma possono quindi anche essere oggetti fisicamente separati senza che questo elimini il legame esistente tra loro.

A testi diversi di uno stesso autore corrispondono firme diverse e quindi risulta perfettamente inutile tentare di associare una firma digitale ad un testo differente da quello originario.

Il ruolo dei Certificatori

Il pieno collegamento soggettivo tra la firma digitale e il soggetto firmatario richiede l'intervento di un soggetto imparziale che agisca quale terza parte fidata per certificare la chiave pubblica e autenticare la firma

Il Codice dell'Amministrazione Digitale distingue in:

A) **Certificatori**: soggetti che prestano servizi di certificazione delle firme elettroniche

B) **Certificatori qualificati**: soggetti che rilasciano al pubblico certificati conformi ai requisiti indicati dal CAD e dalle regole tecniche

C) **Certificatori accreditati**: soggetti che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato in termini di qualità e sicurezza inseriti in un apposito elenco gestito dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione

I certificati elettronici e la validazione temporale

I certificati sono documenti elettronici che contengono informazioni garantite circa il titolare della chiave. Si distinguono in elettronici e qualificati a secondo del contenuto del certificato e della qualità del certificatore.

La **validazione temporale** consente di attribuire ad uno o più documenti una data ed un orario opponibile a terzi, garantendo il momento della loro formazione e sottoscrizione.

Premesso che il certificato elettronico ha una durata limitata nel tempo è possibile protrarre l'effetto e la validità di un documento elettronico attraverso l'apposizione di una **marca temporale**.

La validazione temporale e la marca temporale sono servizi che deve necessariamente garantire l'ente certificatore.

Il dispositivo di firma

Il dispositivo di firma può essere una smart card o un token usb contenente la chiave privata che associata ad un software specifico, genera la firma digitale apponendola ad un documento informatico.

Il dispositivo deve garantire che la firma sia:

1) Riservata
2) Protetta da contraffazioni
3) Protetta dall'uso da parte di terzi

Firma digitale e crittografia

La firma digitale è il risultato dell'applicazione al documento in forma elettronica di una coppia di **chiavi asimmetriche**, secondo determinati standards e procedure previste dalla legge

Tali chiavi sono il risultato di una particolare tecnica di **crittografia** nata con l'avvento della tecnologia informatica

La **crittografia** consiste nella capacità di rendere segreto il contenuto di un messaggio ad eccezione del destinatario finale prescelto

Crittografia simmetrica

Con **crittografia simmetrica** si intende una tecnica di **cifratura**. Uno schema di crittografia simmetrica è caratterizzato dalla proprietà che, data la chiave di cifratura “X", sia facilmente calcolabile la chiave di decifratura “Y". Nella pratica, tale proprietà si traduce nell'utilizzo di una sola chiave sia per l'operazione di cifratura che quella di decifratura. La forza della crittografia simmetrica è dunque riposta nella segretezza dell'unica chiave utilizzata dai due interlocutori che la usano, oltre che nella grandezza dello spazio delle chiavi, nella scelta di una buona chiave e nella resistenza dell'algoritmo agli attacchi di crittanalisi

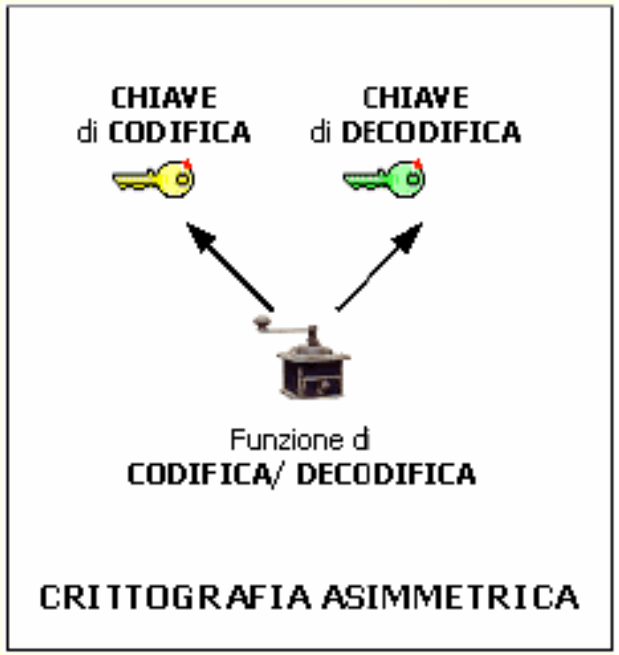
Crittografia asimmetrica

Con **crittografia asimmetrica** si intende un tipo di crittografia dove, ad ogni attore coinvolto, è associata una coppia di chiavi:

- **chiave privata**: personale e segreta, viene utilizzata per decifrare un documento cifrato;
- **chiave pubblica**: serve a cifrare un documento destinato alla persona che possiede la relativa chiave privata.

La chiave pubblica e privata utilizzano per cifrare e decifrare il documento una funzione matematica detta di **hashing**

L'**hash code** è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata



Apposizione firma digitale

1. Si calcola, tramite una funzione di Hash, l'impronta del documento informatico
2. Al risultato della funzione si applica l'algoritmo di crittografia asimmetrico utilizzando la propria chiave privata presente sul dispositivo di firma
3. Si unisce il risultato dell'elaborazione al documento originario

Verifica firma digitale

1. Si ricava la chiave pubblica del firmatario del documento informatico
2. Si verifica la validità temporale del certificato rispetto alla data di firma del documento
3. Si applica l'algoritmo di crittografia asimmetrico per decodificare, con la chiave pubblica del firmatario, l'impronta del documento
4. Si ricalcola l'impronta del documento informatico
5. Si confrontano i risultati della due funzioni: se coincidono la firma è valida, altrimenti è falsa

Le caratteristiche di un documento informatico firmato digitalmente

- **Integrità**
  Garanzia che il documento non è stato manomesso dopo la sottoscrizione.
- **Autenticità**
  Garanzia dell'identità di chi firma.
- **Non ripudio**
  L'autore non può disconoscere il documento firmato.
- **Valore legale**
  il documento elettronico sottoscritto digitalmente ha lo stesso valore legale di un documento cartaceo sottoscritto con firma autografa.

Il sistema a doppia cifratura: verifica mittente

1. Il mittente spedisce il suo plico postale (mail) al destinatario chiudendolo con il suo lucchetto (chiave privata)
2. Il destinatario apre il plico postale (mail) con la chiave pubblica del mittente

Il sistema a doppia cifratura : verifica destinatario

1. Il mittente preleva il lucchetto aperto (chiave pubblica) del destinatario
2. Il mittente chiude il suo plico (mail) con il lucchetto e lo spedisce al destinatario
3. Il destinatario una volta ricevuto il plico potrà aprirlo con la sua chiave privata

Valore probatorio

Art. 20 - Il documento informatico

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice .

1-bis. L'idoneita' del documento informatico a soddisfare il requisito della forma scritta e' liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di **qualita', sicurezza, integrita' ed immodificabilita**', fermo restando quanto disposto dal comma 2.

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, …, che garantiscano l'identificabilita' dell'autore, l'integrita' e l'immodificabilita' del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullita', dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

Art. 21. Valore probatorio del documento informatico sottoscritto

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrita' e immodificabilita.
2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.
3. 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.

Efficacia del documento informatico

Firma elettronica “Semplice”	Il documento informatico a cui è stata apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio	Firma “debole” o “leggera”
Firma elettronica qualificata o firma digitale	Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l’efficacia prevista dall’articolo 2702 del codice civile (scrittura privata con inversione dell’onere della prova)	Firma “sicura”
Firma elettronica autenticata	L’autenticazione della firma digitale o di altro tipo di firma elettronica qualificata avviene mediante attestazione di un Pubblico Ufficiale (articolo 2703 del codice civile)	Firma “autenticata”

Art. 22. Documenti informatici originali e copie. Formazione e conservazione

1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.
2. Nelle operazioni riguardanti le attività di produzione, immissione, conservazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate, sia il soggetto che ha effettuato l'operazione.
3. Le copie su supporto informatico di documenti formati in origine su altro tipo di supporto sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

Art. 23. Copie di atti e documenti informatici

1. All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «, informatiche».
2. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge, se conformi alle vigenti regole tecniche.

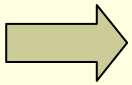
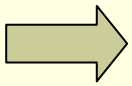
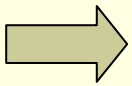
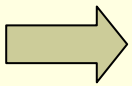
2-bis. Le copie su supporto cartaceo di documento informatico, anche sottoscritto con firma elettronica qualificata o con firma digitale, sostituiscono ad ogni effetto di legge l'originale da cui sono tratte se la loro conformita' all'originale in tutte le sue componenti e' attestata da un pubblico ufficiale a cio' autorizzato.

3. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.

Art. 23. Copie di atti e documenti informatici

4. Le copie su supporto informatico di qualsiasi tipologia di documenti analogici originali, formati in origine su supporto cartaceo o su altro supporto non informatico, sostituiscono ad ogni effetto di legge gli originali da cui sono tratte se la loro conformità all'originale è assicurata da chi lo detiene mediante l'utilizzo della propria firma digitale e nel rispetto delle regole tecniche di cui all'articolo 71.
5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione ottica sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.
6. La spedizione o il rilascio di copie di atti e documenti di cui al comma 3, esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.
7. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71 di concerto con il Ministro dell'economia e delle finanze.

Originale e Copia

Originale		**Copia**	
Cartaceo		Cartaceo	Copia Conforme Manuale
Cartaceo		Digitale	Copia Conforme Digitale
Digitale		Digitale	Copia Autentica
Digitale		Cartaceo	Copia Conforme Manuale

Art. 34. Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati

Comma 2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71.

Art. 35. Dispositivi sicuri e procedure per la generazione della firma

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
   - sia riservata;
   - non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
   - possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

Art. 36. Revoca e sospensione dei certificati qualificati

1. Il certificato qualificato deve essere a cura del certificatore:

   a. revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;
   b. revocato o sospeso in esecuzione di un provvedimento dell'autorità;
   c. revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;
   d. revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

Art. 38. Pagamenti informatici

1. Il trasferimento in via telematica di fondi tra pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche stabilite ai sensi dell'articolo 71 di concerto con i Ministri per la funzione pubblica, della giustizia e dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia

Art. 39. Libri e scritture

1. I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice e secondo le regole tecniche stabilite ai sensi dell'articolo 71

Conclusioni

Pro

- Utilizzare il supporto cartaceo comporta costi considerevoli di materia prima e di personale addetto all'archiviazione e al reperimento dei documenti stessi. Senza contare il costo più rilevante, vale a dire il rallentamento nei processi decisionali dettato dall'uso del supporto cartaceo.

L'alternativa è di ricorrere al documento informatico.

- Questa alternativa è resa possibile dalla tecnologia della firma digitale. Tale possibilità tecnica apre nuovi scenari: il flusso documentale cartaceo può essere sostituito dal flusso documentale informatico. Il ciclo di vita dei documenti elettronici può quindi essere completamente gestito in maniera elettronica con conseguenti vantaggi sia in termini di incremento della velocità di trattamento delle informazioni sia economici.

Contro

I vantaggi scompaiono se il flusso documentale non è omogeneo: cartaceo o digitale

Ogni passaggio cartaceo-digitale o viceversa comporta:

- Incremento del lavoro di digitalizzazione
- Incremento dell'uso della carta
- Incremento delle azioni di autenticazione