IL DOCUMENTO INFORMATICO

Premessa.
Da oltre un decennio si è registrato un graduale abbandono dei tradizionali documenti cartacei in favore dei documenti su supporto informatico.
La diffusione delle ICT (Information and Communications Technology) ha favorito il progressivo abbandono del documento cartaceo tradizionale in favore di documenti realizzati su supporto informatico: il contenuto del documento rimane lo stesso, mentre varia il contenuto estrinseco dall'analogico al digitale, con notevoli ricadute in termini di sicurezza informatica. Il passaggio da un segno analogico ad uno digitale infatti aumenta l'esposizione ad effrazione e modifiche.
L'uso delle ICT solleva diverse questioni, prima fra tutte quella della rilevanza giuridica dei nuovi strumenti di memorizzazione e rappresentazione, in particolare dal punto di vista processuale e della prova documentale. Gli operatori del diritto si trovano di fronte all'interrogativo se tale documento informatico possa generare effetti di natura privatistica e pubblicistica.
Il principio generale riconosciuto dal nostro ordinamento giuridico è che al documento informatico è riconosciuta validità e rilevanza a tutti gli effetti di legge. Tuttavia ci sono delle differenziazioni secondo il documento che ci si trova di fronte e, come meglio si vedrà in seguito, al tipo di forma digitale che in esso è apposta.

Il ruolo dell'*e-Government*.
Con l'espressione ***e-Government*** comunemente si indica il processo di informatizzazione della P.A., ovvero la possibilità di avvalersi delle moderne ICT per lo svolgimento delle attività amministrative, al fine di offrire ai cittadini un servizio pubblico più efficiente, più rapido, più economico e più trasparente.
La progressiva implementazione dei progetti di ***e-Government*** ha via via determinato lo sviluppo e all'introduzione dei sistemi di ***document management*** volti a favorire una più efficiente gestione delle risorse e delle informazioni all'interno della P.A.
Il ***Document Management Sistem*** **(DMS)** consiste in particolari sistemi di *software* che consentono, e facilitano, la formazione, l'organizzazione e lo scambio di documenti all'interno di una stessa organizzazione.

Le fonti normative del documento informatico
L'excursus legislativo, caratterizzato dall'eterogeneità dei testi normativi di riferimento, prende le mosse dalla legge n. 241 del 1990 per culminare nel d.lgs. n. 82 del 2005 (cd. CAD, Codice dell'Amministrazione Digitale), una disciplina valevole *erga omnes* che ha avuto il compito di recepire e riordinare in un unico testo la normativa esistente in materia.

a) **Legge 241/1990**: l'art. 22, comma 1, lett. d) costituisce il primo riconoscimento del documento informatico e attribuisce rilevanza giuridica all'atto amministrativo elettronico.
Con l'espressione documento informatico si intende: "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale*".

b) **D.Lgs. 39/1993:** l'art. 3 è particolarmente significativo, non solo perché al **primo comma** affermava "*gli atti amministrativi adottati da tutte le pubbliche amministrazioni sono di norma predisposti tramite i sistemi automatizzati*", ma anche – e soprattutto – perché nel **secondo comma** introduceva un'importante novità nel criterio di imputazione degli atti amministrativi: "*Nell'ambito*

delle pubbliche amministrazioni l'immissione, la riproduzione su qualunque supporto e la trasmissione di dati, informazioni e documenti mediante sistemi informatici o telematici, nonché l'emanazione di atti amministrativi attraverso i medesimi sistemi, devono essere accompagnate dall'indicazione della fonte e del responsabile dell'immissione, riproduzione, trasmissione o emanazione. Se per la validità di tali operazioni e degli atti emessi sia prevista l'apposizione di firma autografa, la stessa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile".
Ulteriore elemento di novità è costituito dalla possibilità di **sostituire** la **firma autografa** del responsabile del procedimento con **un'indicazione a stampa del suo nominativo**.

c) **Legge 547/1993**: il testo legislativo, meglio noto come Legge sui crimini informatici, poi abrogato, dalla Legge 48/2008, ha compiuto un ulteriore passo in avanti in ambito penale introducendo l'art. 491- *bis* c.p. che ha fornito una definizione di documento informatico, chiarendo che con tale espressione si intende "*qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*".

d) **D.L. 357/1994:** l'art. 7 comma 4-*ter* ha sancito espressamente la regolarità a tutti gli effetti di legge delle scritture contabili tenute con sistemi meccanografici.

e) **Legge 59/1997** cd. Prima Legge Bassanini: l'avvento del complesso legislativo costituito dalle Leggi Bassanini (nn. 59/1997, 127/1997, 191/1998 e 50/1999) costituisce uno dei passaggi più significativi in tema di riordino della Pubblica Amministrazione, anche e soprattutto nei rapporti con i privati e sempre nell'ottica più generale di e-Government. In particolar modo, la Legge n. 59 si è occupata di documenti informatici sintetizzando, ampliando, riordinando ed elaborando ulteriormente l'evoluzione normativa in tale ambito.
Prima dell'avvento di tale legge si parlava ancora di atti ad elaborazione elettronica, ovvero di atti non assistiti da strumenti di firma in senso proprio: si trattava cioè di atti predisposti mediante personal computer ma stampati su formato cartaceo, non si trattava quindi di documento dematerializzato.
La legge Bassanini ha avuto il grande merito di riunire in un unico *corpus* la disciplina relativa all'attività di formazione, archiviazione e trasmissione, ma soprattutto di introdurre il principio di generale rilevanza e validità dell'attività giuridica in forma elettronica. In particolare l'art. 15**,** comma 2, afferma che**:** "*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*".
Conseguentemente si può affermare che con la legge Bassanini gli atti della P.A. e i negozi privati – emanati e stipulati mediante l'utilizzo di sistemi informatici e telematici – divengono dunque validi e rilevanti a prescindere dalla loro trasposizione sulla carta: la versione cartacea dell'atto deve dunque considerarsi alla stregua di una copia del documento originale informatico.

f) **D.P.R. 513/1997:** con il "*Regolamento contenente i criteri e le 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. 59/1997*" si è voluto delineare un quadro normativo di riferimento in tema di firma elettronica volto a garantire l'applicazione del sistema generale di sottoscrizione elettronica e a uniformare i procedimenti legati alla generazione, conservazione e certificazione delle chiavi elettroniche in modo da rendere interoperabili le applicazioni e i sistemi, pubblici e privati.

g) **D.P.R. 445/2000:** il "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*", in materia di gestione informatizzata dei documenti

amministrativi, ha segnato profondamente l'organizzazione dei documenti generati dalla P.A., proponendosi di garantire una maggiore efficienza dell'attività amministrativa e un migliore accesso ai documenti e ai procedimenti amministrativi.

h) **D.P.C.M. del 13/01/2004**: ha ultimato il recepimento della Direttiva europea 1999/93/CE introducendo le "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici". Questo testo normativo ha disciplinato le modalità di formazione dei documenti amministrativi attraverso i supporti informatici, riservando una particolare attenzione alle attività di generazione**,** apposizione e verifica delle firme digitali.

i) Deliberazione **CNIPA n. 4 del 17/02/2005:** ha introdotto le "Regole per il riconoscimento e la verifica del documento informatico" che devono essere rispettate e applicate dai certificatori accreditati.

l) **D.Lgs. 82/2005:** recentemente modificato e integrato dalla Legge 98/2013 e dalla Legge 147/2013, il testo è meglio conosciuto come **CAD** – Codice della Pubblica Amministrazione Digitale e ha riconosciuto l'importanza fondamentale del documento informatico, dal momento che non può esistere una P.A. digitale senza quelle imprescindibili attività di formazione, trasmissione e conservazione di documenti amministrativi realizzati interamente in formato elettronico.
Inoltre il CAD fornisce all'art.1 le definizioni attuali di documento informatico, "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*" (lett. p), per distinguerlo dal documento analogico di cui alla successiva lett. p bis) "*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*".
Fra le numerose modifiche introdotte con l'entrata in vigore del Codice dell'Amministrazione Digitale, deve necessariamente menzionarsi l'art. 21 il cui comma 2 ha accresciuto ulteriormente il valore probatorio del documento informatico, sancendo che "*Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria*".

Il documento informatico e le sue categorie.
In linea generale un documento è costituito da due elementi che riguardano parimenti il documento informatico:
•un elemento **"materiale" ed "estrinseco"**, che costituisce il supporto e l'involucro espressivo della capacità rappresentativa del documento stesso;
•un contenuto **"immateriale" e "intrinseco"** che esprime una determinata porzione di realtà.
La categoria del documento informatico è scindibile in 3 categorie che individuano tre situazioni diverse.
a) DOCUMENTO ELETTRONICO: è il documento frutto della procedura di **acquisizione elettronica** di **documenti già esistenti**, che si articola in tre fasi: l'acquisizione mediante scansione elettronica, la conversione in formato *file*, la distribuzione e diffusione all'interno di un sistema informatico.
Vantaggi: diminuzione dei tradizionali archivi cartacei e maggiore riproducibilità dei documenti su differenti supporti.
b) DOCUMENTO DIGITALE: è il risultato del processo di creazione e gestione di documenti ottenuto utilizzando il canale digitale.

Si tratta di un documento che – affrancandosi completamente dal suo corrispondente cartaceo – può essere generato e utilizzato anche esclusivamente nel contesto dematerializzato di una rete telematica.
Vantaggi: l'impiego del documento digitale comporta notevoli vantaggi soprattutto a livello di interoperabilità e di cooperazione. Inoltre, la sua struttura standardizzata garantisce una facile veicolazione e un migliore scambio delle informazioni anche attraverso sistemi informativi diversi.
c) DOCUMENTO INFORMATICO: è definito dall'art.1, comma 1, lett p) CAD come "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".
In particolare, l'art. 20, comma 1, CAD dispone che "*Il documento informatico da chiunque formato, la memorizzazione 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*". È evidente che il documento ha acquisito definitivamente piena rilevanza giuridica a prescindere che ad esso sia o meno assistito da un dispositivo di firma.

Il valore probatorio del documento informatico.
In realtà l'equiparazione del valore probatorio del documento informatico a quella del documento cartaceo viene specificata dal combinato disposto degli art. 20, comma 1-bis – a norma del quale "*l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21*" – e dell'art. 23-quater – che, previa modifica dell'art. 2712 del codice civile, ha inserito le riproduzioni informatiche nell'elenco delle rappresentazioni meccaniche di fatti o di cose che "*formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime*".
Ne deriva che il documento informatico – ancorché non sottoscritto – è giuridicamente rilevante, al pari di qualunque altra registrazione di atti o fatti. Dal punto di vista sostanziale dunque esso è equiparabile a un documento cartaceo: è valido ed è liberamente valutabile in giudizio esattamente come un qualsiasi atto scritto.

Il valore probatorio del documento informatico munito di forma digitale.
Riguardo al documento informatico munito di firma digitale è necessario procedere ad ulteriori considerazioni, che presuppongono la distinzione tra firme deboli (elettronica semplice) e firme forti (elettronica avanzata, elettronica qualificata, digitale), la quale si ripercuote anche sul valore probatorio del documento medesimo.
Tale differenziazione ha trovato riscontro anche sul piano normativo, come emerge dalla bipartizione prevista dai primi due commi dell'art. 21 del CAD:
a) dal comma 1 del predetto articolo – a norma del quale "*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, integrità e immodificabilità*" – si evince che il documento informatico munito di firma elettronica semplice è sottoposto alla valutazione del giudice, libera e discrezionale;
b) in base al comma 2 – a norma del quale "*Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria*" – il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale fa piena prova, sino a querela di falso, della provenienza delle dichiarazioni dal sottoscrittore, a meno che questi non provi il contrario.

La firma elettronica.
Nell'ambito del progressivo adattamento dell'ordinamento giuridico alle nuove tecnologie dell'informazione e della comunicazione, la firma digitale – *rectius* elettronica – ha assunto lo specifico ruolo di strumento di validazione e di garanzia della certezza della provenienza dei documenti informatici, assicurandone inoltre l'integrità e la segretezza.
Il passaggio dalla **sottoscrizione analogica** a quella **digitale** ha comportato considerevoli ricadute poiché la firma analogica svolge una duplice funzione: a) indicativa della provenienza del documento dal soggetto che appone la firma, il quale viene indicato come il titolare e responsabile del documento e b) dichiarativa, nel senso che attribuisce la paternità del documento sottoscritto.
Si tratta tuttavia di funzioni che permangono con l'avvento della firma digitale, ma che assumono una connotazione diversa in quanto se è vero che un codice alfanumerico può sostituire un segno, sorgono problemi in ordine al concetto di identificazione e attribuzione di paternità del documento: il codice alfanumerico dà certezza in ordine alla proprietà del dispositivo di forma digitale.

Le funzioni indicativa e dichiarativa della firma digitale.
L'avvento dei dispositivi di firma elettronica ha reso evidente la necessità di ripensare e rivedere le funzioni svolte dalla sottoscrizione autografa dei documenti. Più precisamente si tratta di due funzioni:
a) **FUNZIONE INDICATIVA,** grazie alla quale è possibile identificare l'autore del documento;
b) **FUNZIONE DICHIARATIVA,** in virtù della quale la paternità del documento viene attribuita al suo sottoscrittore.
Le nuove firme non fanno venir meno dette funzioni che continuano ad operare seppur in modo assolutamente diverso. In particolare, la sostituzione della firma autografa con quella elettronica ha determinato un radicale mutamento della funzione indicativa.
Per assolvere tale funzione, la firma autografa doveva possedere alcuni requisiti:
• **nominatività**, nel senso che essa doveva contenere l'indicazione del nome e del cognome del soggetto scrivente;
• **autografia**, nel senso che doveva essere apposta di proprio pugno e "a mano libera";
• **leggibilità**, nel senso che doveva essere chiara, e, dunque, non doveva richiedere particolari sforzi di decifrazione.
Con l'avvento della firma elettronica di questi requisiti "resiste" solo la nominatività che, però, si trasforma, o, meglio, viene sostituita dalla "nominatività elettronica". In pratica, sebbene non contenga l'indicazione del nome e del cognome del sottoscrittore ma sia **costituita da un codice**, la firma svolge comunque la funzione indicativa, consentendo di individuare l'autore del documento.
Il passaggio dalla sottoscrizione autografa a quella meccanico-eterografa ha modificato anche la funzione dichiarativa in quanto la firma viene apposta tramite la digitazione di un codice che permette l'applicazione della chiave privata. Ne deriva una vera e propria spersonalizzazione della firma in quanto non si ha più la paternità di questa, ma la titolarità del dispositivo.

Il riconoscimento giuridico della forma elettronica.
Nel contesto dell'Unione Europea, l'ordinamento giuridico italiano è stato uno dei primi a sviluppare una normativa volta al pieno riconoscimento della validità giuridica della firma digitale, stabilmente introdotta con il D.P.R. 513/1997.
A partire dal 1997, e poi via via sino all'entrata in vigore del Codice dell'Amministrazione Digitale, la firma è così diventata uno degli strumenti-cardine del processo di *e-Government*.
Il CNIPA, già nel maggio del 2004, aveva predisposto le prime *Le linee guida per l'utilizzo della firma digitale*, un testo elaborato al fine di fornire ai cittadini, alle imprese e alle pubbliche amministrazioni i riferimenti tecnici necessari per l'utilizzazione dei meccanismi di firma digitale, esplicitamente qualificati come mezzi utili "*nel momento in cui risulta necessario sottoscrivere una dichiarazione ottenendo la garanzia di integrità dei dati oggetto della sottoscrizione e di autenticità delle informazioni relative al sottoscrittore*".

Le firme digitali.
Il CAD distingue 4 tipologie di firme digitali – semplice, avanzata, qualificata e digitale – ulteriormente qualificabili in "forti" (firme avanzata, qualificata e digitale) e "debole" (firma semplice) in ragione del differente valore probatorio.

A) **Firma semplice**: "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*" (art. 1, comma 1, q).
Rappresenta la forma più leggera di sottoscrizione elettronica dei documenti. Si tratta, infatti, di una firma non assistita da un sistema di certificazione accreditato. Quindi sotto il profilo sostanziale è equivalenti a tanti meccanismi già adottati in rete (es. password o pin), sotto il profilo probatorio è liberamente valutabile in giudizio.

B) **Firma avanzata**: "*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*" (art. 1, comma 1, q-bis).
Si tratta di una firma elettronica che si distingue per la presenza di alcune peculiari caratteristiche di sicurezza aggiuntive rispetto alla firma elettronica semplice, consentendo di attribuire al documento un maggiore valore probatorio. È definita la più leggera delle firme "forti".
Questa tipologia di firma consente l'identificazione del firmatario e la connessione univoca dello stesso al documento firmato, prevede l'uso di mezzi sui quali il firmatario può conservare il controllo esclusivo e consente di rilevare se i dati sono stati modificati successivamente all'apposizione della firma.

C) **Firma qualificata**: "*un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma*" (art. 1, comma1, r).
Questa firma ha assunto un'efficacia parificabile a quella di una scrittura privata, ai sensi e per gli effetti di cui all'art. 2702 c.c. in quanto garantisce l'assoluta riconducibilità del documento al titolare della firma e conferisce piena efficacia ai documenti informatici e alle loro copie.

D) **Firma digitale**: "*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*" (art. 1, comma 1, s).
Il sistema prevede una doppia chiave asimmetrica necessaria alla cifratura e la decifratura del documento. La correlazione e l'uso simbiotico delle chiavi assicura l'autenticità, l'integrità e la segretezza del documento. In particolar modo:
la **chiave privata** è l'elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto soltanto dal titolare; serve ad apporre la firma sul documento, o per decifrare un documento in precedenza cifrato mediante la corrispondente chiave pubblica;
la **chiave pubblica** è invece l'elemento della coppia di chiavi asimmetriche, destinato a essere reso pubblico, usato per verificare la firma apposta sul documento dal titolare delle chiavi asimmetriche, o per cifrare i documenti da trasmettere al titolare delle chiavi.
Dal punto di vista probatorio, il mero dato legislativo attribuisce a questa firma il medesimo valore probatorio delle firme avanzata e qualificata.

Infine, va ricordato che il **D.P.C.M. del 22/02/2013**, recante le *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e* digitali, ha previsto diverse tipologie di chiavi, quali:
•**chiavi di sottoscrizione**, destinate alla generazione e verifica della firma elettronica qualificata o della firma digitale apposta o associata ai documenti;
•**chiavi di certificazione**, utilizzabili per la generazione e verifica delle firme apposte o associate ai certificati qualificati, per la sottoscrizione delle informazioni sullo stato di validità dei certificati, per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
•**chiavi di marcatura temporale**, destinate alla generazione e verifica delle marche temporali;
•**chiavi dedicate alla sottoscrizione delle informazioni sullo stato di validità dei certificati**.
Questo complesso sistema di strumenti di validazione è volto a garantire l'assoluta riferibilità della firma digitale a colui che ne è il titolare e che dovrà custodirne il dispositivo con diligenza, per evitare furti, smarrimenti o anche solo danneggiamenti affinché si possa essere certi che il documento informatico sia da lui firmato e non contenga alterazioni.

Il certificatore.
Un ruolo fondamentale in tema di firme elettroniche è ricoperto dal certificatore, il "*soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime*" (art. 1, comma 1, g). Si tratta cioè del soggetto che rilasciando i certificati di firma digitale, garantisce la sicurezza delle firme stesse, della corrispondenza biunivoca dispositivo di firma/identità del titolare.
Al fine di garantire l'identità dei soggetti che si servono di uno strumento di validazione digitale e di fornire la massima protezione dai possibili danni derivanti da un esercizio non adeguato delle attività di certificazione, le norme vigenti richiedono che il certificatore sia un soggetto in possesso di particolari requisiti tecnici, organizzativi e societari, ampiamente specificati sia dall'art. 26 che dall'art. 27 del CAD (onorabilità, professionalità e anche quelli prevista dal TUB). Qualora il certificatore venga meno o non compia le proprie attività con assoluta diligenza, viene meno la certezza che vi sia la corrispondenza tra il dispositivo di firma e il titolare del dispositivo stesso.
Inoltre, lo stesso CNIPA, con le *Linee guida per la vigilanza sui certificatori qualificati* pubblicate il 10 settembre 2008, ha definito una serie di regole finalizzate ad assicurare il massimo controllo sull'attività svolta dai certificatori.
Più in particolare, questo documento delinea gli obblighi e le responsabilità di tale categoria di professionisti secondo quanto disposto dagli articoli 30, 31 e 32 del CAD.
I compiti del certificatore possono essere così sintetizzati:
1) garantire l'univoca associazione tra la firma digitale e il titolare/sottoscrittore, al fine di assicurare a quest'ultimo l'incontestabile paternità dei documenti informatici sottoscritti;
2) provvedere alla pubblicazione *on-line* dell'elenco dei certificati relativi alle chiavi pubbliche dei titolari che si sono avvalsi delle loro attività di certificazione,
3) ha la responsabilità di mantenere aggiornato l'elenco pubblico dei certificati sospesi o revocati.

Il certificato elettronico.
La sicurezza del dispositivo di firma digitale è garantita dal certificato elettronico che viene rilasciato dal certificatore qualificato per ciascuna coppia di chiavi crittografiche.
Tale certificato costituisce essenzialmente un attestato informatico avente lo scopo di collegare i dati, utilizzati per verificare le firme elettroniche, ai rispettivi titolari, confermando l'identità informatica del soggetto firmatario.
A tal fine, l'art. 28, comma 1, CAD elenca i requisiti minimi del certificato elettronico:
a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;

d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;
e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica e che sono corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica del certificatore che ha rilasciato il certificato, conforme alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.