COS'E' LA FIRMA DIGITALE

La firma digitale è **l'equivalente informatico di una tradizionale firma apposta su carta**.

La sua funzione è quella di attestare la validità, la veridicità e la paternità di un documento, come una lettera, un atto, un messaggio o, in generale, qualunque file di dati (testo, immagini, musica, ecc.). Come tale, non va confusa con altri oggetti omofoni definiti genericamente "elettronici", come ad esempio la firma autografa scannerizzata e conservata come immagine. La firma digitale è infatti il risultato di una procedura informatica basata su un sistema di codifica crittografica a chiavi asimmetriche (una pubblica e una privata), che consente:

- la sottoscrizione di un documento informatico
- la verifica, da parte dei destinatari, dell'identità del soggetto firmatario
- la sicurezza della provenienza del documento
- la certezza che l'informazione contenuta nel documento non sia stata alterata

La **firma digitale** può essere apposta su qualunque documento informatico. Alcuni esempi di casi d'uso:

- bilanci e atti societari
- fatture elettroniche
- notificazioni al Garante della Privacy
- iscrizione al registro dei revisori contabili
- comunicazioni degli operatori finanziari con l'Agenzia delle Entrate
- richiesta di pareri al CNIPA

I **requisiti necessari** per richiedere un dispositivo di firma digitale sono:

- aver compito 18 anni
- essere in possesso del codice fiscale
- essere in possesso di un documento di identità in corso di validità

Il **certificato di sottoscrizione** è presente all'interno del dispositivo di firma. Esso è un insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica. Nel certificato compaiono altre informazioni tra cui il Certificatore che lo ha emesso, il periodo di tempo in cui il certificato può essere utilizzato, ecc. Lo scopo di questo certificato è di dare il valore della "forma scritta" ai documenti informatici.

Il **certificato di autenticazione** può essere presente all'interno del dispositivo di firma. Nel certificato compaiono altre informazioni tra cui il Certificatore che lo ha emesso, il periodo di tempo in cui il certificato può essere utilizzato, ecc. Lo scopo di questo certificato è quello di firmare messaggi di posta elettronica (garanzia dell'identità del mittente); può anche essere usato per accedere a siti web (al posto di user/password). A questo certificato, al momento del rilascio, viene associato un

indirizzo di posta elettronica in modo univoco, quindi il certificato potrà essere usato solo con quell'indirizzo.

La **marcatura temporale** di un documento informatico consiste nella generazione, da parte di una terza parte fidata, di una firma digitale del documento (anche aggiuntiva rispetto a quella del sottoscrittore) cui è associata l'informazione relativa ad una data e ad un'ora certa. La marcatura temporale consente quindi di stabilire l'esistenza di un documento informatico a partire da un certo istante temporale e di opporlo a terzi. Il tempo, cui fanno riferimento le marche temporali è riferito al Tempo Universale Coordinato, ed è assicurato da un ricevitore radio sintonizzato con il segnale emesso dall'Istituto Elettrotecnico Nazionale Galileo Ferraris.