IMPLEMENTAZIONI PRATICHE DI FIRMA ELETTRONICA

Definizioni legali delle diverse tipologie di firma elettronica:

- La **firma elettronica semplice** è per la Legge Italiana "*un insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*": è quindi la forma più debole di firma in ambito informatico, in quanto non prevede meccanismi di autenticazione del firmatario o di integrità del dato firmato.
- La **firma elettronica qualificata** è definita invece come una "*firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma*": è quindi un tipo di firma sicura.
- La **firma digitale** è "*un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata (crittografia asimmetrica), 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*": questa norma introduce l'uso di algoritmi di crittografia a chiave pubblica.

Tecnica e pratica della Firma Digitale:

Per firmare digitalmente un documento occorre un algoritmo software che produca una coppia di chiavi asimmetriche: quella privata resta nelle mani dell'autore del documento, mentre quella pubblica andrà allegata al documento firmato.
Si prenda un documento che si voglia firmare: da esso mediante una funzione Hash pubblica se ne ricava l'impronta digitale detta anche message digest. Questa impronta è costituita da un numero di 128 o più bit e rappresenta una sorta di *riassunto* del documento ed ha le seguenti caratteristiche: documenti diversi hanno message digest diversi, la modifica del documento comporta la modifica del message digest. La funzione Hash è a senso unico: cioè è semplice calcolarla nella forma diretta ma è quasi impossibile ricavarne a ritroso il documento calcolato con essa.
Una volta espletata la funzione Hash, il message digest viene crittografato con la chiave privata del mittente. Egli forma quindi un plico costituito dal documento originale, dal message digest crittografato e dalla chiave pubblica corrispondente. A questo punto il documento è stato firmato digitalmente e viene recapitato al destinatario.
Questi apre il plico, ne estrae il message digest e lo decifra con la chiave pubblica allegata. Quindi prende la funzione Hash pubblica e ricalcola l'Hash del documento ricevuto. Se il numero di 128 bit così ottenuto è uguale a quello decifrato con la chiave pubblica del plico è certo che il documento è stato prodotto dal mittente, non è stato modificato da nessuno ed il mittente, unico possessore della chiave privata, non può negare di averlo prodotto. Questa firma digitale ha la stessa validità legale della firma autografa.

Kit commerciali:

- In commercio vi sono alcuni Kit di firma digitale che comprendono: un lettore da collegare al PC o dispositivo analogo, il software, il certificato di firma elettronica e il certificato di autenticazione per la **Carta Nazionale dei Servizi** (CNS). Mediante la carta nazionale dei servizi il suo titolare può collegarsi a qualunque sito della Pubblica Amministrazione per ottenere le informazioni a lui relative e per interagirvi.
- Vi è poi la **Firma Digitale Remota**, che consente di apporre la firma senza la necessità di ricorrere all'installazione di hardware o software su PC, Tablet o Smartphone. Il Kit di Firma Remo-

ta è composto da un certificato di firma digitale residente su un server sicuro HSM, "Hardware Security Module" ed un dispositivo OTP, One Time Password, che permette al titolare di autenticarsi con le proprie credenziali e di firmare così i propri documenti da qualsiasi postazione connessa a Internet.

❖ Incidentalmente citiamo un altro kit che permette di assegnare, con forza di valore legale, data ed ora ad un documento: è il kit di **Marca Temporale**, un servizio analogo a quello di firma digitale.

Dr. Silvio Coccaro
ex allievo A. S. 1972/73