



LA CRITTOGRAFIA

La Firma Digitale si basa sulla crittografia a chiavi pubbliche o asimmetriche. E', sostanzialmente, un meccanismo di cifratura che prevede due chiavi una pubblica ed una privata (segreta). Applicando la chiave pubblica ad un documento informatico si ottiene un messaggio cifrato che può essere decifrato solo con la chiave privata corrispondente.

In breve...

Argomento
Firma digitale

In questo modo si può inviare telematicamente un documento essendo certi che solo il destinatario potrà leggerlo perchè l'unico in possesso della chiave privata (unica e segreta) corrispondente al quella pubblica con si è eseguita la crittografia.

LA FIRMA DIGITALE

La firma digitale se viene applicata ad un documento informatico gli conferisce piena validità giuridica. Questo avviene perchè, se si cifra un documento con la chiave privata, si potrà essere leggerlo solo dopo averlo riportato in chiaro con la corrispondente chiave pubblica. La decifrazione corretta, automaticamente, conferisce al documento il carattere di AUTENTICITA' del sottoscrittore in quanto unico possessore della chiave privata con cui si è eseguita la cifratura. Applicando la marcatura temporale nel meccanismo di firma si è anche certi della data e quindi il documento NON E' RIPUDIABILE (un contratto stipulato in questo modo è legalmente valido). Per poter applicare correntemente la firma digitale occorre un sistema che garantisca: SICUREZZA e PUBBLICITA' DELLA CHIAVE PUBBLICA.

LA SICUREZZA

Il funzionamento della Firma Digitale si basa sulla CERTEZZA che le chiavi private non possano essere carpite indebitamente da nessuno e che, pertanto, siano in possesso soltanto dei legittimi proprietari. Per questo motivo la legge impone regole da seguire per conservare la smart card ed i certificati di revoca se viene smarrita. Algoritmi di cifratura di provata efficienza e con un numero elevato di bit (1024) rendono la vita dura a coloro che intendono risalire alla chiave con mezzi non leciti. Si stima che per FORZARE la chiave privata con un algoritmo a 1024 bit bisogna impiegare simultaneamente circa 130000 PC per 4096 anni. Il meccanismo di firma, in effetti, basandosi su algoritmi così potenti non può essere applicato direttamente ad un documento per cui occorre passare per uno step intermedio: la funzione di hash.

LA FUNZIONE DI HASH

La funzione di hash è anch'essa un algoritmo con la quale è possibile ottenere dai documenti delle IMPRONTE DIGITALI con la caratteristica di essere tutte della stessa grandezza in bit. In sostanza, applicando la funzione di hash ad un documento si ottiene una impronta digitale dello stesso di dimensione ridotta e costante su cui si può applicare validamente la firma digitale. Si definiscono impronte digitali perchè gli algoritmi della funzione di hash anch'essi, rigidamente imposti dalle leggi, hanno una caratteristica specifica: non è assolutamente possibile ottenere da documenti diversi, DIGEST (le impronte appunto) uguali. Variando un file anche di un solo bit (per esempio aggiungendo uno spazio ad una lettera scritta con un word processor) l'impronta di questo nuovo documento è totalmente differente da quella del documento originario.

LO SCAMBIO

Nel meccanismo della Firma Digitale può intromettersi il solito furfante. Infatti, Il sign. X potrebbe inviare a MARCO un messaggio cifrato con la sua chiave privata (quella del signor X per essere chiari) facendo credere di essere Anna. Questo impostore, inviando anche la chiave pubblica con cui decifrare il messaggio potrebbe abusare dello scambio di identità e frodare Marco.

il CERTIFICATO

L'unico modo per impedire ai furfanti il giochino dello scambio di identità è il CERTIFICATO. Nel certificato vengono indicati i dati identificativi delle persone fisiche e/o giuridiche con la corrispondente chiave pubblica. Così se Marco riceve un messaggio in cui il Sign. X dice di essere Anna, basta che vada a vedere il certificato di Anna e leggere la chiave pubblica. Verificando la corrispondenza fra la chiave pubblica del certificato e quella inviata dal sign. X, il bravo Marco è in grado di tutelarsi da ogni frode. E' necesario, però, che il certificato sia immediatamente a disposizione di Marco e per questo motivo i certificati vengono pubblicati on line da apposite Società. Le Società di Certificazione sono molto importanti perchè assicurano la pubblica' e certificano l'identita' dei soggetti associando opportunamente: chiave pubblica-identita' soggettiva.

LE SOCIETA' DI CERTIFICAZIONE

Nel sistema di funzionamento della firma digitale le società di certificazione assumono un ruolo fondamentale. Esse assicurano curando l'emissione certificati la necessaria pubblicità della chiave pubblica (è indispensabile la divulgazione massima delle chiavi pubbliche) e attribuiscono all'evidenza informatica del possessore della chiave la sua identità giuridica. Compito, quest'ultimo, di fondamentale importanza perchè i soggetti di diritto nel nostro ordinamento sono le persone fisiche e giuridiche. Vincoli strettissimi per la nascita e l'operatività delle Società di Certificazione sono dettati dal DPCM 8/2/99, proprio per l'importanza che esse assumono nel Sistema Public Key Infrastructure.

LA PUBLIC KEY INFRASTRUCTURE

La Public Key Infrastructure non è altro che un sistema in cui apposite Società certificano l'identità dei soggetti associando loro la chiave pubblica, assicurano la pubblicità massima della stessa e pubblicano altresì i certificati di revoca per impedire, a chi entrando in possesso con frode, dolo o altro della chiave privata di un'altro soggetto, di compiere frodi. Data la loro importanza la legge italiana impone rigide condizioni di sicurezza per il loro funzionamento e solo dopo che L'A.I.P.A. le ha verificate iscrive le Società nell'elenco dei certificatori permettendo loro di operare. Ciò solleva problemi di armonizzazione con l'Unione Europea che è molto meno garantista e vieta l'autorizzazione preventiva per l'esercizio di attività di certificazione.