Firma Digitale

dott. Andrea Mazzini

acs s.r.l.

SISTEMI INFORMATICI
SOLUZIONI SOFTWARE

La Crittografia

La prima persona che usò la crittografia fu Giulio Cesare! Egli doveva inviare messaggi ma non si fidava dei messaggeri, così inventò un metodo per codificare quei messaggi. Solo il destinatario prestabilito conosceva il metodo per decodificare il messaggio e quindi poteva leggerli. La crittografia è quindi l'arte che crea ed usa i sistemi di crittografia. Un sistema di crittografia è un metodo per rendere illeggibili i messaggi, in modo da renderli decodificabili solo dal destinatario prestabilito. I sistemi di crittografia sono chiamati anche sistemi di cifratura. Il messaggio originale è chiamato testo in chiaro, ed il messaggio codificato è chiamato testo cifrato. Per codificare un messaggio, si una procedura che lo converte in testo cifrato. Questa procedura è chiamata cifratura. Viceversa, per rendere leggibile un messaggio, si usa il procedimento opposto, chiamato decifratura.

La Firma Digitale

- La **firma digitale** è **l'equivalente elettronico** della firma autografa, ed ha il suo stesso valore legale.

- Associata ad un documento elettronico ne garantisce l'integrità, l'autenticità la paternità e la non ripudiabilità.

Il Certificato di Sottoscrizione

- L'elemento chiave di un sistema di firma è rappresentato dal **certificato digitale di sottoscrizione** che i Certificatori accreditati presso il CNIPA (Centro Nazionale per Informatica nella Pubblica Amministrazione), rilasciano al titolare di una smart card.

Il Certificato di Sottoscrizione

- Il certificato di sottoscrizione è un file che contiene al suo interno informazioni che riguardano l'identità del titolare, la chiave pubblica attribuitagli al momento del rilascio, il periodo di validità del certificato stesso oltre ai dati del certificatore accreditato che lo ha rilasciato.

Il Certificato di Sottoscrizione

- **Il certificato digitale** di un titolare, una volta entrato a far parte dell'elenco pubblico dei certificati, tenuto dal certificatore accreditato, **garantisce la corrispondenza tra la chiave pubblica e l'identità del titolare** permettendo, a chi riceve un file firmato digitalmente, di verificare la validità del certificato stesso e di ottenere informazioni sul firmatario del documento informatico.

Il documento firmato digitalmente

- **Integrità**: garanzia che il documento non è stato manomesso dopo la sottoscrizione.
- **Autenticità**: garanzia dell'identità di chi firma.
- **Paternità**: riferibilità dell'autore firmante al documento.
- **Non ripudiabilità**: 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.

Come funziona

Per firmare un documento elettronico è necessario essere dotati di un Kit per Firma Digitale composto da:

1. Dispositivo di generazione delle firme (smart card)

2. lettore di smart card

3. software di firma e verifica

Come funziona

- Attraverso il software di firma sarà possibile scegliere il certificato con il quale si intende firmare e selezionare il documento elettronico da sottoporre a firma digitale.

- La scelta del certificato si rende necessaria in quanto ogni dispositivo può contenere più certificati rilasciati, al medesimo titolare, per scopi diversi.

Come funziona

- Al momento della firma del documento, il software chiederà l'inserimento del codice di protezione del dispositivo (PIN) e procederà con la creazione del file firmato digitalmente.

- Il file firmato assumerà l'estensione .p7m che si sommerà all'estensione del file originario (ad es. un documento .pdf, diventerà un file .pdf.p7m che rappresenta la **busta informatica PKCS#7**).

La Busta Informatica

La busta incorpora al suo interno il documento originario, il certificato del sottoscrittore, un hash del documento firmato con il certificato del sottoscrittore (funzione operante in un solo senso, non può essere invertita, atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta *valore di hash*, *checksum crittografico* o *message digest*).

La Busta Informatica

Tali componenti consentiranno, in fase di verifica della firma da parte del destinatario del documento firmato, di accertare che:

- il documento non sia stato modificato dopo la firma
- il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori
- il certificato del sottoscrittore non sia scaduto
- il certificato del sottoscrittore non sia stato sospeso o revocato

La Busta Informatica

Se tutte le verifiche daranno esito positivo, il documento sottoscritto digitalmente potrà essere considerato valido a tutti gli effetti di legge.