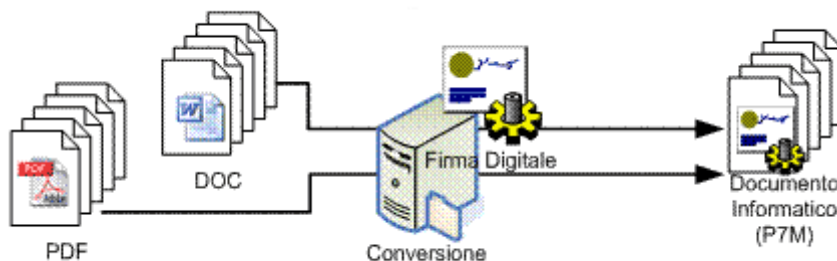


Cosa e' la Firma Digitale

La firma digitale, all'atto pratico, ha ben poco da spartire con la firma a cui siamo abituati. Il segno grafico che apponiamo in calce al testo, riconosciuto da sempre come indiscutibile prova della originalità del documento, ha un sapore romantico se confrontato con il processo di apposizione di una firma digitale. La prima e più importante differenza nell'uso dei due metodi è che il documento firmato con la penna resta perfettamente leggibile, mentre quello firmato digitalmente cambia il suo stato, la sua forma, e richiede un programma specializzato per la sua apertura.

La firma digitale è un processo matematico che permette di criptare una rappresentazione univoca del file, detta 'impronta', e di inserirla nel file stesso trasformandolo in un nuovo tipo di file. Questa in particolare è la caratteristica che va ben compresa: il risultato del processo di firma digitale di un file è un altro file, di formato diverso. Ad esempio il file in formato Microsoft Word 'Documento.doc', al termine del processo di firma diventa il file 'Documento.doc.p7m'. L'estensione 'p7m' indica che il file non è più un documento Microsoft Word e quindi non può più essere aperto da questo programma. Per poterlo leggere è necessario l'uso di un nuovo programma, facilmente reperibile su internet, prodotto da vari autori. Questo programma ha lo scopo di estrarre nuovamente il file originale e di confermare l'autenticità dell'autore del documento.



Attenzione quindi: il file firmato digitalmente non può essere letto con i sistemi oggi comunemente diffusi. Se, ad esempio, decidiamo di adottare il formato Portable Document Format (PDF) per pubblicare ed inviare i nostri documenti è perché si tratta di un formato ormai capillarmente diffuso che garantisce la leggibilità del documento presso il destinatario. In altre parole non dobbiamo preoccuparci di accordarci con lui per essere certi che sarà in grado di leggere il nostro file. Ma il file firmato non è più in formato PDF, è in formato 'p7m', uno standard in effetti, ma ancora poco diffuso. Molti destinatari del nostro documento non sapranno come aprire il file e saranno costretti a procurarsi un prodotto che sia in grado di farlo. Va detto che lo scopo di questa trasformazione non è nascondere il contenuto del file, tutt'altro: chiunque potrà aprire ed estrarre il file originale ed infine consultarlo, ma il nuovo formato è una necessaria trasformazione per aggiungere le informazioni che garantiscono l'originalità del file e la sua provenienza.

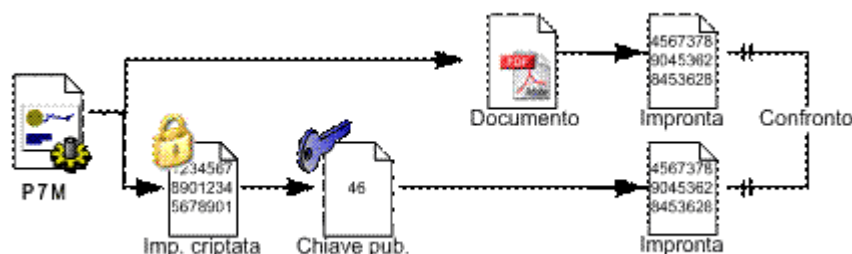
Come abbiamo visto la firma digitale è un processo matematico che può essere così sintetizzato.

- a. Creazione dell'impronta del documento: attraverso un algoritmo detto 'algoritmo di Hash' (Secure Hash Algorithm, SHA-1) è possibile estrarre un numero di lunghezza fissa (160 bit) che ha la caratteristica di rappresentare univocamente il nostro documento. Se cambiamo anche una sola virgola al documento anche il numero che lo rappresenta cambierà. Questo numero è detto 'impronta' del file. Le due caratteristiche importanti sono 1) l'impronta rappresenta il file, se il file cambia l'impronta cambia 2) è un numero.
- b. Firma dell'impronta: un altro algoritmo matematico permette di criptare l'impronta (che è un numero) con un altro numero, la chiave privata. Questa operazione è molto semplice da effettuare, ma è computazionalmente molto difficile effettuare l'operazione inversa, cioè ricavare la chiave privata. L'impronta così criptata è sicura e non può essere alterata. La chiave privata viene creata sempre in coppia con un altro numero, la chiave pubblica. Quest'ultima permette di estrarre l'impronta criptata, ma non di criptarla.
- c. Creazione del nuovo formato di file. Questa operazione può essere immaginata come la creazione di una sorta di busta all'interno della quale trovano posto 1) il file originale 2) l'impronta firmata 3) la chiave pubblica 4) il certificato dell'autore. Quest'ultimo è una vera e propria carta d'identità elettronica e viene rilasciata da una autorità preposta.



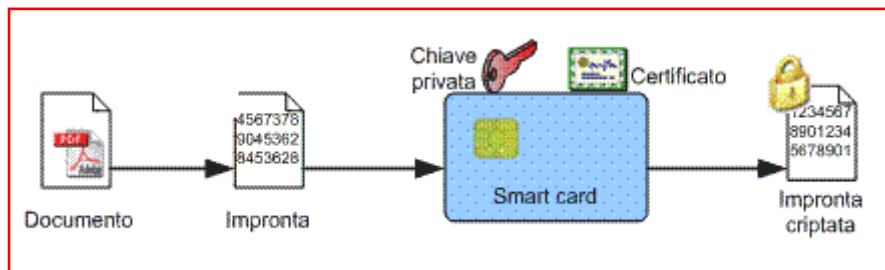
Vediamo ora cosa deve fare il destinatario per sapere se il file è originale o se è stato manomesso. Il principio consiste nell'estrarre il file originale e creare una nuova impronta che poi confronteremo con quella criptata contenuta nella busta: se le due impronte coincidono il file è intonso. In sintesi:

- Estrazione del file originale dalla busta.
- Creazione di una impronta attraverso l'applicazione dell'algoritmo SHA-1.
- Estrazione dell'impronta criptata con la chiave pubblica, anch'essa contenuta nella busta.
- Confronto delle due impronte.



Queste operazioni vengono svolte da programmi specializzati per la firma e la verifica dei documenti che vengono distribuiti gratuitamente su internet dalle stesse autorità che rilasciano i certificati e le chiavi private e pubbliche per la firma digitale. Attenzione non è necessario dotarsi degli strumenti per la firma digitale per leggere un file firmato. Il file può essere aperto scaricando l'apposito programma da internet.

Ma chi garantisce l'invulnerabilità dei certificati e della chiave privata? Le autorità di cui abbiamo parlato, preposte al rilascio dei certificati per firma digitale, installano questi ultimi su supporti che non possono essere contraffatti o alterati. Questi supporti sono smart card o token USB. L'operazione di criptaggio dell'impronta, la firma digitale, avviene a bordo di questi supporti: il programma dopo aver estratto l'impronta la invia al supporto che applica la chiave privata e restituisce l'impronta firmata. Il supporto si comporta come una cassaforte intelligente, che non permette l'uscita dei suoi valori, ma è in grado di operare al suo interno.



Come ottenerla

Per poter firmare digitalmente è necessario procurarsi il certificato d'identità. Tale certificato viene rilasciato su smart card o token USB da alcune autorità. L'elenco dei certicatori attivi alla data di pubblicazione dell'articolo è riportato in calce. L'elenco aggiornato è sul sito del CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) all'indirizzo: www.cnipa.gov.it...

Il costo è generalmente modesto se non addirittura gratuito. Istruzioni dettagliate sono facilmente reperibili sui siti delle autorità. In generale è necessario presentarsi agli sportelli muniti di carta d'identità e codice fiscale. Dopo alcuni giorni riceverete la vostra smart card ed il kit per utilizzarla.

Elenco certificatori attivi

Rag.Soc.: Infocamere S.p.A.
Indirizzo Internet: <http://www.card.infocamere.it>
Manuale operativo: <http://www.card.infocamere.it/firma/cps/cps.htm>
Man. oper. sottoscritto dal Presidente CNIPA: Infocamere_MO_v2.12.pdf.p7m

Rag.Soc.: Postecom S.p.A.
Indirizzo Internet: <http://www.poste.it>
Manuale operativo: <http://www.poste.it>
Man. oper. sottoscritto dal Presidente CNIPA: Postecom_MO_v2.zip.p7m

Rag.Soc.: In.Te.S.A. S.p.A.
Indirizzo Internet: <http://e-trustcom.intesa.it>
Manuale operativo: <http://e-trustcom.intesa.it>
Man. oper. sottoscritto dal Presidente CNIPA: INTESA_MO_v05.pdf.p7m

Rag.Soc.: Trust Italia S.p.A.
Indirizzo Internet: <https://firmadigitale.trustitalia.it>
Manuale operativo: <https://firmadigitale.trustitalia.it>
Man. oper. sottoscritto dal Presidente CNIPA: Trustitalia_MO_v1.1.pdf.p7m

Rag.Soc.: Cedacri S.p.A. (già Cedacrinord S.p.A.)
Indirizzo Internet: <http://www.cedacricert.it>
Manuale operativo: <http://www.cedacricert.it>
Man. oper. sottoscritto dal Presidente CNIPA: Cedacri_MO_v8.pdf.p7m

Rag.Soc.: ACTALIS S.p.A.
Indirizzo Internet: <http://www.actalis.it>
Manuale operativo: <http://ca.actalis.it>
Man. oper. sottoscritto dal Presidente CNIPA: Actalis_MO_3.zip.p7m

Rag.Soc.: Consiglio Nazionale del Notariato
Indirizzo Internet: <http://ca.notariato.it>
Manuale operativo: <http://ca.notariato.it>
Man. oper. sottoscritto dal Presidente CNIPA: CNN_MO_v2.pdf.p7m

Rag.Soc.: Comando Trasmissioni e Informazioni Esercito (già Comando C4 - IEW)
Indirizzo Internet: <http://www.eicert.esercito.difesa.it>
Manuale operativo: <http://www.eicert.esercito.difesa.it>
Man. oper. sottoscritto dal Presidente CNIPA: C4IEW_MO_v1.pdf.p7m

Rag.Soc.: Consiglio Nazionale Forense
Indirizzo Internet: <http://ca.consiglionazionaleforense.it>
Manuale operativo: <http://ca.consiglionazionaleforense.it>
Man. oper. sottoscritto dal Presidente CNIPA: CNF_MO_v1.pdf.p7m

Rag.Soc.: SOGEI S.p.A.
Indirizzo Internet: <http://ca.sogei.it>
Manuale operativo: <http://ca.sogei.it>
Man. oper. sottoscritto dal Presidente CNIPA: Sogei_MO_v1.pdf.p7m

Rag.Soc.: Sanpaolo IMI S.p.A.
Indirizzo Internet: <http://ca.sanpaoloimi.com>
Manuale operativo: <http://ca.sanpaoloimi.com>

Man. oper. sottoscritto dal Presidente CNIPA: SanPaoloIMI_MO_v1.pdf.p7m

Rag.Soc.: Banca Monte dei Paschi di Siena S.p.A.

Indirizzo Internet: <http://www.mps.it>

Manuale operativo: <http://www.mps.it>

Man. oper. sottoscritto dal Pres. CNIPA: MontedeiPaschidiSiena_MO_v1.pdf.p7m

Rag.Soc.: Lombardia Integrata S.p.A. Servizi Infotelematici per il Territorio

Indirizzo Internet: <http://www.lisit.it>

Manuale operativo: <http://www.lisit.it/firmadigitale/documentazione>

Man. oper. sottoscritto dal Presidente CNIPA: Lisit_MO_v1.pdf.p7m

Rag.Soc.: Banca Intesa S.p.A.

Indirizzo Internet: <http://www.bancaintesa.it>

Manuale operativo: <http://www.bancaintesa.it>

Man. oper. sottoscritto dal Presidente CNIPA: BancaIntesa_MO_v2.pdf.p7m

Rag.Soc.: Banca di Roma S.p.A.

Indirizzo Internet: <http://www.bancaroma.it>

Manuale operativo: <http://www.bancaroma.it>

Man. oper. sottoscritto dal Presidente CNIPA: BancadiRoma_MO_v1.pdf.p7m

Rag.Soc.: CNIPA - Centro nazionale per l'informatica nella pubblica amministrazione (già Centro Tecnico per la RUPA)

Indirizzo Internet: <http://www.cnipa.gov.it>

Manuale operativo: <http://www.cnipa.gov.it>

Man. oper. sottoscritto dal Presidente CNIPA: Cnipa_MO_v2.pdf.p7m

Rag.Soc.: I.T. Telecom S.r.l.

Indirizzo Internet: <http://www.firmasicura.it>

Manuale operativo: <http://www.firmasicura.it>

Man. oper. sottoscritto dal Presidente CNIPA: ITTelecomSrL_MO_v1.01.pdf.p7m

Rag.Soc.: Consorzio Certicomm - "Autorità di certificazione dei Consigli Nazionali dei Ragionieri e dei Dottori Commercialisti"

Indirizzo Internet: <http://www.certicomm.it>

Manuale operativo: <http://www.certicomm.it>

Man. oper. sottoscritto dal Presidente CNIPA: Certicomm_MO_v1.1.pdf.p7m