La Firma Digitale

Manuale d’uso Fornitore - Introduzione alla Firma Digitale

Marzo 2016

Cenni generali sulla Firma Digitale

- La firma digitale può essere definita come un sistema di autenticazione di documenti digitali tale da garantire il cosiddetto "non ripudio" e al contempo l'integrità del documento stesso

- La firma digitale di un documento informatico si propone di soddisfare tre esigenze:

  › che il destinatario possa verificare l'identità del mittente (autenticità)

  › che il mittente non possa disconoscere un documento da lui firmato (non ripudio)

  › che il destinatario non possa creare o modificare un documento firmato da qualcun altro (integrità)

Caratteristiche della Firma Digitale

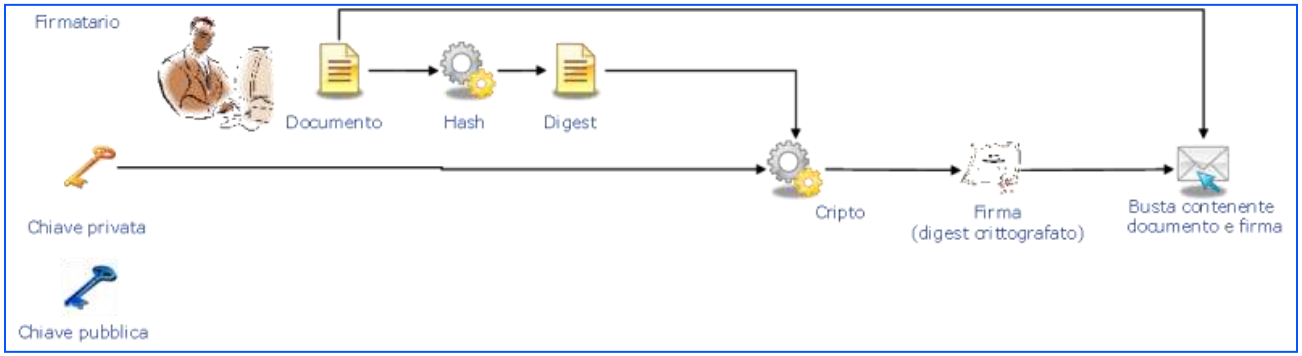
Per soddisfare le esigenze nell'utilizzo della firma digitale, è necessario che tale strumento:

- sia basato su un sistema di chiavi crittografate asimmetriche
- garantisca la riservatezza del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso di una "chiave" (intesa secondo la definizione crittologica) per interpretarli
- fornisca ad ogni utente una coppia di chiavi certificate: una chiave privata, da non svelare a nessuno, con cui può decifrare i messaggi che gli vengono inviati e firmare i messaggi che invia, e una chiave pubblica, che altri utenti utilizzano per cifrare i messaggi da inviargli e per decifrare la sua firma e stabilirne quindi l'autenticità
- adotti chiavi provenienti da un certificatore soggetto a vigilanza da parte di AgID (Agenzia per l'Italia digitale)
- sia creato mediante un dispositivo con elevate caratteristiche di sicurezza (smartcard/token USB)

Schema di funzionamento Firma Digitale

Processo di firma (utente A)

Nello schema di seguito riportato viene illustrato il percorso di firma di un documento da parte dell'utente A:

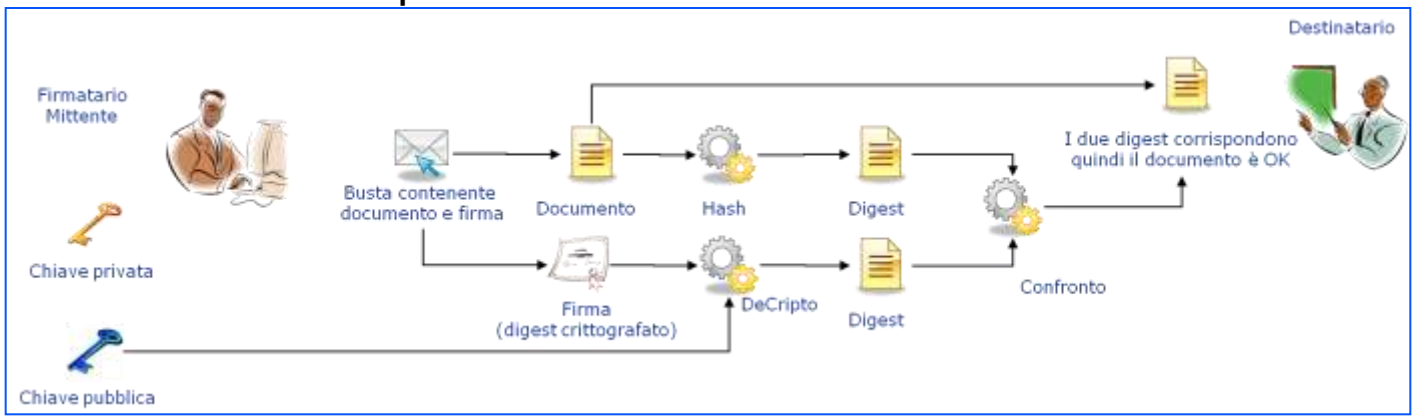


1. Il documento da firmare è sottoposto all'algoritmo di hash generando un digest che lo rappresenta univocamente
2. Il digest è quindi crittografato utilizzando la chiave privata del firmatario generando la firma
3. Infine documento e firma sono inseriti in una busta elettronica a costituire il documento firmato
4. La firma digitale è associata stabilmente al documento informatico e lo arricchisce d'informazioni che attestano con certezza l'integrità, l'autenticità e la non ripudiabilità dello stesso.
5. L'utente deve dotarsi in proprio di un apposito kit costituito da una smart card, da un lettore di smart card e da un software di firma. In alternativa alla smart card l'utente può utilizzare un token USB (chiavetta). Attraverso questi strumenti l'utente ha la possibilità di applicare la propria firma digitale e la marca temporale a qualsiasi documento

Schema di funzionamento Firma Digitale

Processo di verifica (utente B)

Nello schema di seguito riportato viene illustrato il percorso di verifica di un documento da parte dell'utente B:



1. Vengono estratti dalla busta il documento e la firma
2. La firma viene decrittata utilizzando la chiave pubblica del firmatario (utente A) ed estraendo il digest originale
3. Il documento viene sottoposto ad hash creando il digest attuale che viene confrontato con quello originale contenuto nella firma
4. Se i due digest coincidono il documento non è stato alterato ed è stato firmato certamente dal possessore della chiave privata che ha criptato la firma

Validità della Firma Digitale

- Il certificato del titolare ha un periodo di validità, ma può anche essere revocato o sospeso prima della naturale scadenza (es. sottrazione o smarrimento del dispositivo di firma, informazioni contenute nel certificato non più corrette)
- La revoca e la sospensione del certificato equivalgono a mancata sottoscrizione del documento
- La revoca è irrevocabile, la sospensione è una condizione transitoria del certificato che può evolvere in revoca o "annullamento della sospensione"
- Potrebbero nascere delle problematiche legate all'utilizzo di documenti sottoscritti con firma digitale il cui certificato è successivamente scaduto, revocato o sospeso
- In queste circostanze è fondamentale l'utilizzo del servizio di marcatura temporale per riuscire a collocare nel tempo, in modo opponibile ai terzi, l'esistenza della firma del documento in questione in modo da dimostrare che la stessa è stata prodotta in un momento in cui il relativo certificato era ancora valido

Formati documentali previsti per la Firma Digitale

Attualmente il nostro ordinamento prevede l'utilizzo di tre formati per produrre file firmati digitalmente:

- **P7M** -> previsto dalla normativa vigente sull'interoperabilità della firma digitale, è quello che le Pubbliche Amministrazioni sono obbligate ad accettare ed è disponibile fin dall'anno 1999.
- **PDF** -> introdotto nel 2006, rappresenta attualmente un formato standard la cui gestione in applicazioni sviluppate a tale scopo non obbliga al pagamento di "royalty" ad alcun soggetto. Caratterizzato da larga diffusione, immediata fruibilità (il software di lettura è scaricabile gratuitamente da Internet ed è di facile utilizzo) e rispondente ai requisiti tecnico e giuridici per poter trasportare firme digitali al suo interno.
- **XML** -> introdotto nel 2006 per incentivare la diffusione della firma digitale in settori come quello bancario e sanitario per la gestione elettronica dei rispettivi flussi documentali.

Riferimento alla legislazione italiana sul tema Firma Digitale

- In Italia è possibile realizzare documenti elettronici aventi valore legale corrispondente a documenti cartacei a firma autografa.

- Il quadro legislativo si è formato a partire dal 1977 con l'emissione dell'articolo 15 della L. 59/97 poi evoluto per recepimento della direttiva europea sulla firma elettronica (Direttiva 1999/93/CE) che ha portato all'emissione di vari emendamenti che hanno formato il quadro attuale.

- Una breve compendio del quadro normativo ed altre informazioni sono disponibili sul sito dell'Agenzia per l'Italia Digitale (AgID):

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche

- L'elenco dei soggetti autorizzati a rilasciare certificati di firma digitale è disponibile al seguente link:

http://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi