SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

SUAP On Line i pre-requsiti informatici:
La firma digitale

SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

La firma digitale

Indice

COMUNE DI NAPOLI

SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

La firma digitale

Cos'è

La Firma Digitale è il risultato di una procedura informatica (validazione) che garantisce **l'autenticità e l'integrità** di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti tradizionali.

Firma digitale ed autografa

La differenza tra firma autografa e firma digitale è che la prima è legata alla caratteristica fisica della persona che appone la firma, vale a dire la grafia, mentre la seconda al possesso di uno strumento informatico e di un PIN di abilitazione da parte del firmatario.

Si ricorre all' **autorità di certificazione** , il cui compito è quello di **stabilire, garantire e pubblicare** l'associazione tra un soggetto e le firme digitali da lui generate. Questa associazione viene formalizzata tramite un certificato elettronico.

COMUNE DI NAPOLI

SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

La firma digitale

Finalità della firma digitale

La firma digitale consente al sottoscrittore di rendere manifesta l'autenticità del documento informatico e al destinatario di verificarne la provenienza e l'integrità.

I suoi requisiti assolti sono:

- **Autenticità**: con un documento firmato digitalmente si può essere certi dell' identità del sottoscrittore

- **Integrità**: sicurezza che il documento informatico non è stato modificato dopo la sua sottoscrizione

- **Non ripudio**: il documento informatico sottoscritto con firma digitale ha piena validità legale e non può essere ripudiato dal sottoscrittore.

COMUNE DI NAPOLI

SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

La firma digitale

Come funziona

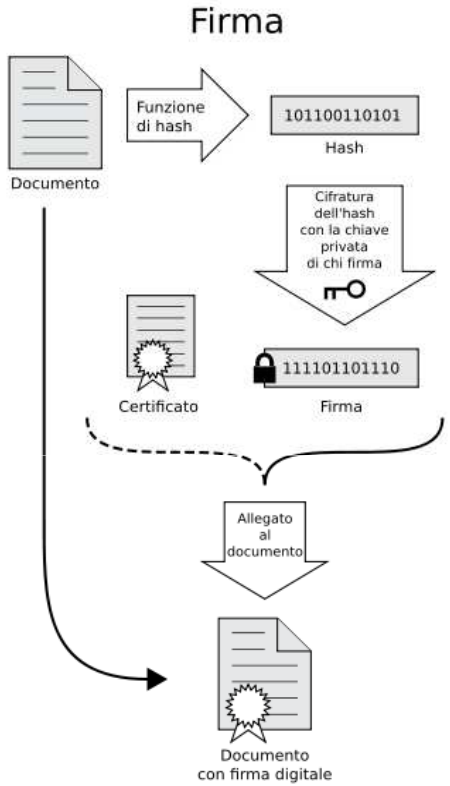
Per generare una firma digitale è necessario utilizzare una **coppia di chiavi digitali asimmetriche**, attribuite in maniera univoca ad un soggetto, detto **titolare** della coppia di chiavi:

la chiave privata, destinata ad essere conosciuta solo dal titolare, è utilizzata per la generazione della firma digitale da apporre al documento;

la chiave da rendere pubblica viene utilizzata per verificare l'autenticità della firma. Essa è contenuta nel certificato rilasciato dal gestore

Caratteristica di tale metodo, detto **crittografia a doppia chiave**, è che, una volta firmato il documento con la chiave privata, la firma può essere verificata con successo esclusivamente con la corrispondente chiave pubblica.

La firma digitale: firmatario



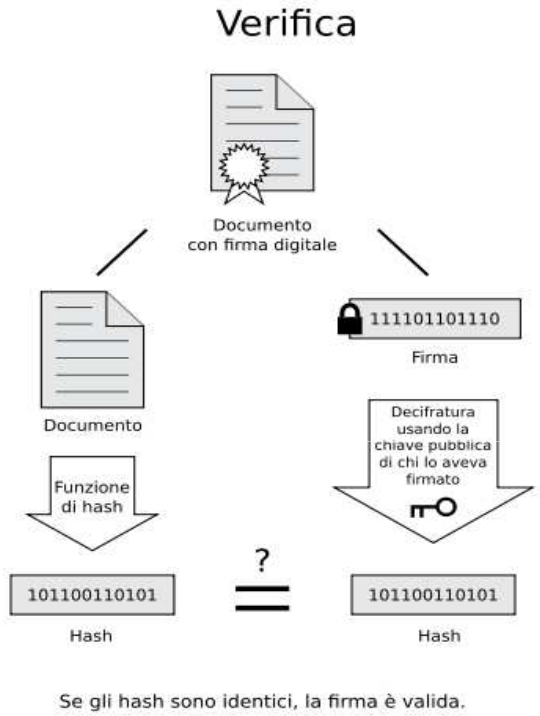
- Genera l'impronta **$hash_{mittente}$** del documento: una stringa binaria di lunghezza fissa ed univoca dello stesso.

- La legge italiana prevede l'algoritmo SHA-1 a 160 bit che ha una resistenza alle collisioni=10^{48} tentativi),

- **Firma il documento**, cioè crittografa con la sua **chiave privata** l'hash del documento,

- **Genera l'associazione documento – firma - certificato** emesso dalla Certification Authoriry secondo lo standard PKCS#7 dando vita alla **"busta elettronica".**

La firma digitale: destinatario



- Apre la busta elettronica, separa il documento in chiaro dalla firma e calcola l'hash del documento (applicando lo stesso algoritmo mittente) ottenendo **l'hash$_{destinatario}$**

- Utilizza la **chiave pubblica** del mittente, estratta dal certificato per **ottenere l'hash$_{mittente}$**,

- Confronta hash$_{mittente}$ con hash$_{destinatario}$: se l'esito è positivo, il messaggio **si deve ritenere, integro.**

SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

La firma digitale: destinatario

Garanzie della firma digitale

- L'associazione tra documento e firma autografa è ottenuta esclusivamente attraverso il supporto cartaceo;
- La firma digitale è invece legata al singolo documento elettronico a cui è apposta;
- A documenti elettronici diversi corrispondono firme digitali diverse;
- Non è possibile trasferire una firma digitale da un documento ad un altro
- **Autorità di certificazione**:
  - Soggetto pubblico o privato che identifica il titolare di dispositivo di firma digitale;
  - certifica la chiave pubblica appartenente al titolare rilasciando e pubblicando il certificato .
  - Pubblica ed aggiorna gli elenchi dei certificati sospesi e quelli dei certificati revocati

COMUNE DI NAPOLI

SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

La firma digitale: destinatario

Certificato

Un certificato è l'equivalente elettronico di un passaporto, di una patente o di una carta di identità. La funzione principale di un certificato consiste nel garantire la validità della chiave pubblica in esso contenuta. Un certificato stabilisce un legame tra l'identità di uno specifico individuo e la sua chiave pubblica.

Impronta (hash)

Sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di hash .

Funzione di hash

Funzione matematica che genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali

La firma digitale: destinatario

Busta crittografica

È la sequenza di bit che ingloba:

- il documento elettronico originale;
- la firma digitale;
- il certificato del sottoscrittore;

Permette a chi esegue la funzione di verifica di appurare senza alcun dubbio l'identità del sottoscrittore e l'integrità del documento .

Algoritmo RSA

Nella crittografica a chiave pubblica (o asimmetrica) si usano due chiavi crittografiche per ogni utente; una delle due chiavi (detta privata) viene conservata gelosamente dall'utente e mai rivelata a terzi, mentre l'altra (detta pubblica) deve essere resa nota; il più noto e diffuso sistema crittografico asimmetrico è il Rivest-Shamir-Adleman **(RSA)** ; un messaggio cifrato con la chiave privata può solo essere decifrato con la corrispondente chiave pubblica, e viceversa; non è possibile dalla conoscenza di una delle due determinare quale sia l'altra.

SUAP SPORTELLO UNICO ATTIVITÀ PRODUTTIVE
COMUNE DI NAPOLI

GRAZIE PER L'ATTENZIONE!