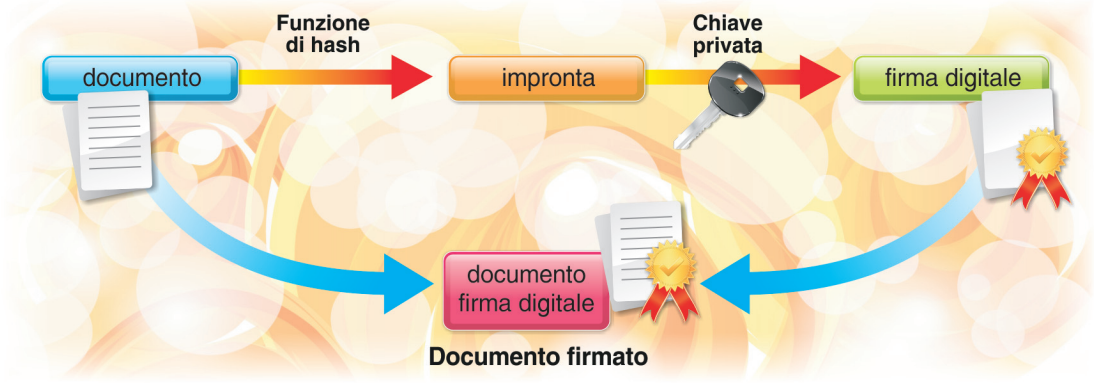
La firma digitale

La **firma digitale** è un metodo elettronico che permette a una persona di apporre un segno distintivo ai documenti digitali. I requisiti della firma digitale sono:

- **autenticità**, per garantire l'identità della persona che ha sottoscritto il documento;
- **integrità**, per essere sicuri che il documento non sia stato modificato dopo la sottoscrizione;
- **non ripudio**, cioè il documento sottoscritto con firma digitale ha piena validità legale e non può essere ripudiato dal sottoscrittore.

Quindi il documento elettronico è un messaggio che il mittente firma in modo digitale e spedisce al destinatario. Quest'ultimo, dopo aver ricevuto il messaggio, può verificare, controllando la firma digitale se il messaggio ha origine dal mittente e se è stato modificato durante la trasmissione. La firma digitale viene realizzata usando i sistemi di crittografia a chiave asimmetrica. In questo caso, il ruolo delle chiavi è diverso rispetto al loro utilizzo per la codifica dei messaggi destinati al possessore della chiave privata. Una persona firma un documento usando la sua chiave privata, mentre le altre persone, che vogliono controllare l'autenticità e l'integrità, usano la chiave pubblica.
A partire dal documento, viene generata un'**impronta** (*fingerprint*), cioè una sequenza binaria di lunghezza fissa (128 o 160 bit) che rappresenta un **digest** (riassunto) del documento. L'impronta viene generata usando una particolare funzione, chiamata **funzione di hash**, con la garanzia che a partire da documenti diversi si ottengono impronte diverse. Questa impronta viene poi codificata utilizzando la chiave privata e il risultato rappresenta la **firma digitale**.
La firma così costruita viene accodata al documento in chiaro.



Le fasi per controllare la veridicità del documento sono:

1. usare la chiave pubblica del firmatario per decifrare l'impronta;
2. avendo il testo in chiaro e usando la stessa funzione di *hash*, calcolare l'impronta del documento;
3. se le due impronte coincidono significa che il documento è stato firmato dalla giusta persona ed è integro, cioè non è stato modificato.

Dopo l'apposizione della firma digitale, ogni modifica al documento comporta una modifica nell'impronta associata. Avendo a disposizione l'impronta originale contenuta nella firma digitale, si può rapidamente controllare se il documento è stato modificato. Si osservi che la firma digitale è diversa per ogni documento diverso, a differenza della firma autografa. La firma digitale, per questo motivo, offre il valore aggiunto dell'integrità.

La coppia di chiavi pubblica e privata, usate per firmare e verificare i documenti, deve essere rilasciata da un **ente di certificazione** (*Certification Authority*) che garantisce l'identità del possessore della chiave.
La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica è indicata con il termine **titolare**.

Uno strumento pratico e sicuro per conservare la chiave privata è rappresentato dalle schede **smart card**, simili per forma e dimensioni a una tradizionale carta di credito e protette da PIN (*Personal Identification Number*) di accesso.
La smart card viene collegata al computer attraverso un apposito lettore ed è gestita con un software che consente di apporre la firma digitale ai documenti elettronici.

Il destinatario può avere la garanzia sull'identità del mittente e nello stesso tempo ottenere la sua chiave pubblica attraverso il **certificato digitale** emesso e firmato dall'ente certificatore.
Il certificato è redatto secondo uno standard riconosciuto (*formato X.509*) e contiene:

- numero di serie del certificato
- ragione e denominazione sociale del certificatore
- nome, cognome e data di nascita del titolare delle chiavi
- valore della chiave pubblica
- algoritmi di generazione e di verifica
- inizio e fine del periodo di validità delle chiavi.

Quindi, in pratica, il destinatario riceve una *busta elettronica* contenente il documento, la firma digitale e il certificato con la chiave pubblica.