ACCORGIMENTI

1. La cifratura dell'**hash del messaggio**, con la chiave privata del *mittente*, rappresenta la **firma del documento digitale**.

2. Si può aggiungere un algoritmo a chiave simmetrica, per la trasmissione del **messaggio firmato**, in modo da garantire anche la confidenzialità della comunicazione.

3. L'**hash del messaggio** ha lunghezza fissa (di solito minore del messaggio originale), per cui la sola cifratura dell'hash, anziché dell'intero messaggio, garantisce un vantaggio notevole in termini di **efficienza** per quanto riguarda la lunghezza della firma e la velocità di trasmissione.

4. C'è bisogno che un'**autorità certificata** (una terza parte fidata) generi la coppia di chiavi del mittente. L'autorità ha il compito di rilasciare le chiavi al mittente insieme ad un **certificato** che ne garantisca l'autenticità.

FIRME FISICHE vs FIRME DIGITALI

Per capire lo scopo delle firme digitali elenchiamo le caratteristiche che, in un mondo ideale, stanno alla base delle firme fisiche (firme a mano su carta).

Vorremmo che la firma fosse:

- **autentica**: la firma può essere ispezionata per capire se è stata realmente posta su un documento;
- **non falsificabile**: solo l'autore può generarla;
- **non riusabile**: una volta posta su un documento non può essere trasferita su un altro documento;
- **non modificabile**: i documenti firmati non devono poter essere modificati;
- **non ripudiabile**: il firmatario non può negare di aver firmato un documento se lo ha effettivamente fatto.

Le **firme digitali** si propongono proprio che tali caratteristiche siano sempre verificate.

RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/firme_digitali_tecnologia/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

LA FIRMA DIGITALE

Scopri cosa è la firma digitale e dai valenza legale ai tuoi documenti digitali.

PERCHÈ LE FIRME DIGITALI?

Con la crittografia si può garantire l'**autenticazione** e la **confidenzialità** di una comunicazione. Nelle applicazioni pratiche dobbiamo anche garantire l'autenticità del mittente, così che il destinatario possa fidarsi di lui (e viceversa).

Es. supponendo che **Bob** e **Mary** abbiano una chiave di comunicazione condivisa, se Bob invia un messaggio a Mary, si potrebbero verificare le seguenti dispute:

- Mary potrebbe inventarsi un messaggio e dire che glielo ha inviato Bob;
- Bob potrebbe negare di aver inviato un certo messaggio a Mary, sostenendo che Mary se lo sia inventato da sola.

L'idea è che quando firmo un documento, non posso negare di non averlo fatto.
Lo scopo di una **firma digitale** è dunque quello di fornire a un'entità un mezzo per legare la propria identità a un'informazione digitale.

PROPRIETÀ DELLE FIRME DIGITALI

Il processo di firma comporta la trasformazione del messaggio, e di alcune informazioni segrete detenute dall'entità, in un tag chiamato **firma**.

In maniera analoga a una firma fisica, la **firma digitale** consente di:

- verificare l'autore e la data della firma;
- autenticare il contenuto del messaggio;
- essere verificata da terze parti per risolvere eventuali controversie.

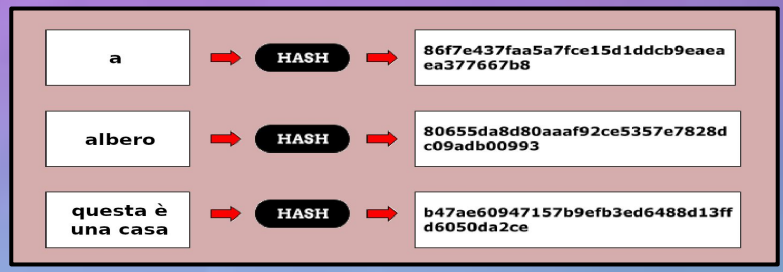
Una **firma digitale** deve:

- dipendere dal messaggio che si vuole trasmettere;
- deve usare delle informazioni specifiche del mittente;
- essere facile da produrre;
- essere facilmente riconoscibile e verificabile;
- essere impossibile da falsificabile.

FIRME DIGITALI CON FUNZIONI HASH

Tra gli approcci più comuni per realizzare **firme digitali** ci sono i metodi basati sulle **funzioni hash** e sugli algoritmi di crittografia a chiave pubblica.

Una funzione hash associa ad ogni possibile messaggio, un solo, ed unico, messaggio di lunghezza fissa (non devono esistere due messaggi diversi con lo stesso hash associato).



Per realizzare la firma, il *mittente* genera l'**hash del messaggio** e cifra quest'ultimo con la sua chiave privata.
Il *destinatario* riceverà il **messaggio** e l'**hash cifrato** che sarà in grado di decodificare con la chiave pubblica del *mittente*.
Il *destinatario* può quindi verificare l'autenticità del messaggio (e del *mittente*) generando l'**hash del messaggio** ricevuto e confrontandolo con l'**hash decodificato**.