

DIGITAL SIGNATURES - DIRETTA

La firma digitale assicura l'autenticità alle due parti, ma non li protegge da se stessi, cioè anche tra di loro ci sono delle possibili controversie, ad esempio, supponiamo che A invii un messaggio autenticato a B, possono comunque nascere queste controversie:

- B può forgiare un messaggio diverso ricevuto da A.
- A può disconoscere la paternità di un messaggio perché appunto B può forgiare finti messaggi, e non esiste modo per provare che A lo abbia realmente inviato.



Per questo motivo nasce la **DIGITAL SIGNATURES-ARBITRARIA**

Cioè per risolvere questo problema abbiamo bisogno di un terzo attore: ARBITRO

- Con la firma arbitraria con chiavi simmetriche, l'arbitro vede il messaggio o no, dipende dal protocollo
- Con la firma arbitraria con chiavi pubblica, l'arbitro non vede il messaggio

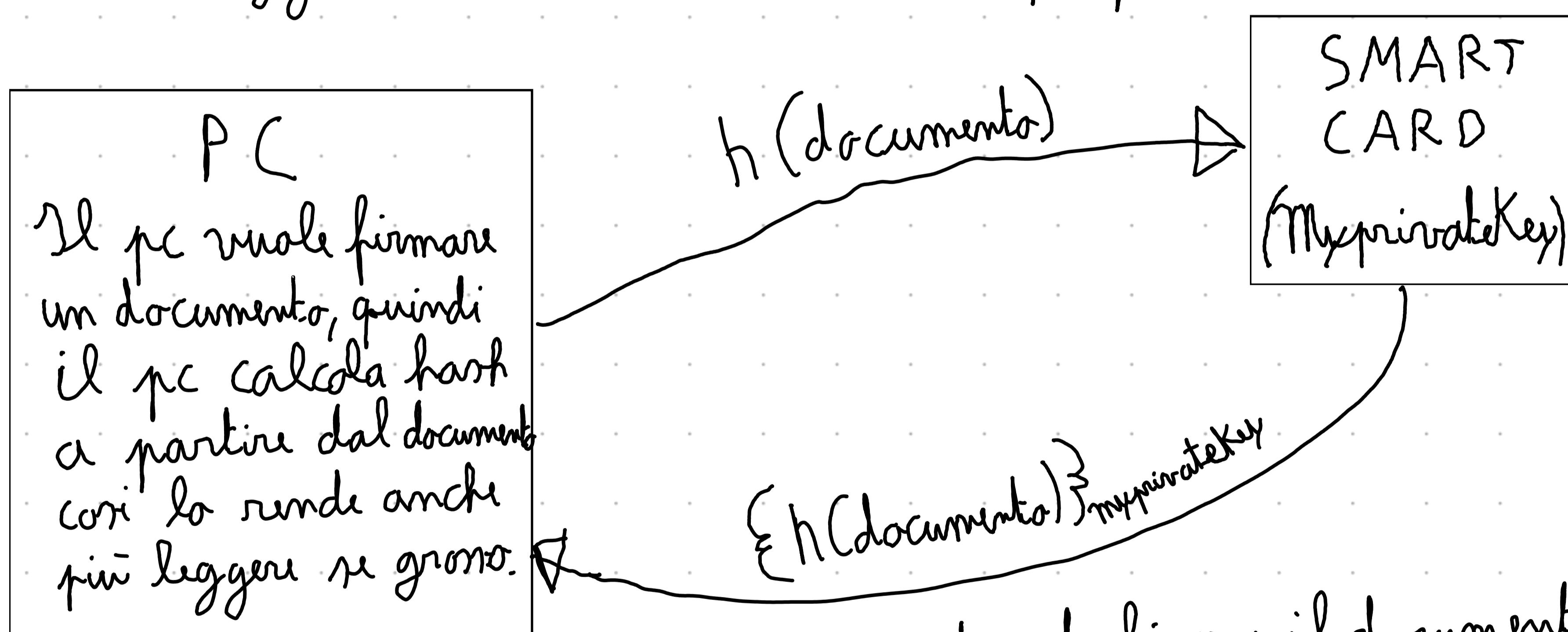
Il destinatario deve conoscere la chiave pubblica della fonte.

La firma è quindi formata:

- crittografando l'intero messaggio con la chiave privata del mittente.
- Cifrando il codice hash del hash del messaggio con la chiave privata del mittente.

la sicurezza della firma dipende dalla sicurezza della chiave privata del mittente.

Ogni messaggio firmato deve contenere una data, però bisogna comunque considerare se un avversario possiede la chiave privata può firmare un messaggio con una data di tempo prima.



La smartcard firma il documento, per farlo critta hash ricevuto con la sua chiave privata salvata dentro la SMARTCARD, la quale per nessun motivo deve abbandonare la SMARTCARD.

La SMARTCARD firma e non convalida la firma digitale, per convalidare la firma digitale serve la chiave pubblica.

- REQUISITI DI UNA FIRMA

- Fornire i mezzi per verificare l'autore, la data è l'ora della firma
- Autenticare il contenuto al momento della firma
- Deve essere verificabile da 3 parti, per risolvere la controversia
- Deve utilizzare alcune informazioni uniche per il mittente, per evitare sia la falsificazione che la negazione.
- Deve essere relativamente facile produrre, riconoscere e verificare la firma digitale.
- Deve essere computazionalmente impossibile forgiare una firma digitale fraudolenta per un dato messaggio.