Una chiave pubblica consiste in un **file** al quale sono collegati una serie di metadati contenenti informazioni come *nome*, *indirizzo mail*, ...

Queste informazioni, però, non garantiscono che la chiave effettivamente appartiene a quella persona. Vengono usate una serie di tecniche per associare un'indentità alla chiave

Informal method 1: Key Fingerprint

1. Alice calcola l'**hash** della sua chiave pubblica
2. Quando Bob vuole inviare un messaggio ad Alice usa la chiave pubblica di Alice
3. Bob controlla che l'hash della chiave pubblica di Alice sia uguale a quello che ha calcolato
4. Bob potrebbe interferire con il punto 2, sostituendo le chiavi, ma i due hash sarebbero diversi
5. Bob, confrontando le fingerprint, può notare se qualcosa è diverso

Questa tecnica risulta poco scalabile: non puoi ricevere le fingerprint di ogni sito che visiti. risulta molto comodo nello scambio di brevi messaggi.

Informal method 2: Key Servers

- Sono dei server nei quali un utente può caricare le chiavi pubblice assieme ai metadati collegati.
- Usano un protocollo di sincronizzazione per fare il mirror negli altri.
- Non garantiscono nulla, danno solamente la possibilità di caricare le chiavi

Informal method 3: Web of Trust

è una rete di fiducia nella quale i partecipanti certificano l'identità degli altri.

Public Key Infrastructure (PKI)

Consiste in un'infrastruttura tutti i componenti si fidano di un ente, chiamata **Certification Authority (CA)** (è in possesso di una chiave privata e della chiave pubblica conosciuta da tutti)

Se Alice e Bob non si fidano l'uno dell'altro, Alice può chiedere alla CA di firmare la sua chiave. Quando Bob la riceve, controlla che sia firmata dalla CA e in caso positivo, si fida di Alce.