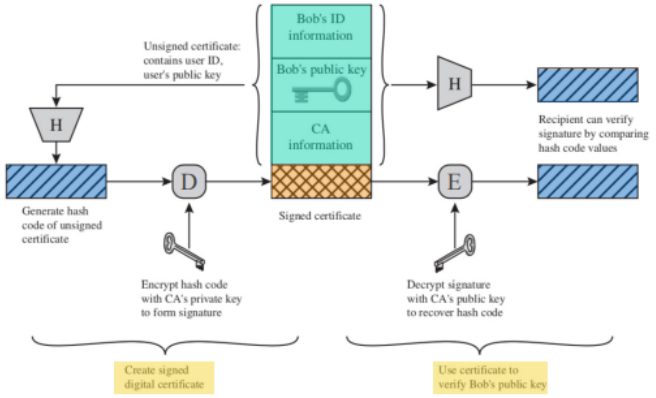
06 - Certificates, Certification Authorities and Public-Key Infrastructures

La firma (autografo) viene rimpiazzata nel modo digitale dal **certificato digitale** (come il covid-19 green pass).
L'uso di un certificato richiede che venga validato verificando che non sia scaduto e che la firma appartenga ad un entità considerata autorevole.

Nella crittografia asimmetrica un certificato digitale è il form in cui le chiavi pubbliche vengono comunicate.
é un **vincolo** tra **chiave pubblica** e **identità** di un soggetto.
é **firmato** da un pubblicatore fidato (CA: **certification authority**)



Qualsiasi partecipante è in grado di **leggere** un certificato e determinarne il nome e chiave pubblica del possessore del certificato.
Qualsiasi partecipante può **validare** un certificato per determinare che è originato da una public authority e non è stato contraffatto.
Solo le certification authority possono **creare** e **aggiornare** i certificati.

X.509 Certificati

X.509 è un standard che specifica certificati con i seguenti campi

```
Subject: Distinguished Name, Public Key
Issuer: Distinguished Name, Signature
Validity: Not Before Date, Not After Date
Administrative Info: Version, Serial Number
Extended Info:   …
```

Distinguished name fields come definiti nello standard:

```
Common Name              CN=Kenneth Lay
Organization or Company  O=Enron
Organizational Unit      OU=Management
City/Locality            L=Houston
State/Province           ST=Texas
Country (ISO Code)       C=US
```

Certification authority

Una certification authority (CA) è responsabile per la **certificazione**, **validazione** e **revoca** dei certificati.

Public key infrastructure

La collezione di hardware, software, persone, politiche e protocolli necessari a creare, gestire, salvare, distribuire e revocare certificati digitali costituiscono la **Public Key Infrastructure** (PKI)

PKI certification

- Il **soggetto** genera una coppia di chiavi (privata, pubblica)
- Chiede a CA che la (subject_ID, public_key) venga certificata e trasformata in un certificato
- La CA **autentica** il soggetto verificando che l'id effettivamente appartenga ad esso
- CA genera la firma per (subject_ID, public_key) usando la chiave privata di CA
- CA attacca la firma al (subject_ID, public_key) per creare il certificato
- CA manda il certificato al soggetto (e a chiunque ne abbia bisogno)

PKI authentication

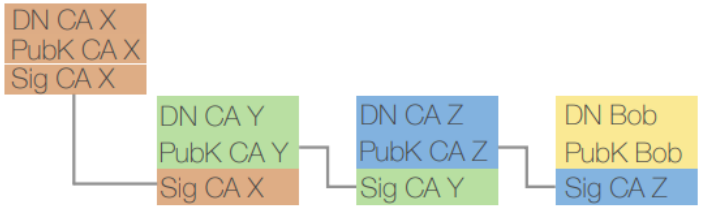
Out-of-band authentication

- eseguito usando metodi tradizionali (email, fax, telefono o meeting)
  **In-band authentication
- Eseguito usando PKI stessa
- Possibile solo per certi tipi di certificato dove l'identità (es email address) può essere verificata.

PKI certification authorities

Il processo di certificazione è basato sulla fiducia.

- L'utente si fida che l'autorità pubblichi solo certificati che associano correttamente i soggetti e la loro public key
- La maggior parte dei PKI danno la possibilità a un CA di certificare un altro CA.
  - un CA dice ai suoi utenti che possono fidarsi di quanto dice l'altro CA nei suoi certificati.

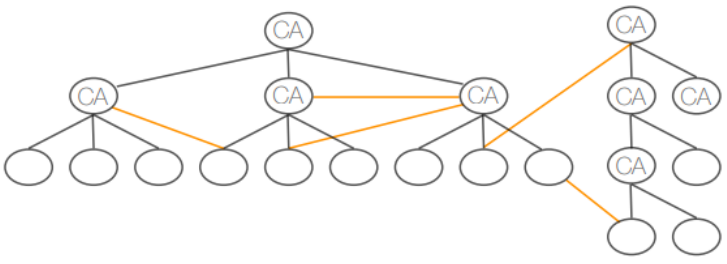


Concatenazioni di certificati:
Possono essere di una lunghezza arbitraria.
Ogni certificato nella catena è **validato** dal certificato precedente fino al certificato radice.
Certificati differenti:

- "*Leaf* " certificati (end user)
- "*intermendiate*" certificates
- "*root*" certificati

I certificati possono essere organizzati come:

- albero con radice (X.509)
- grafo (PGP)



Gerarchia di fiducia (X.509)
Basato su catene di certificati che formano un albero tra entità con abbastanza fiducia da essere CA.
La blind trust la si pone sul certificato radice (root) e deve essere guadagnata tramite esperienza, competenza e altri aspetti non tecnici.
Chiunque dica di essere un CA deve essere una entità con fiducia

Web of Trust (PGP)
In PGP qualunque utente può fingersi un CA e firmare le chiavi pubbliche di altri utenti.
Una chiave pubblica è valida solo se viene firmata da abbastanza utenti.

Il sistema può evolversi a formare un web "dinamico"
Fiducia deve essere simmetrica o transitiva

PKI validation

Validazione, controllo che il certificato sia:

- corrente (in un certo range di date)
- deve essere stato firmato da un root CA o c'è una catena di firme che portano a un root CA
- non deve essere stato falsificato
- non deve essere stato revocato

Verificare la correntezza, la firma e la falsificazione può essere fatto in locale
Verificare la revocazione è complesso.

Revocazione - il processo tramite il quale si rompe il collegamento tra una chiave pubblica e il soggetto collegato.

- visto che i certificati sono inviati agli utenti è impossibile richiamarli
- la revoca può solo inserire il certificato in una lista di certificati da revocare

Il controllo se il certificato è in una lista di revoca può essere fatto:

- Online:
  - consultando il database centralizzato
- Offline:
  - consultando una copia locale del database dei certificati revocati
  - la copia può essere out-of-date

Certificate Revocation List (CRL)

- lista di certificati da revocare distribuita periodicamente dai CA
- l'utente deve verificare l'ultimo CRL durante la validazione per essere sicuro che il certificato sia valido
- X.509 include a CRL profile, che descrive il fromato dei CRL

Problemi dei CRL:

- Tempo: ogni quanto rilasciare i CRL
- dimensione: incrementale vs bulk