Certificate authority

Il sistema delle CA permette di contrastare attacchi MITM basati sull'intercettazione e sostituzione di chiavi pubbliche. Le CA rilasciano certificati che garantiscono l'associazione di una chiave pubblica all'utente che l'ha generata.

Certificato digitale

Contiene:

- indicazione del formato (numero di versione);
- nome della CA che l'ha rilasciato;
- numero seriale unico all'interno della CA;
- indicazione dell'algoritmo usato per la firma del certificato;
- periodo di validità;
- chiave pubblica e dati dell'utente;
- indicazione del protocollo (e i suoi parametri) da usare con la chiave pubblica;
- firma della CA.

Ricezione della chiave pubblica

Se U vuole comunicare con V, può richiedere il certificato di V alla CA o a V stesso, verificarne la firma e se è corretta estrarre la chiave. Le chiavi pubbliche delle CA fidate sono fornite dal SO/browser, quindi un attacco MITM diventa equivalente a compromettere il sistema dell'utente.

La verifica del certificato potrebbe richiedere più passaggi, se è rilasciato da una CA che non è nota all'utente ma che ha un certificato firmato da una CA fidata.

Revocazione

È fondamentale per la sicurezza avere un meccanismo di revocazione di certificati non validi: le CA mettono a disposizione archivi pubblici di certificati revocati, che devono essere controllati regolarmente.