

Certificati digitali e infrastruttura a chiave pubblica

Alessandro Armando



Università
di **Genova**



ini

**Cybersecurity
National Lab**

introduzione

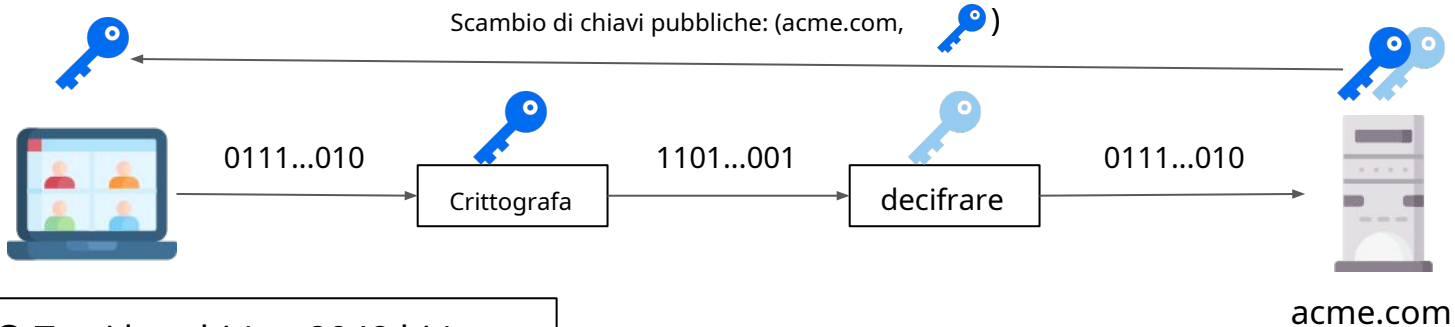
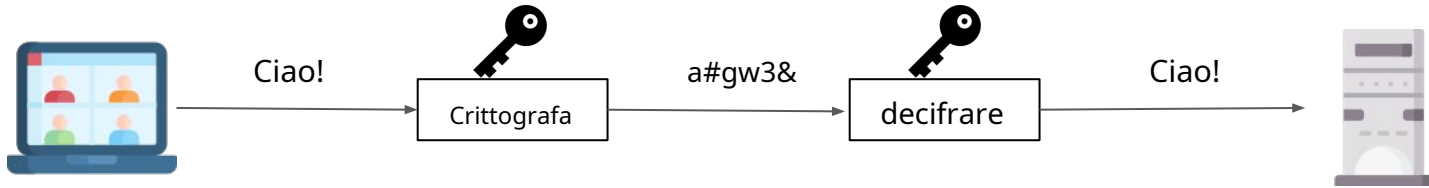
- I certificati digitali sono oggetti digitali che servono:
 - distribuzione chiavi
 - autenticazione (con non ripudio)
- I certificati digitali svolgono un ruolo chiave nella protezione del Web
- La Public Key Infrastructure (PKI) fornisce gli elementi tecnici e legali per consentire l'uso sicuro del Web.

Tabella di marcia

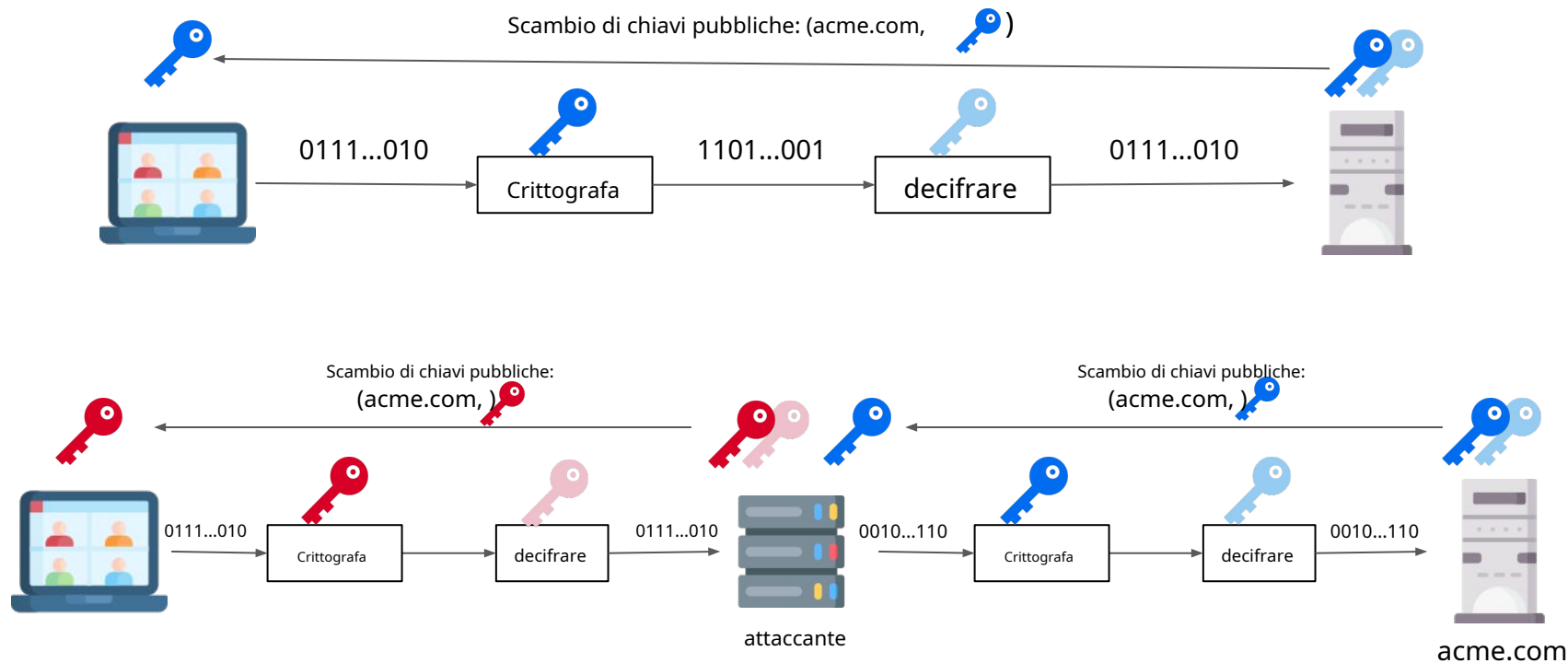
1. Revisione della crittografia a chiave pubblica
2. Il problema della distribuzione delle chiavi
3. Certificati digitali
4. Infrastruttura a chiave pubblica (PKI)

Crittografia simmetrica e crittografia a chiave pubblica

- Tasti brevi (es. 256 bit)
- Crittografia veloce



Attacco Man-in-the-Middle



Il client ora può comunicare in modo sicuro... con l'attaccante!

Certificati digitali



- Un Certificato Digitale consente il **parte affidata** per verificare l'autenticità di una chiave pubblica
- Associando la chiave pubblica del Titolare al suo nome.
- Normalmente l'Emittente è un'Autorità di Certificazione

Proprietario	acme.com
Chiave pubblica	00...01001001
Emittente	trustme.com
....
Firma	10...011101101

- Una carta d'identità consente all'affidatario di verificare l'autenticità di una persona
- Legando l'immagine del Titolare al suo nome.



Certificati digitali

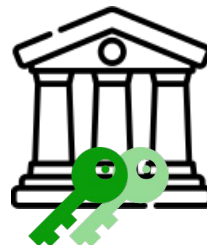
Permettere  e  essere la chiave pubblica e privata di rispettivamente l'Emittente.

Scriviamo (acme.com, , trustme.com)  as una scorciatoia per

Proprietario	acme.com
Chiave pubblica	00...01001001 
Emittente	trustme.com
....
Firma	10...011101101







acme.com



trustme.com

Fidato
Emittente
(CIRCA)

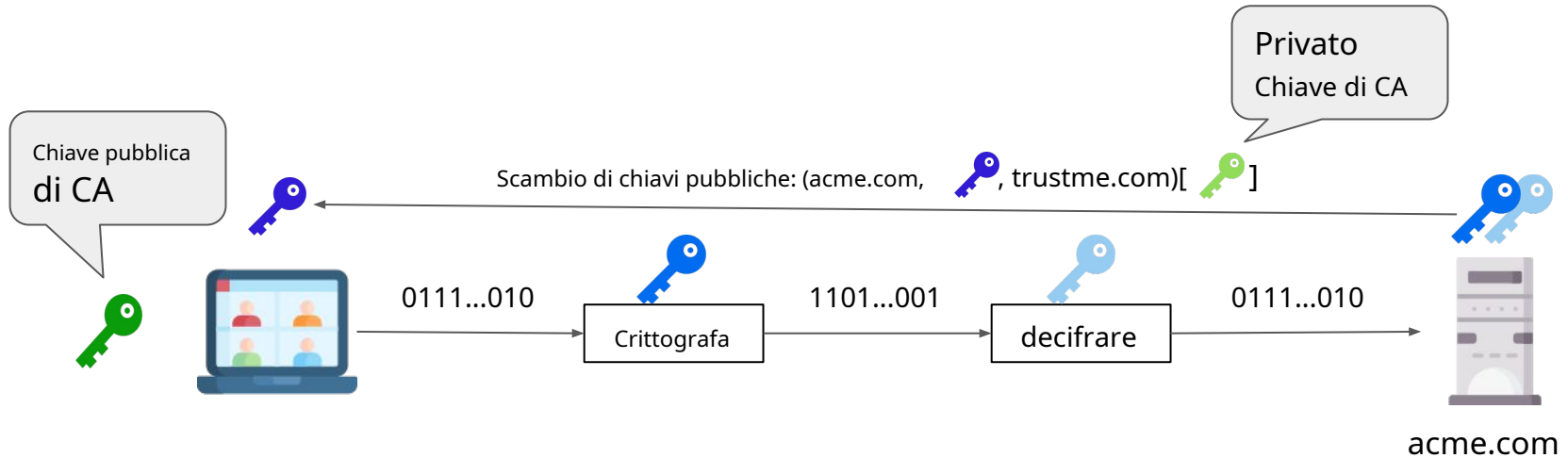
Usando  noi possiamo

- **Verificare** la validità di (acme.com, , trustme.com) 
- **Rifiutare** la validità di (acme.com, , trustme.com)  [Se  non è la chiave privata di trustme.com

Verifica del certificato

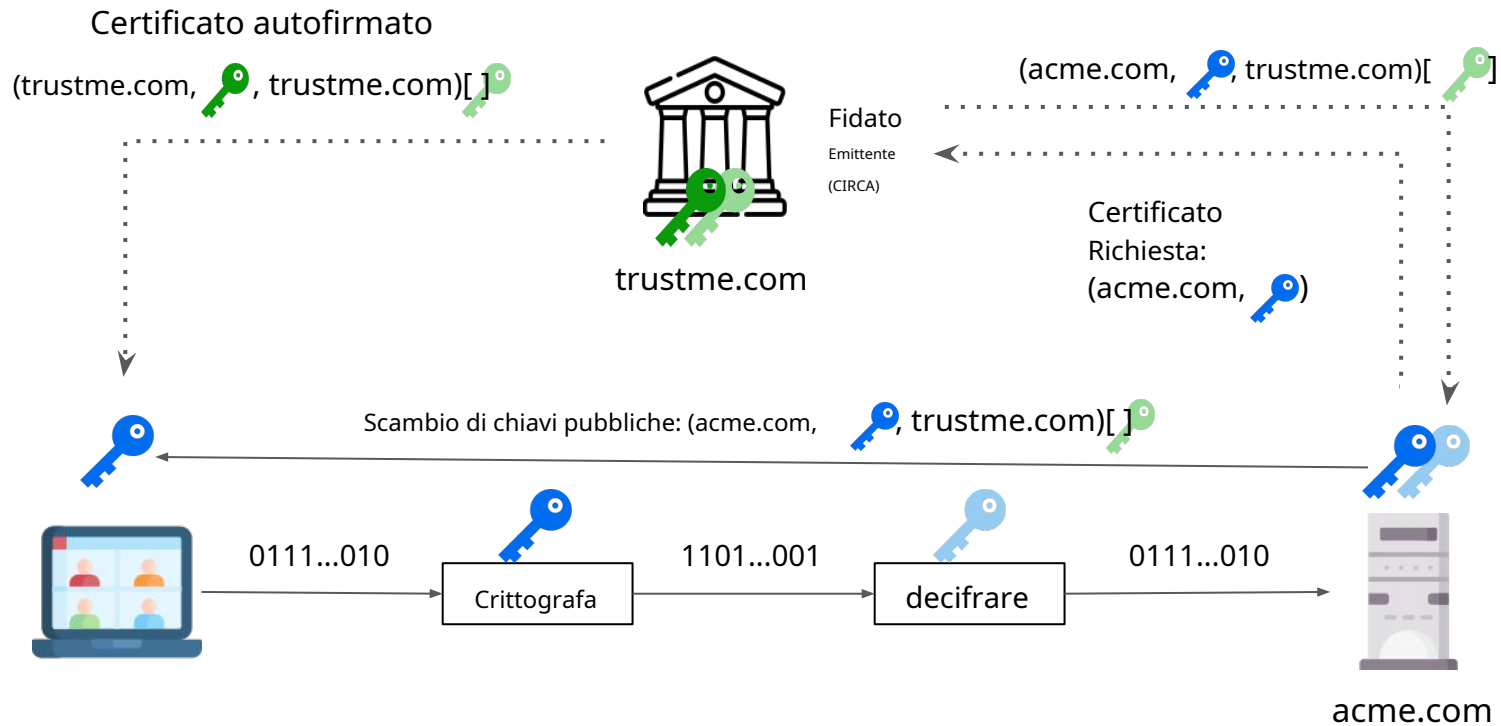
- Prima di fidarsi di un certificato (digitale) **devi verificarne la validità**.
- Ciò può essere fatto verificando la validità della firma (digitale) generata dall'Emittente e inclusa nel certificato.
- Ovviamente un certificato emesso da un emittente non affidabile deve essere scartato.

Scambio di chiavi pubbliche con certificati digitali

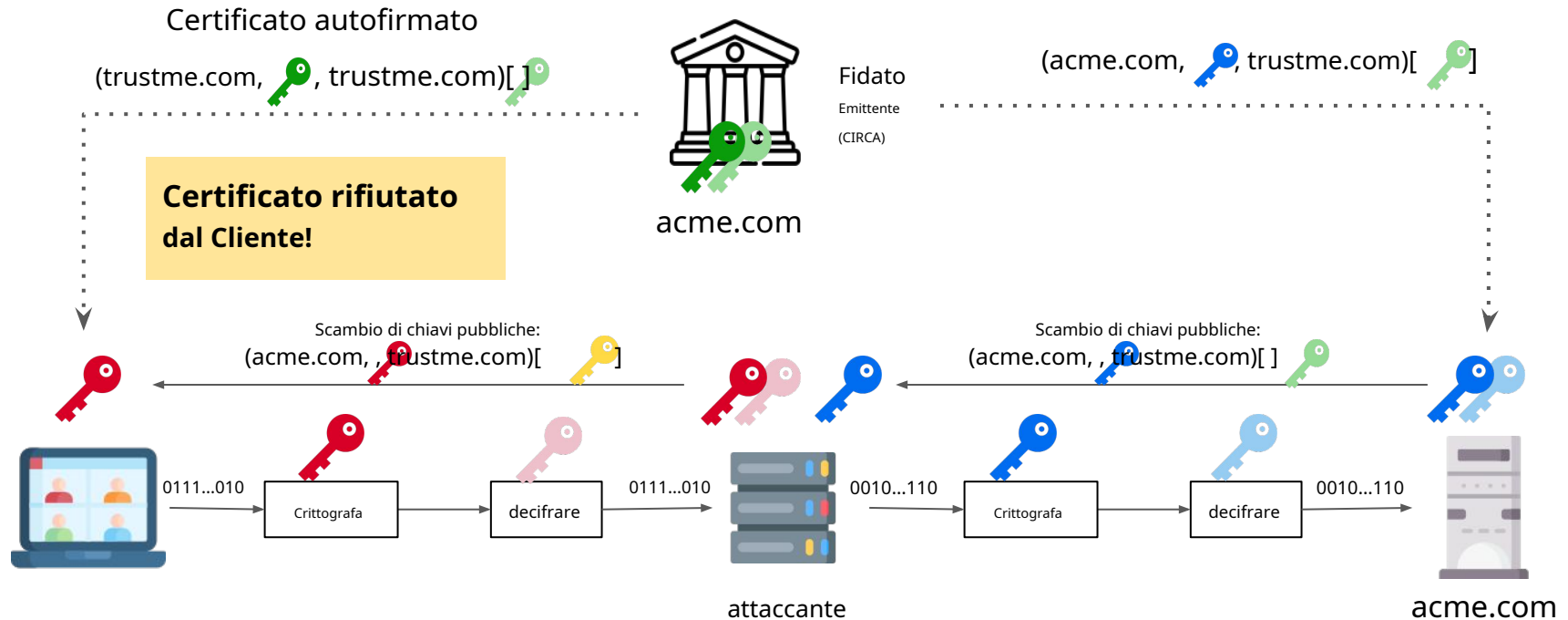


- Da dove il cliente ha ottenuto la chiave pubblica della CA?
- Come può essere certo che appartenga davvero a CA?

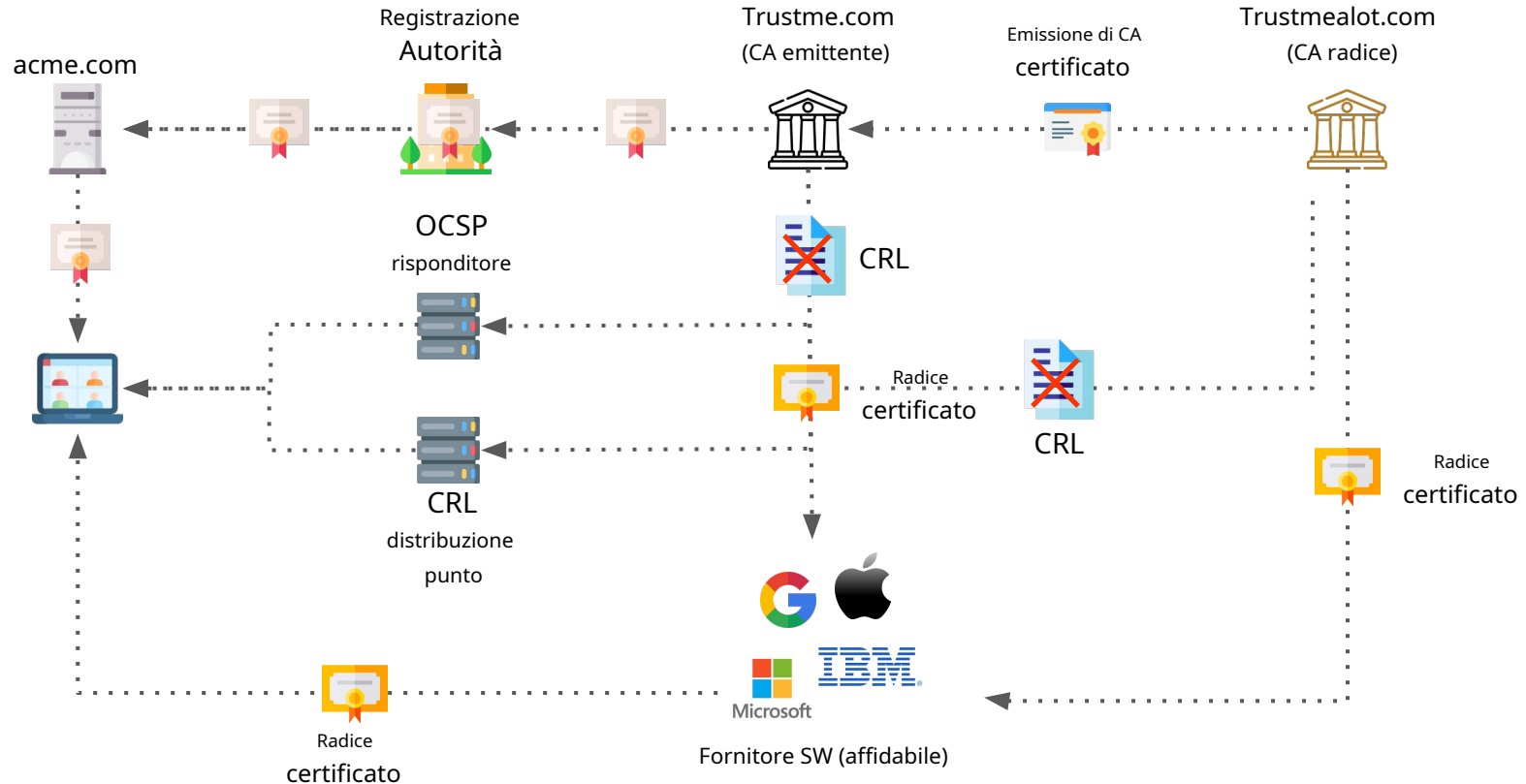
Ciclo di vita del certificato



Attacco Man-in-the-Middle contrastato



Infrastruttura a chiave pubblica



Tipi di certificati digitali

Diversi tipi di certificati riflettono diversi tipi di verifica CA delle informazioni sull'oggetto del certificato.

- **Convalida del dominio (DV)** i certificati sono di gran lunga il tipo più comune. L'unica convalida che la CA deve eseguire nel processo di emissione del DV è verificare che il richiedente abbia un controllo effettivo del dominio. La CA non è tenuta a tentare di verificare l'identità reale del richiedente.
- **Convalida dell'organizzazione (OV) e Convalida estesa (EV)** certificati, in cui il processo ha lo scopo di verificare anche l'identità reale del richiedente.)