Schema tradizionale di autenticazione in applicazioni di rete

Davide Quaglia

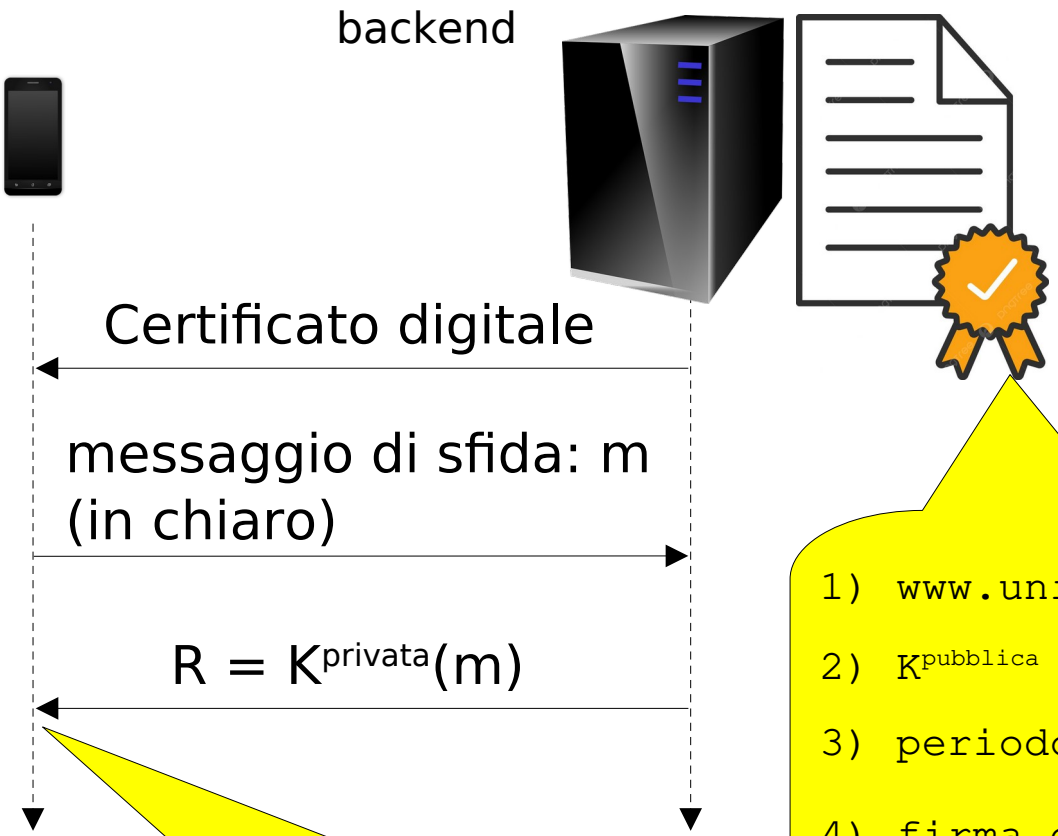
Ambiti di utilizzo

- Interazione tra frontend e backend di una web application
  - Frontend = browser
  - Backend = web server
- Interazione tra frontend e backend di una applicazione mobile
  - Frontend = APP
  - Backend = server
- Interazione tra publisher (o subscriber) e broker in MQTT

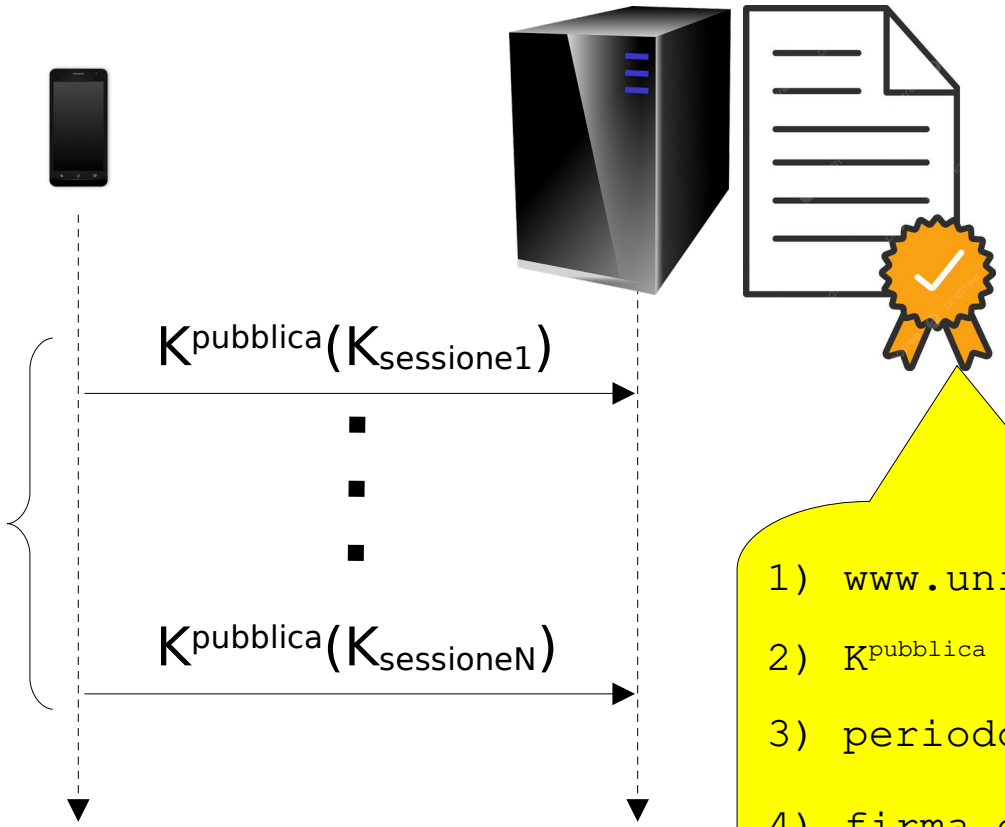
Concetti generali da seguire

- Autenticazione remota diretta del processo che fa da server
  - Backend nel caso di web application o APP
  - Broker nel caso di MQTT
- Il server deve dare certezza circa la coppia nome_host/indirizzo_IP
- Durante l'autenticazione del server vengono decise le chiavi simmetriche di sessione con cui viene cifrato il flusso dati
- Il processo client si può autenticare mediante user/password (come se fosse autenticazione locale) perché il flusso è cifrato

Autenticazione del backend



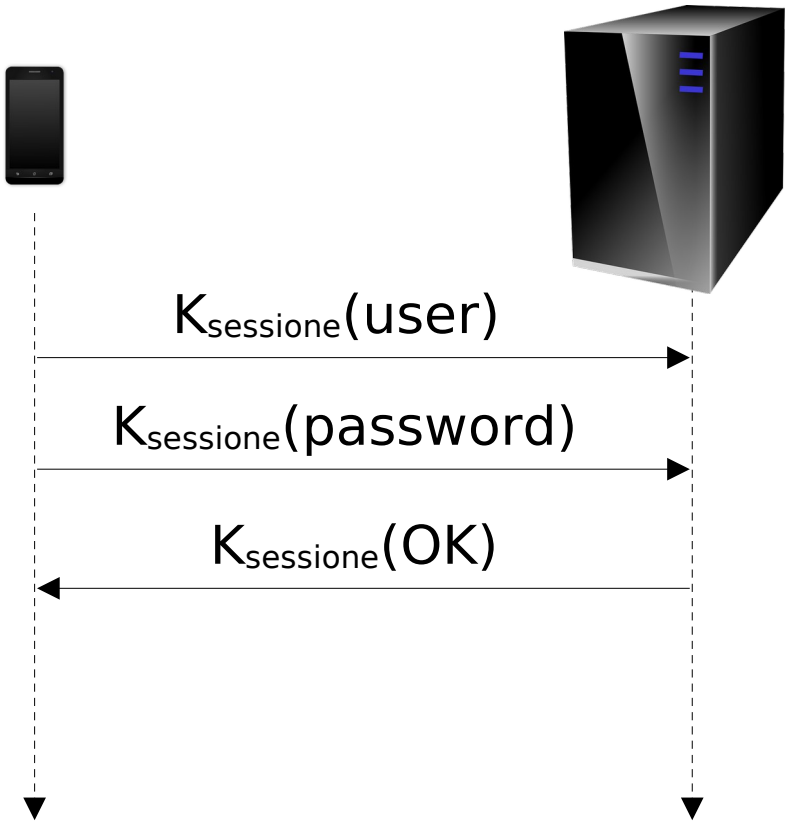
Scambio della chiave simmetrica di sessione $K_{sessione}$



Rinnovo periodico della chiave di sessione

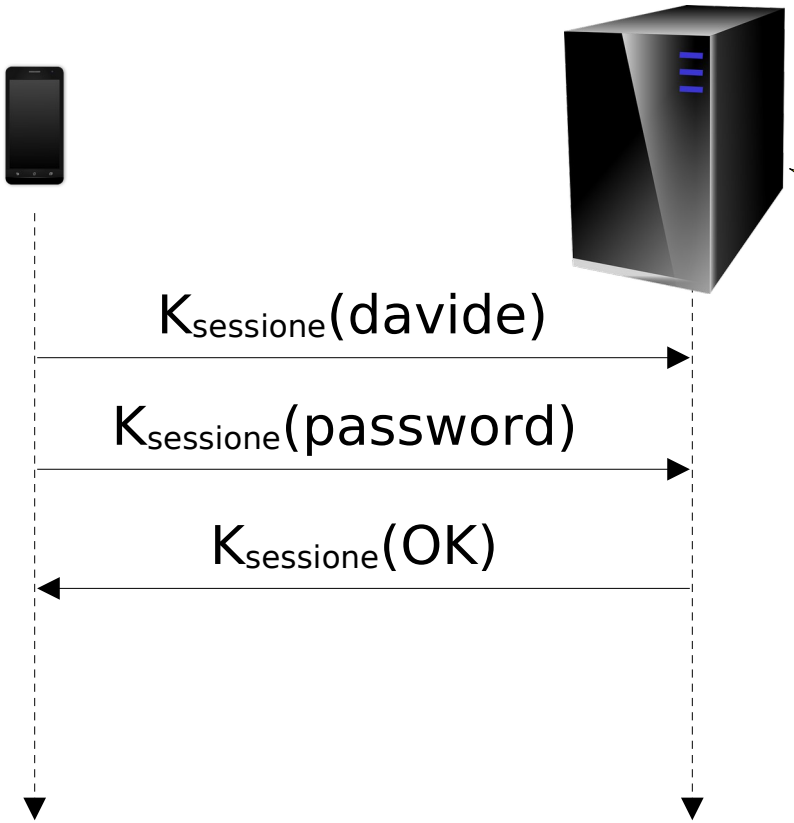
1) www.univr.it=157.27.10.23
2) $K^{pubblica}$
3) periodo di validità
4) firma digitale della CA

Autenticazione semplificata del frontend



Alternativamente il client potrebbe autenticarsi con un certificato come ha fatto il server (ad es. quando usiamo SPID o CIE)

Controllo della password da parte del backend



Chiave primaria della tabella

Il sale è in chiaro

USER	PASSWD	SALT
...	...	...
davide	HASH(passwd + salt)	2025-06-19-01-41
...	...	...