

Accesso Sicuro Ai Servizi

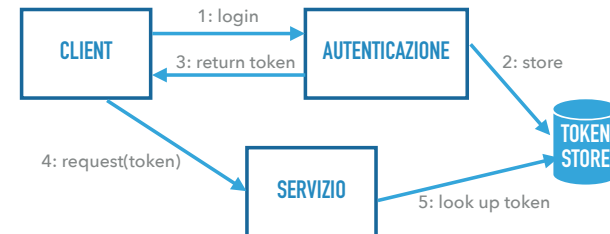
- In un sistema distribuito le richieste ai servizi (lato server) devono essere vagliate: solo gli utenti autenticati e autorizzati possono usare i servizi
- Bisogna far sì che le singole richieste siano autorizzate, ovvero provenienti da utenti conosciuti e autorizzati, ma bisogna evitare di chiedere continuamente le credenziali agli utenti
- Inoltre bisogna far sì che la prova di identità e la verifica delle credenziali sia gestita in un solo server



1

Prof. Tramontana - Ottobre 2022

Autenticazione Basata Su Token



2

Prof. Tramontana - Ottobre 2022

Token

- Una volta autenticato l'utente, gli si fornisce un token che userà per le sue successive richieste ai servizi
- Un token per l'accesso è una credenziale che può essere usata per accedere a servizi
- Un token può essere una stringa (opaque, ovvero incomprensibile), per es. `kPoPMRYrCEoYO6s5` oppure un oggetto, per es. un oggetto JSON, detto JSON Web Token (JWT)
- Lo scopo del token è informare che chi lo possiede è stato autorizzato ad accedere al servizio
- Il token tipicamente indica: l'utente identificato, chi lo ha emesso, il timestamp al momento dell'emissione, la durata, a chi è rivolto (il client che lo ha chiesto)

3

Prof. Tramontana - Ottobre 2022