WEB DAY 2023

MILANO 16 MARZO

Autenticazione Federata e Sicura con Keycloak

Ing. Raffaele Rialdi @raffaeler
Senior Software Architect, Consultant

Microsoft Most Valuable Professional

/* Sponsor */

webscience an adesso company

.NET on aws

improove

/* Partner */

Cloud Champions

Serverless Italy

TOMORROWDEVS

TORINO

AWS User Groups Milano

{CODEMOTION}

BLAZOR DEVELOPER ITALIANI

tag Talent Garden

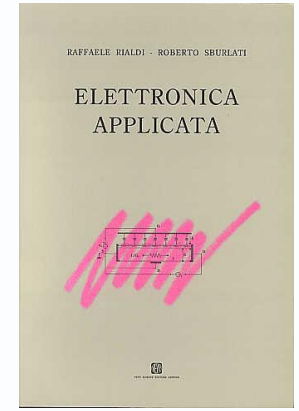
ACCESSIBILITY DAYS

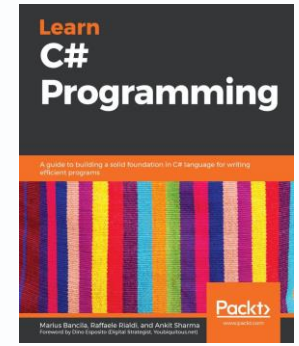
AZURE MEETUP MILANO

POINTER PODCAST

Chi sono?

- Raffaele Rialdi: @raffaeler o più semplicemente "Raf"
  - Laura magistrale in Ingegneria Elettronica all'università di Genova
  - Insegnante di supporto all'Università di Ingegneria Informatica di Genova
- Consulente in diversi campi
  - Manufacturing, racing, healthcare, financial, …
- Speaker e Trainer un po' ovunque
  - Italy, Romania, Bulgaria, Russia, USA, …
- Orgoglioso membro della grande famiglia dei Microsoft MVP dal 2003





Oggi parliamo di di Autenticazione

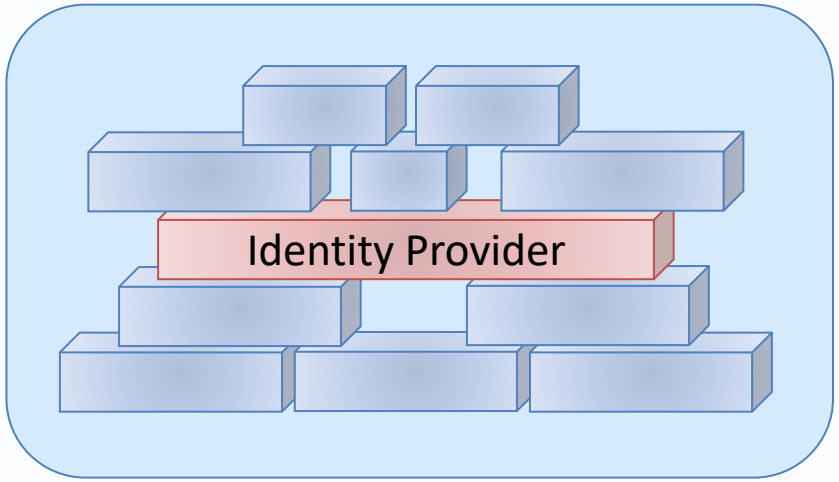
https://github.com/raffaeler/authentication

Takeaways di oggi:

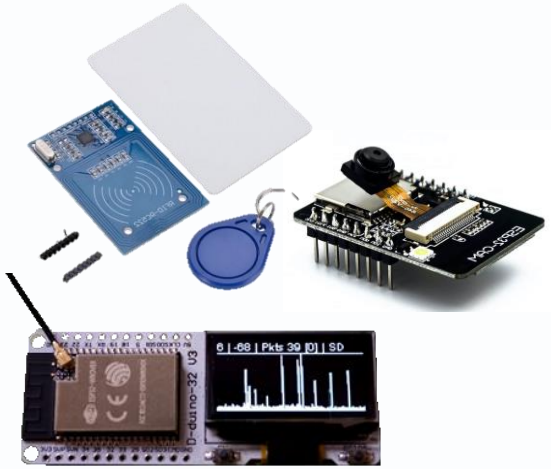
- DNS+DHCP
- Cloud first != Always on
- Bassa latenza in scenari di microservizi

Come autenticate oggi?

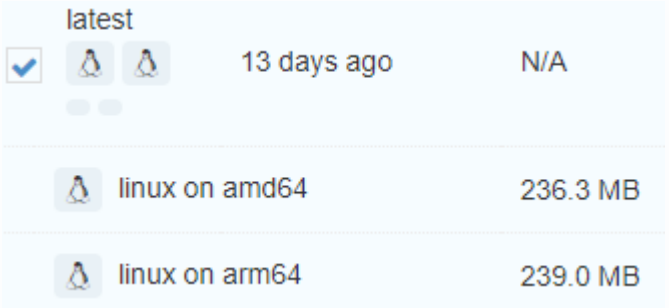
- Autenticate con le password?
  - Tanto codice, niente SSO
  - GDPR!
- Usate una libreria come Identity Server?
  - Tanto codice per la UI e l'integrazione
  - Dovete inseguire i bollettini di sicurezza
- Usate un cloud provider?
  - Penalizzante negli scenari disconnessi
  - Impossibile per l'automazione industriale
  - Bloccante in certi scenari IoT
    - Es: autorizzazione apertura porte



container / kubernetes



Cos'è Keycloak



- Keycloak è l'Identity Provider di Red Hat
  - Fornisce tutto il necessario per autenticare e autorizzare
  - Espone WebApi, ma è una appliance, quindi "pronta all'uso"
- La configurazione è semplice:
  1. Si definisce un Realm: un confine per applicazioni, gruppi e utenti
  2. Ogni applicazione è associata al flusso di oAuth appropriato
  3. Si definiscono i mapping tra attributi utente e claim
- Supporta la federazione con cloud providers e sync con LDAP
- Supporta il deploy in container e Kubernetes (anche su ARM64)

I flussi oAuth supportati da Keycloak

- Standard Flow (Authorization code flow): RFC 6749 – 4.1
  - Classic web app, SPA or Mobile
- Service account roles (Client Credentials Grant): RFC 6749 - 4.4
  - Console application
- Device authorization grant: RFC 8628
  - Scenario: client (device Iot) con capacità limitate e senza browser
- CIBA - Client initiated backchannel authentication grant
  - OpenId Connect
  - Scenario: device limitati o app server
  - Il back-end comunica direttamente con l'IP (non ci sono redirect via Browser)

Standard flow with PKCE (RFC 7636)

- Estende sullo standard flow
- PKCE aka "pixy" serve a proteggere i client pubblici da attacchi al codice di autorizzazione
  - PKCE = Proof Key for Code Exchange
  - Client pubblici == **App SPA e Mobile**
- Il "authorization_code" è spedito dal client all'IP per ottenere l'**access token**.
- PKCE dovrebbe essere richiesto dal client OIDC
  - Keycloak può imporlo anche se non richiesto (Client – Advanced configuration)

OpenId Connect: finalmente un po' di ordine

- OpenId Connect è il protocollo che mette ordine nei protocolli basati sulla specifica oAuth
  - Standardizzato e ampiamente adottato ➔ supportato lato client
  - Fornisce, su richiesta, dettagliate "user info"
  - Prevede le revoche delle sessioni attive grazie al back-channel
- I 3 token di OpenId Connect sono:
  - Id token: l'Identity Token che rappresenta l'utente
  - Refresh token: il Token che serve a generare nuovi token
  - Access token: il Token JWT che spendiamo presso le batterie di servizi

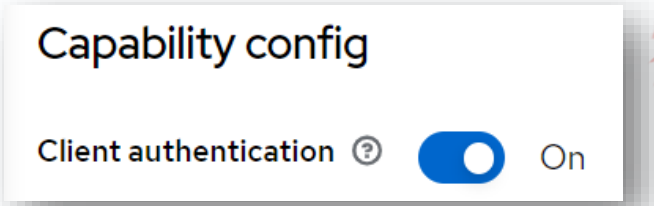
I Mapper di Keycloak

- I Mapper scrivono i Claim in uno o più dei 3 token
- In un classico scenario SPA + WebAPI avremo almeno 2 mapper
  1. *audience*: determina a chi è destinato il token
  2. *roles*: usati dall'applicazione per autorizzare l'utente
- Tra poco vedremo *acr/loa* usati per la step-up authentication

Name	Category	Type
acr loa level	Token mapper	Authentication Context Class Reference (ACR)
audience	Token mapper	Audience
realm roles	Token mapper	User Realm Role

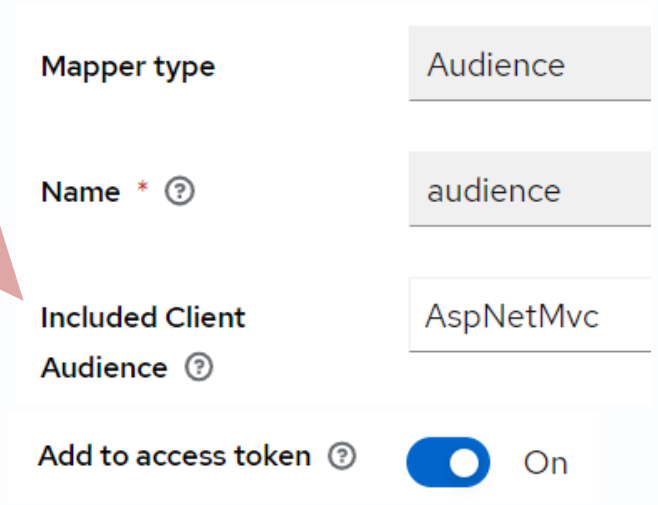
Audience e Issuer (scenario SPA + WebApi)

- Il client SPA e WebApi sono due client (app) dello stesso realm
  - SPA: Client authentication off (nessun secret)
  - WebApi: Client authentication on (la App ha il client secret)
  - Ogni token è inteso solo per lo **specifico client**



- Il client SPA può emettere un token da spendere nell'App della WebAPI

- Issuer: è l'URL del Realm
  - Determina chi ha emesso il token
  - Tutti i client condividono lo stesso URL
  - Viene validato dal client



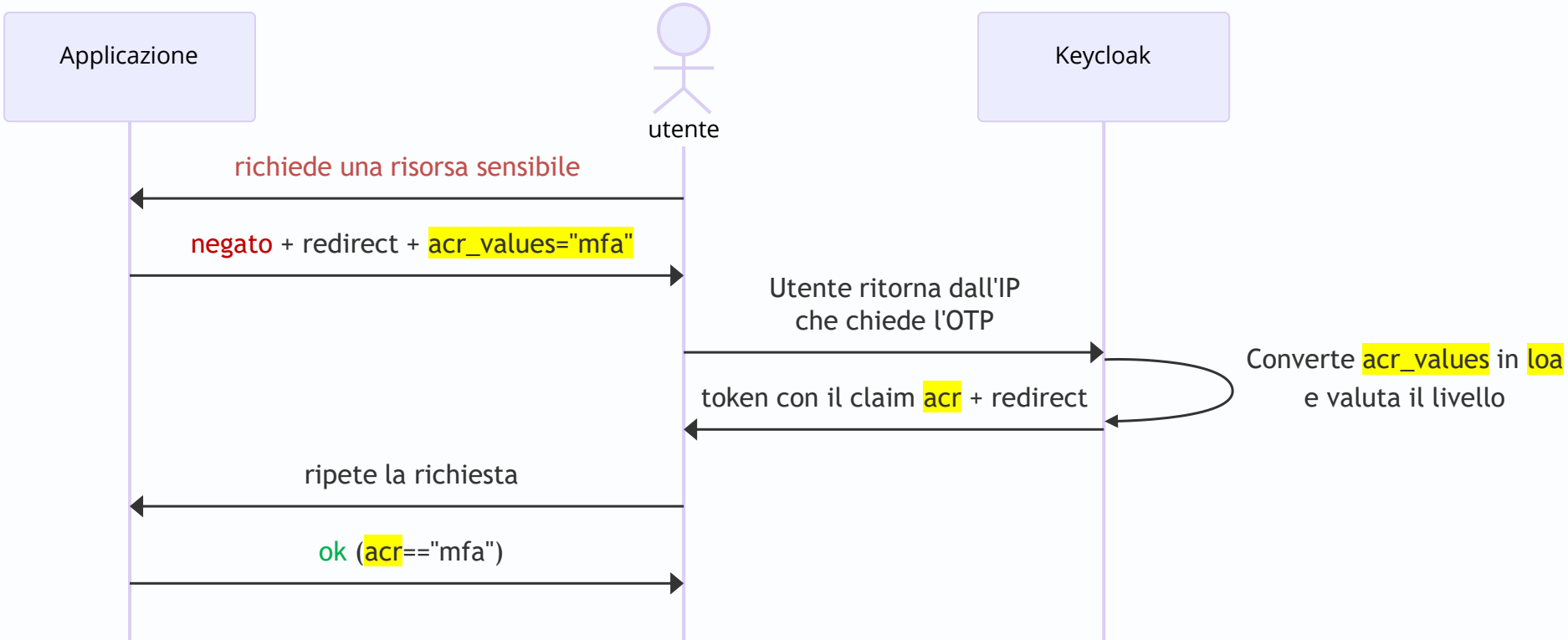
Autenticazione step-up

L'utente è già autenticato

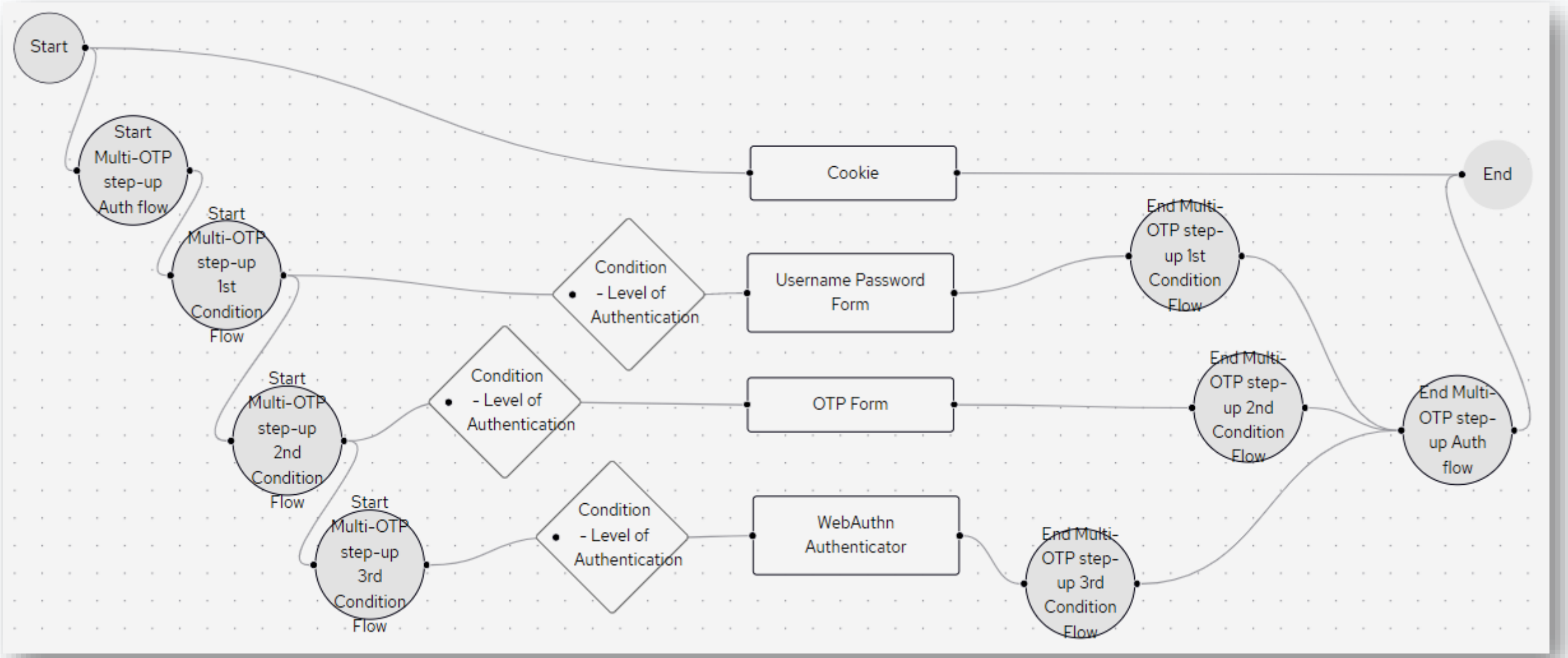
ma vuole accedere ad una **risorsa sensibile**

Step-up: ri-autenticare un utente che ha già un token

- Richiedere un metodo di autenticazione più forte
  - TOTP (acr = "mfa") (Google Authenticator), Hardware Key (acr = "hwk") (FIDO2)
  - acr = Authentication Context Class Reference (stringa)
  - loa = Level of Authentication (numero)



Il flusso step-up di Keycloak



Federazione

Federazione

- Keycloak può federarsi con moltissimi provider esterni
  - Google, Microsoft, AWS e molti altri
- I custom Claim disponibili dei provider sono salvati da Keycloak
  - Il token conterrà l'unione dei claim del provider e di Keycloak
- Sincronia con AD
  - Gli utenti sono "copiati" nel DB di Keycloak database così da supportare scenari disconnessi
  - Es: Autenticazione di un utente che deve aprire una porta, ma:
    - non c'è connettività internet
    - oppure la sala server è in manutenzione.

Per concludere

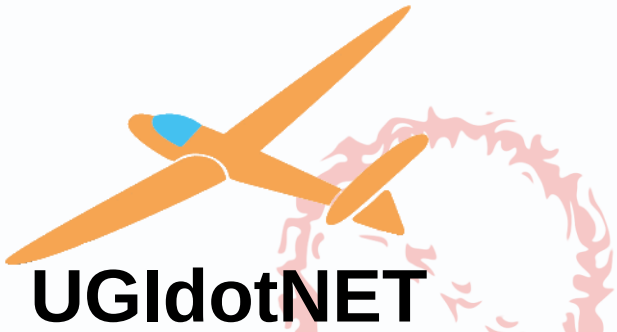
- Eliminate il codice di autenticazione dalle vostre applicazioni
- La bassa latenza di rete e gli scenari disconnessi sono importanti
- I Realm in Keycloak isolano un gruppo di app, utenti e policies
- Usate l'autorizzazione di .NET, non quella di Keycloak
  - Invece Javascript (SPA o Mobile) può beneficiare dell'**autorizzazione** di Keycloak
- Federare provider esterni è facile (compresi quelli custom)
- La sincronia gli utenti di AD abilita scenari ibridi e disconnessi

WEB DAY 2023

MILANO 16 MARZO

GRAZIE

Domande?



Dubbi? Curiosità?

Volete vedere il codice?

Cercatemi nelle sale