**WSO2 identity server - OAuth 2.0**

# Indice generale



# OAuth2 - OpenID Connect

Il seguente documento riguarda il supporto del protocollo OAuth 2.0 da parte del sistema di identificazione di Silfi SpA.

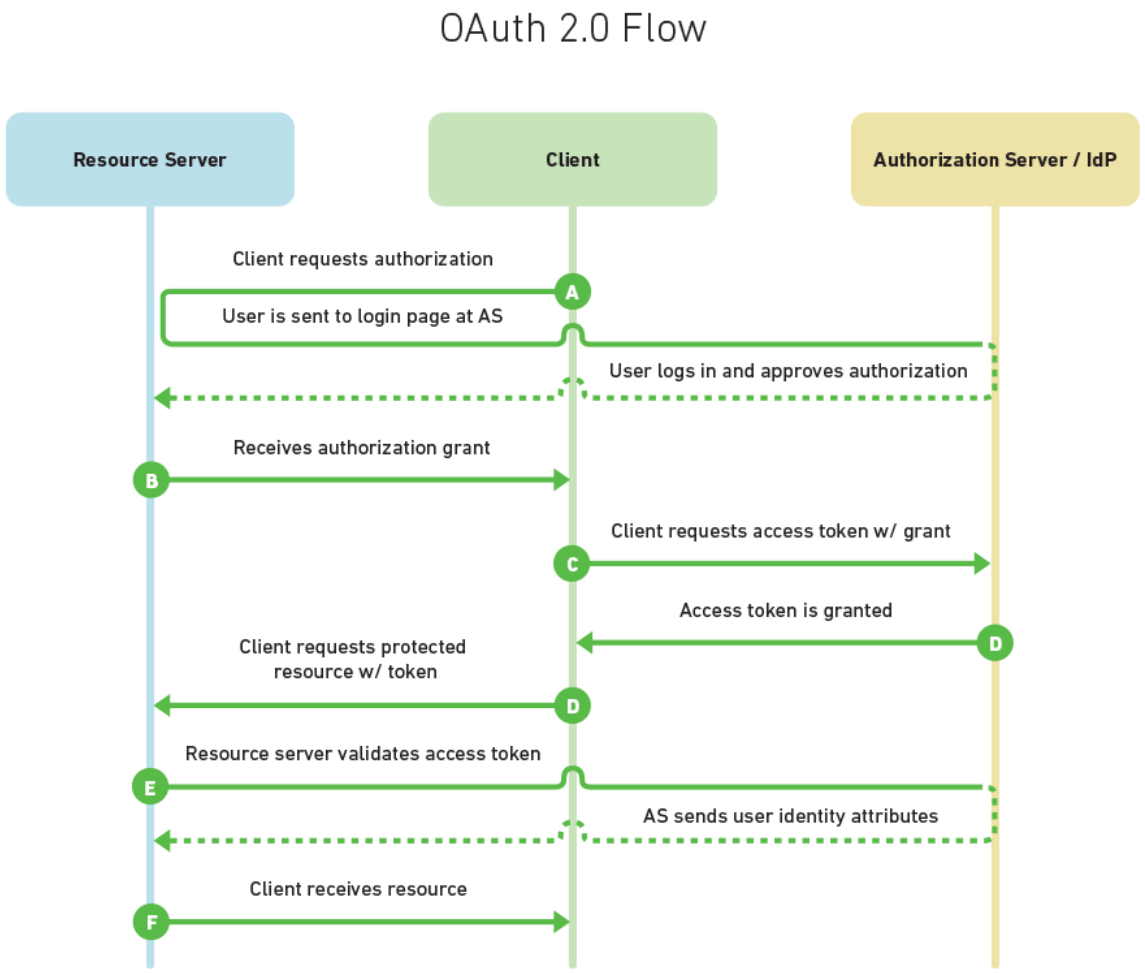
Le specifiche che riguardano il protocollo OAuth 2.0 possono essere trovate all’indirizzo:

https://datatracker.ietf.org/doc/html/rfc6749

Il sistema di identificazione di Silfi SpA rispetta le specifiche definite nel RFC 6749 con alcune eccezioni che verranno descritte più avanti ma che non vanno in alcun modo a modificare il flusso del protocollo

## Descrizione

Il protocollo OAuth 2.0 consente ad un applicativo terzo di avere un accesso limitato ad un servizio HTTP, sia per conto di un proprietario di una risorsa orchestrando un’interazione di approvazione tra il proprietario delle risorse e il servizio HTTP, sia consentendo ad un’applicazione di terze parti di ottenere l’accesso per conto proprio.
Il seguente diagramma riassume il flusso del protocollo OAuth 2.0.




## *Registrazione del servizio*

Come previsto dall' RFC 6749 il servizio deve registrarsi all'Authorization server di Silfi SpA, fornendo il redirection URIs. (vedi https://datatracker.ietf.org/doc/html/rfc6749#section-2)

## *Ottenere l'autorizzazione*

(vedi https://datatracker.ietf.org/doc/html/rfc6749#section-4.1)

## *Authorization Request*

(vedi https://datatracker.ietf.org/doc/html/rfc6749#section-4.1.1)

La url per la richiesta del grant è la seguente:

https://id.055055.it:9443/oauth2/authorize

L'Authorization request è usata dal client (applicativo) per ottenere l'autorizzazione dal proprietario della risorsa mediante il re-direzionamento dello user agent sul server di autenticazione. Il paragrafo 4.1.1 del RFC 6749 definisce i parametri obbligatori ed opzionali per la costruzione

dell’Authorization URL. Rispetto a quanto definito dall’ RFC il parametro redirect_uri diventa obbligatorio. É possibile comunque definire in fase di registrazione del servizio una o più redirect uri.

Altri parametri wso2 obbligatori:
agEntityId=[ENTE] es. agEntityId=FIRENZE

Per abilitazione CIE:
comEntityId=[ENTE] es. comEntityId=FIRENZE

- **solo** per abilitare credenziali utenze interne WSO2 (ex credenziali 055055):
&isAuthSilfi=yes

### *Access Token Request*

(vedi https://datatracker.ietf.org/doc/html/rfc6749#section-4.1.3)

La url alla quale richiedere il token è:
https://id.055055.it:9443/oauth2/token

L’Access Token Request è usato dal client (applicativo) per ottenere un access token. Il redirect_uri diventa un parametro obbligatorio perché definito nell’Authorization Request.

### *Accessing Protected Resources*

(vedi https://datatracker.ietf.org/doc/html/rfc6749#section-7)

La url alla quale richiedere gli attributi utenti è:
https://id.055055.it:9443/oauth2/userinfo

Il client (applicativo) usa l’access token per accedere alle risorse definite nell’Authorization Request mediante il parametro scope (vedi https://datatracker.ietf.org/doc/html/rfc6749#section-3.3).

### *Access Token*

(vedi https://datatracker.ietf.org/doc/html/rfc6749#section-1.4)

L'Access Token viene rilasciato solo una volta è ha una validità per un periodo limitato di tempo.