Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Una breve introduzione a OpenID Connect

Davide Vaghetti <davide.vaghetti@garr.it>

Università degli Studi Roma Tre, 07-10-2019

Workshop GARR 2019 "Net Makers"

OpenID Connect è uno ***standard aperto*** *pubblicato dalla OpenID Foundation nel 2014.*

Principi di design

Keep Simple Things Simple

Make Complex Things Possible

OpenID Connect 1.0...

- *is a simple identity layer on top of the OAuth 2.0 protocol*
- permette di verificare l'identità degli utenti
- definisce un profilo di base per gli utenti
- è basato su REST e JSON
- è mobile friendly

Attori

Utente

Tenta di accedere ad una risorsa utilizzando uno user-agent HTTP.

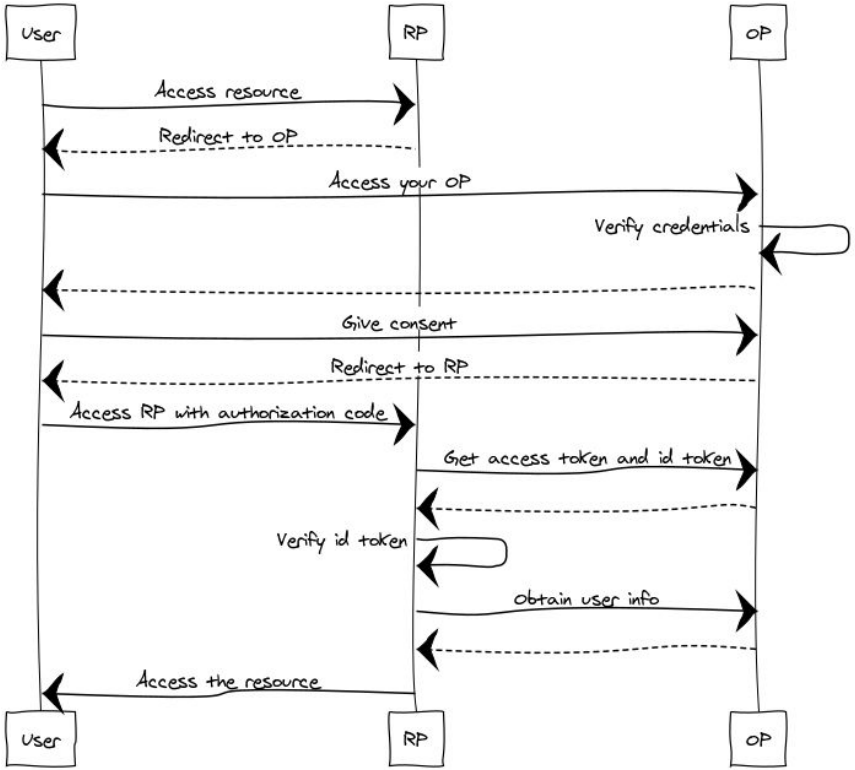
Relying Party o Client

L'entità che richiede e consuma gli access token, di solito un'applicazione web o mobile.

OpenID Provider

L'entità che autentica gli utenti e rilascia i token che permettono l'accesso alle identità degli utenti.

Authorization code grant



1. L'utente tenta l'accesso ad una risorsa.
2. L'RP redirige lo User-Agent al OP trasmettendo la Authentication Request come parametri HTTP.
3. L'OP autentica l'utente e ne chiede l'autorizzazione per trasmettere la sua identità al RP.
4. L'OP redirige l'utente al RP trasmettendo la Authentication Response e l'Authorization code.
5. L'RP accede al Token Endpoint scambiando l'Authorization code.
6. L'RP riceve l'ID token e l'access token, li valida e accede allo User Info endpoint per ottenere il profilo dell'utente.

Endpoint HTTP (OpenID Provider)

Obbligatori

- **Authorize endpoint**: dove avviene l'autenticazione dell'utente e dove si **autorizza** il Relying Party ad ottenere un token.
- **Token endpoint**: dove il Relying Party richiede un token per poter accedere all'identità dell'utente.
- **UserInfo endpoint**: dove il Relying Party richiede il profilo dell'utente.

Opzionali

- **Discovery**: (non un vero e proprio endpoint, ma una *well-known localtion*) dove l'OpenID Provider pubblica i metadata con tutti i parametri di configurazione (ad es. le URL degli endpoint).
- **Client Registration**: dove un Relying Party si può registrare dinamicamente presso un OpenID Provider.

Token

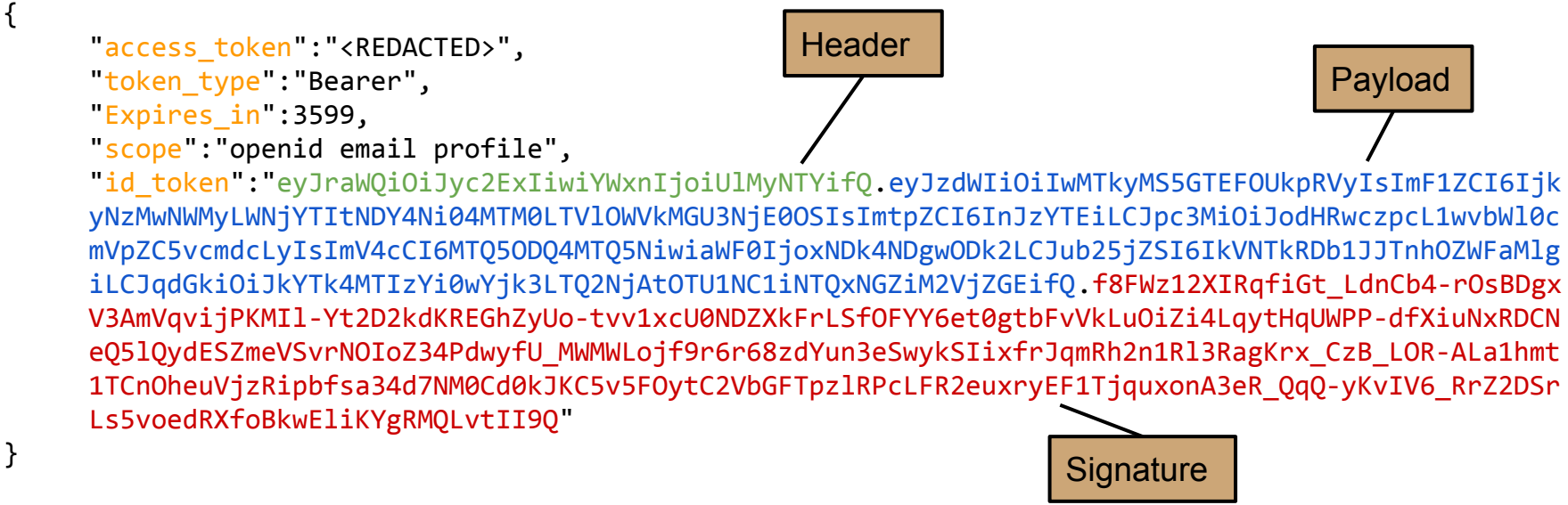
Access token: una stringa che rappresenta l'autorizzazione concessa ad un Relying Party. Il formato non è

Refresh token: un token che permette di ottenere altri access token quando questi scadono o diventano invalidi.

ID token: un **JSON Web Token** firmato e potenzialmente criptato che contiene le informazioni relative al processo di autenticazione e rappresenta la **credenziale** per accedere alle risorse del Relying Party.

ID Token

L'ID Token è sempre relativo ad una sessione attiva.



ID Token payload


```
{
    "sub":"01921.FLANRJQW",
    "aud":"927305c2-cca2-4686-8134-5e9ed0e76149",
    "kid":"rsa1",
    "iss":"https:\/\/mitreid.org\/",
    "exp":1498481496,
    "iat":1498480896,
    "nonce":"EMNDCoRINxNeaZ2X",
    "jti":"da98123b-0b97-4660-9554-b5414fb3ecda"
}
```

Claims e scope

Scope	Claims
email	email, email_verified
phone	phone_number, phone_number_verified
profile	name, family_name, given_name, middle_name, nickname, preferred_username, profile, picture, website, gender, birthdate, zoneinfo, locale, updated_at
address	address

Reference

OpenID Foundation Research and Education Working Group

https://openid.net/wg/rande/

OpenID Connect Federations specification

http://openid.net/specs/openid-connect-federation-1_0.html

OpenID Foundation International Government Assurance Profile (iGov) Working Group

https://openid.net/wg/igov/

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Grazie

Davide Vaghetti (davide.vaghetti@garr.it)