



OAuth Introduction

OAuth Roles

- Resource Owner
 - Owns access to protected resources

OAuth Roles

- Resource Owner
 - Owns access to protected resources
- Resource Server
 - Protected server; accepts access tokens

OAuth Roles

- Resource Owner
 - Owns access to protected resources
- Resource Server
 - Protected server; accepts access tokens
- Client
 - Application making request to protected resources

OAuth Roles

- Resource Owner
 - Owns access to protected resources
- Resource Server
 - Protected server; accepts access tokens
- Client
 - Application making request to protected resources
- Authorization Server
 - Issues access tokens to client

OAuth Review

- OAuth v2.0
 - clients grant access to server resources without sharing credentials

OAuth Review

- OAuth v2.0
 - clients grant access to server resources without sharing credentials
- Client IDs and Secrets
 - used to identify and authenticate applications

OAuth Review

- OAuth v2.0
 - clients grant access to server resources without sharing credentials
- Client IDs and Secrets
 - used to identify and authenticate applications
- Tokens
 - Client IDs and Secrets exchanged for tokens
 - Grant access to a resource
 - Time bound

OAuth Review

- Scopes
 - limits the tokens access for a resource

OAuth Review

- Scopes
 - limits the tokens access for a resource
- Grant Types
 - 4 Grant Types: client credentials, password, implicit and authorization code

OAuth Review

- Scopes
 - limits the tokens access for a resource
- Grant Types
 - 4 Grant Types: client credentials, password, implicit and authorization code
- Requires TLS
 - OAuth 2.0 must be protected via TLS

Access Tokens



Identification from the requesting application (client ID and secret)

Access Tokens



Identification from the requesting application (client ID and secret)

+



Resource owner credentials (optional: user of the app)

Access Tokens



Identification from the requesting application (client ID and secret)

+



Resource owner credentials (optional: user of the app)

+



Optional information about what the application wants to do with the resource (scope)

Access Tokens



Identification from the requesting application (client ID and secret)

+



Resource owner credentials (optional: user of the app)

+



Optional information about what the application wants to do with the resource (scope)

=



Access Token and (optional) refresh token

Refresh Tokens



Identification from the requesting application (client ID and secret)

Refresh Tokens



Identification from the requesting application (client ID and secret)

+



Refresh token

Refresh Tokens



Identification from the requesting application (client ID and secret)

+



Refresh token

+



Optional information about what the application wants to do with the resource (scope)

Refresh Tokens



Identification from the requesting application (client ID and secret)

+



Refresh token

+



Optional information about what the application wants to do with the resource (scope)

=



Access Token and (optional) refresh token

Scopes

Scope 1: “READ”

- GET /photos
- GET /photos/{id}

Scopes

Scope 1: “READ”

- GET /photos
- GET /photos/{id}

Scope 2: “UPDATE”

- GET /photos
- GET /photos/{id}
- POST /photos
- PUT /photos/{id}

Scopes

Product Details

Display Name Certification_OAuthAuthCodeGrant

Description OAuth Authorization Code Grant Example For Certification Class

Environment ☒ test ☐ prod

Access Internal only

Key Approval Type Automatic

Quota

Allowed OAuth Scopes READ, UPDATE

OAuth Grant Types

Grant Type	Typical Use Case	Complex?
No specific resource owner is involved		
Client Credentials	Business system interactions, where resources being operated on are owned by the partner, not a particular user	No

OAuth Grant Types

Grant Type	Typical Use Case	Complex?
No specific resource owner is involved		
Client Credentials	Business system interactions, where resources being operated on are owned by the partner, not a particular user	No
A specific resource owner is involved		
Resource Owner Password Credentials	Resources are owned by a particular user and the requesting application is trusted	A bit

OAuth Grant Types

Grant Type	Typical Use Case	Complex?
No specific resource owner is involved		
Client Credentials	Business system interactions, where resources being operated on are owned by the partner, not a particular user	No
A specific resource owner is involved		
Resource Owner Password Credentials	Resources are owned by a particular user and the requesting application is trusted	A bit
Authorization Code	Resources are owned by a particular user and the requesting application is untrusted	Very

OAuth Grant Types

Grant Type	Typical Use Case	Complex?
No specific resource owner is involved		
Client Credentials	Business system interactions, where resources being operated on are owned by the partner, not a particular user	No
A specific resource owner is involved		
Resource Owner Password Credentials	Resources are owned by a particular user and the requesting application is trusted	A bit
Authorization Code	Resources are owned by a particular user and the requesting application is untrusted	Very
Implicit	Resources are owned by a particular user, and the requesting application is an untrusted browser-based app written in a scripting language such as JavaScript	Very complex, and less secure than Auth Code



Thank You

OAuth Review

- Scopes
 - limits the tokens access for a resource