How to develop to be compliant with OAuth 2.1 out of the gate

Nahid Farrokhi – Software Engineer @Microsoft

@nahid_fa

nahidf

Agenda:

- OAuth 2.0
- The future : OAuth 2.1
- Demo
- Question?

Authentication

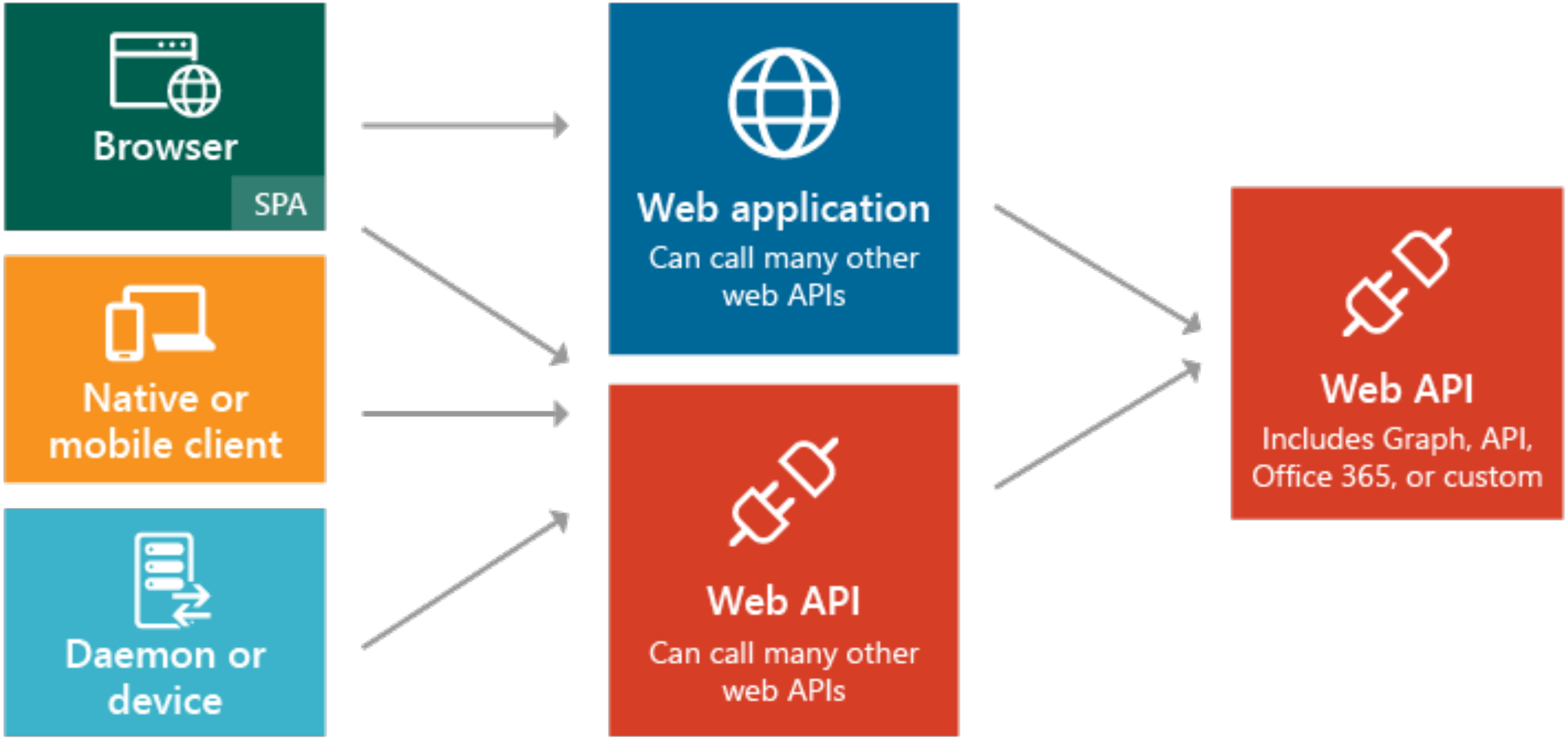
Who you are

OpenID Connect (OIDC)

Authorization

What you can do

OAuth 2.0



Browser

SPA

Native or mobile client

Daemon or device

Web application

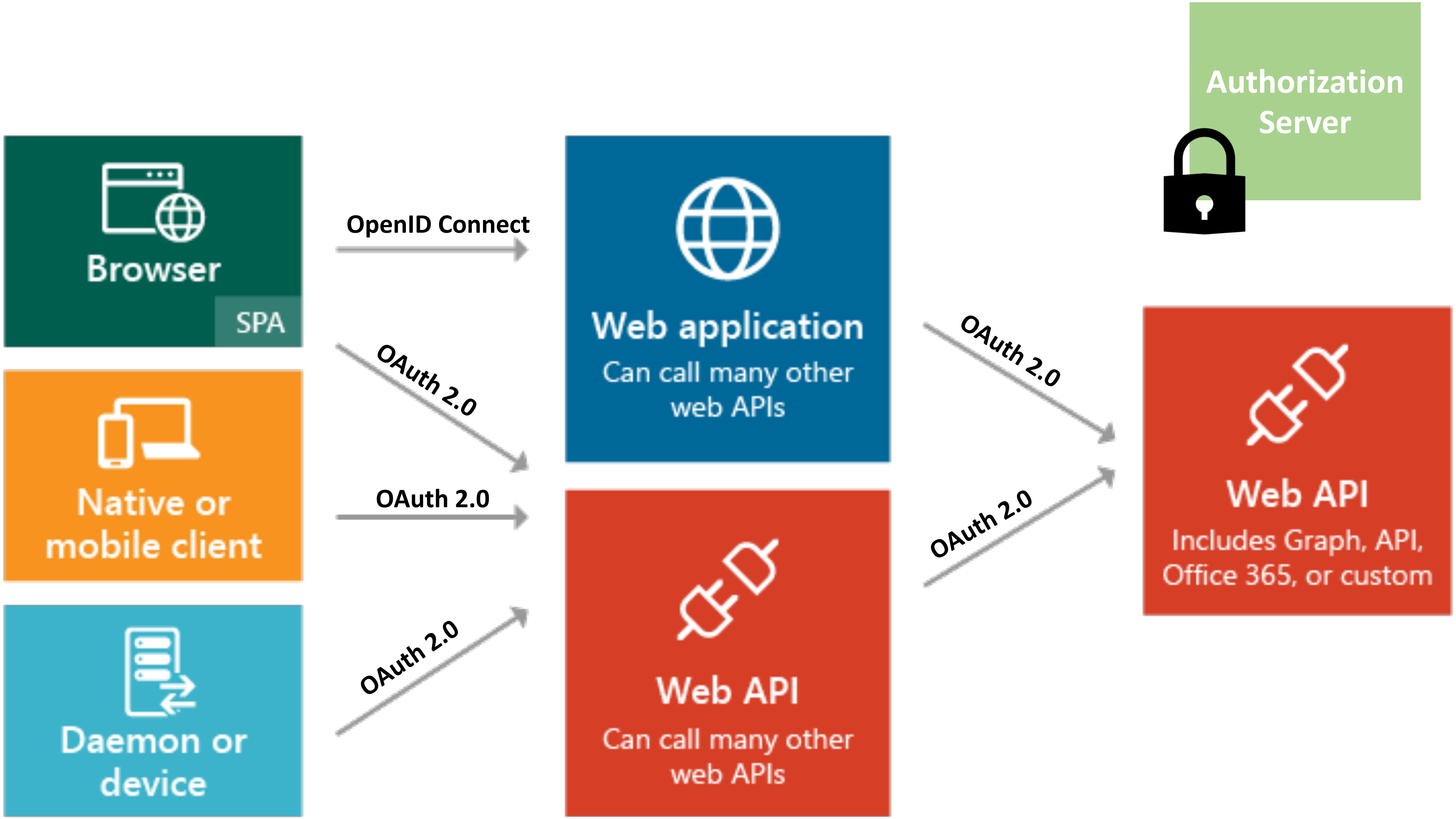
Can call many other web APIs

Web API

Can call many other web APIs

Web API

Includes Graph, API, Office 365, or custom



Authorization Server

Browser

SPA

OpenID Connect

OAuth 2.0

Native or mobile client

OAuth 2.0

Daemon or device

OAuth 2.0

Web application

Can call many other web APIs

Web API

Can call many other web APIs

OAuth 2.0

OAuth 2.0

Web API

Includes Graph, API, Office 365, or custom

Authorization --> OAuth 2.0

OAuth 2.0 Terminology

- Roles
- Client Types
- Scopes & Consent
- Access Token
- Grant Types
- Endpoints
- Refresh Token

○ Resource Owner (RO) – User
○ Client – Application
○ User Agent
○ Resource Server (RS) - API
○ Authorization Server(AS)

OAuth 2.0 Terminology

- Roles
- Client Types
- Scopes & Consent
- Access Token
- Grant Types
- Endpoints
- Refresh Token

○ Confidential

○ Public

OAuth 2.0 Terminology

- Roles
- Client Types
- **Scopes & Consent**
- Access Token
- Grant Types
- Endpoints
- Refresh Token

```
"scope":
[
    "order.write",
    ”order.delete",
    "order.read",
    "invoice.read "
]
```

OAuth 2.0 Terminology

- Roles
- Client Types
- Scopes & Consent
- **Access Token**
- Grant Types
- Endpoints
- Refresh Token

OAuth 2.0 Terminology

- Roles
- Client Types
- Scopes & Consent
- Access Token
- Grant Types
  - Client Credentials
  - *Authorization Code*
  - Proof Key for Code Exchange(PKCE)
  - *Password*
  - *Implicit*
- Endpoints
- Refresh Token

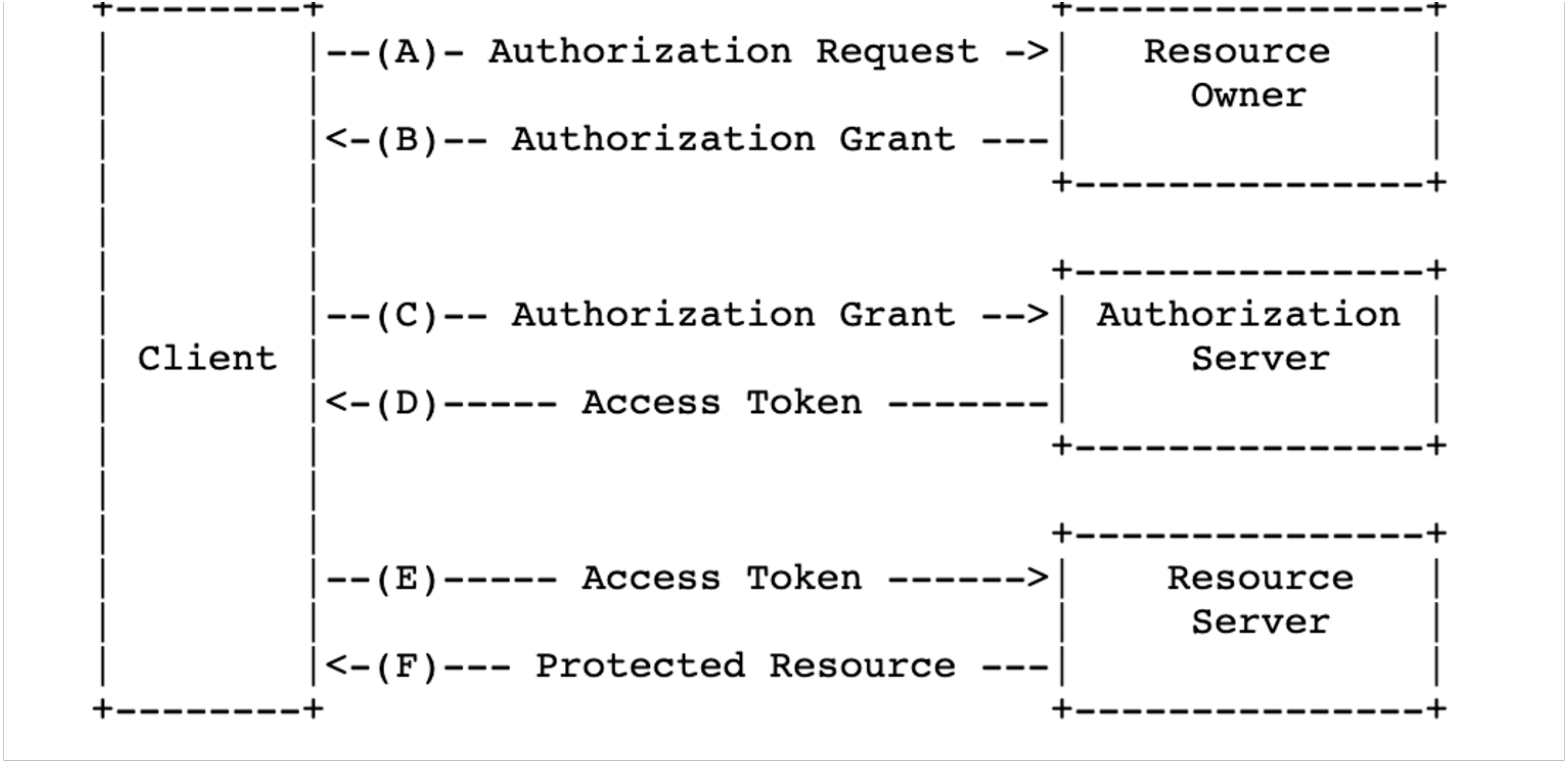
OAuth 2.0 Terminology

- Roles
- Client Types
- Scopes & Consent
- Access Token
- Grant Types
- Endpoints
- Refresh Token

- Authorization Endpoint
- Token Endpoint

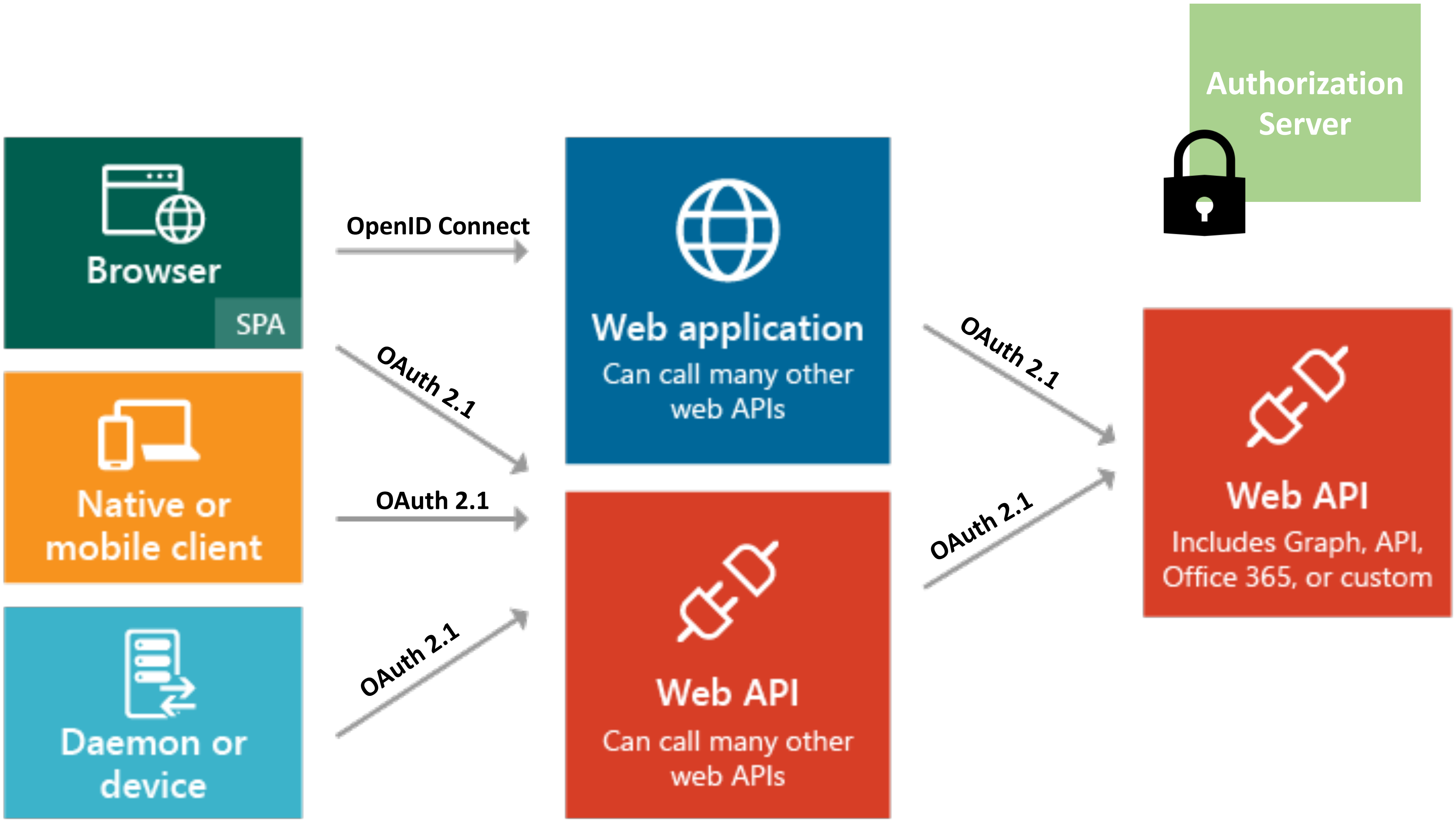
OAuth 2.0 Terminology

- Roles
- Client Types
- Scopes & Consent
- Access Token
- Grant Types
- Endpoints
- Refresh Token



```
+--------+                               +---------------+
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(C)-- Authorization Grant -->| Authorization |
| Client |                               |     Server    |
|        |<-(D)----- Access Token -------|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(E)----- Access Token ------>|    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
+--------+                               +---------------+
```

OAuth 2.1



Authorization Server

Browser

SPA

OpenID Connect

Native or mobile client

OAuth 2.1

OAuth 2.1

Daemon or device

OAuth 2.1

Web application

Can call many other web APIs

Web API

Can call many other web APIs

OAuth 2.1

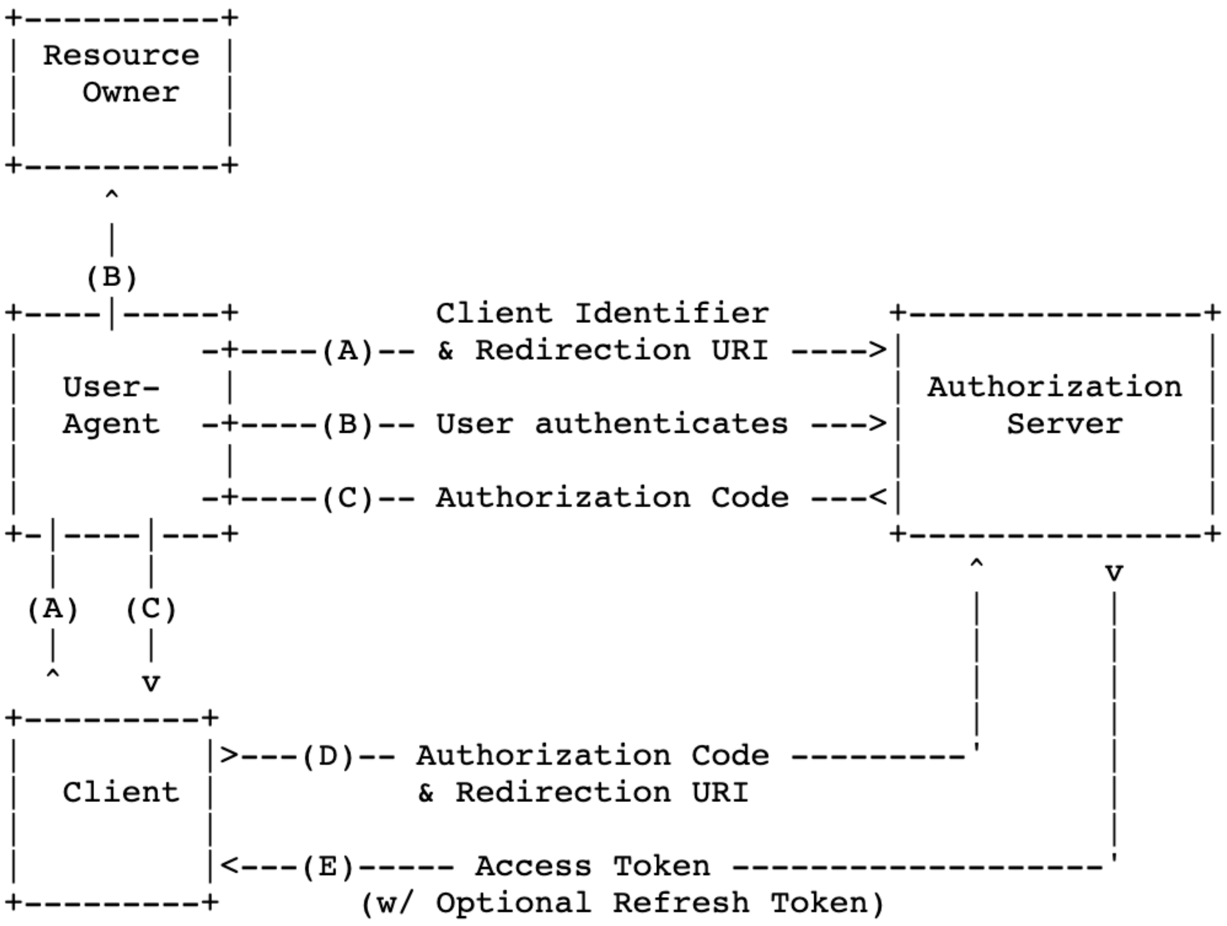
OAuth 2.1

Web API

Includes Graph, API, Office 365, or custom

PKCE is required for all OAuth clients using the authorization code flow

Authorization Code Grant



```
+----------+
| Resource |
|   Owner  |
|          |
+----------+
     ^
     |
    (B)
+----|-----+          Client Identifier      +---------------+
|         -+----(A)-- & Redirection URI ---->|               |
|  User-   |                                 | Authorization |
|  Agent  -+----(B)-- User authenticates --->|     Server    |
|          |                                 |               |
|         -+----(C)-- Authorization Code ---<|               |
+-|----|---+                                 +---------------+
  |    |                                         ^      v
 (A)  (C)                                        |      |
  |    |                                         |      |
  ^    v                                         |      |
+---------+                                      |      |
|         |>---(D)-- Authorization Code ---------'      |
|  Client |          & Redirection URI                  |
|         |                                             |
|         |<---(E)----- Access Token -------------------'
+---------+       (w/ Optional Refresh Token)
```

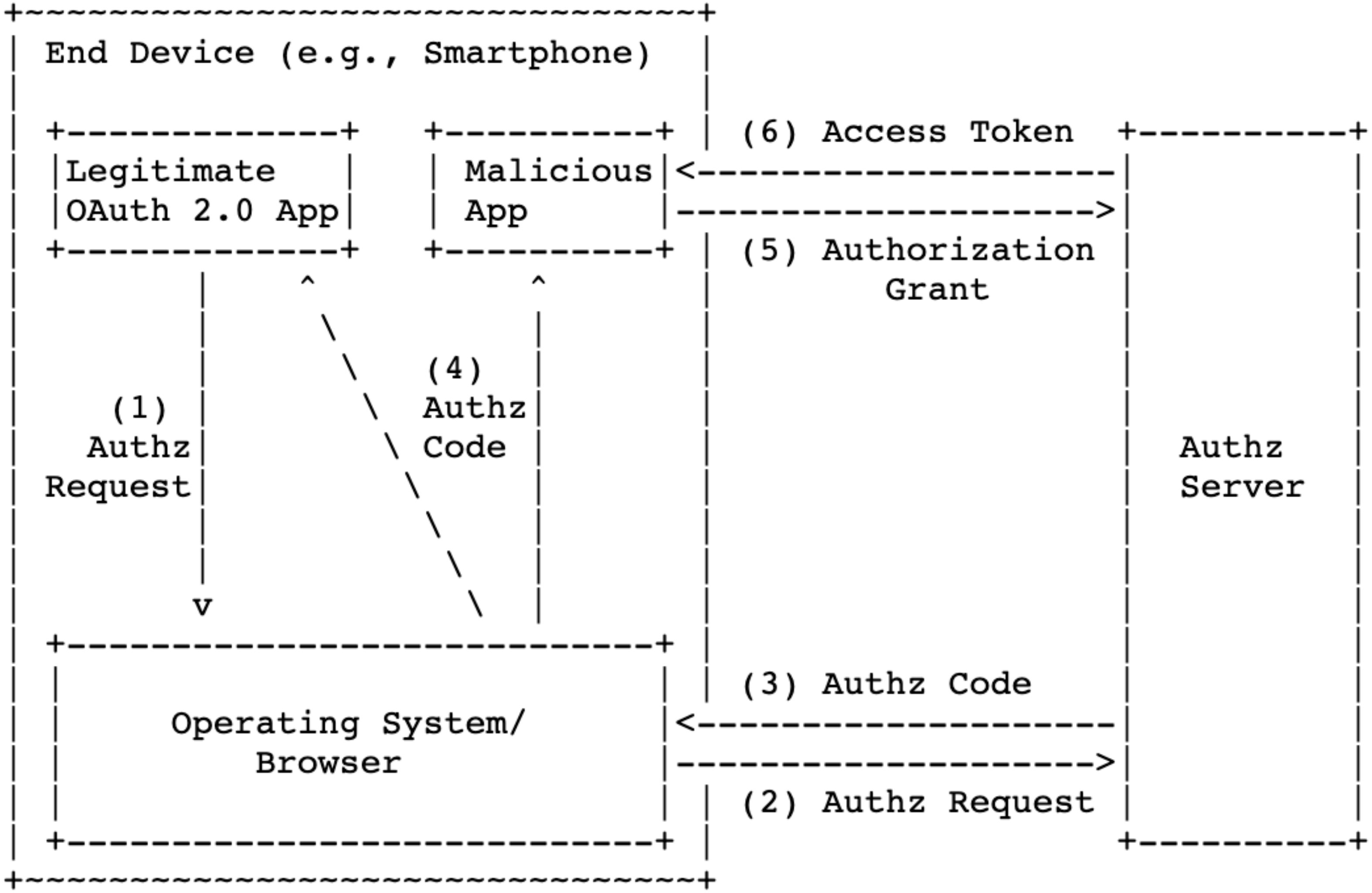
```
https://authorization-server.com/auth
?response_type=code &client_id= xxxxxxxxxx
&redirect_uri=https://example-app.com/redirect
&scope=create+delete
&state=xcoiv98y2kd22vusuye3kch
```

```
https://example-app.com/redirect
?code=g0ZGZmNjVmOWIjNTk2NTk4ZTYyZGI3
&state=xcoiv98y2kd22vusuye3kch
```

```
POST /oauth/token HTTP/1.1
Host: authorization-server.com

grant_type=authorization_code
&code=xxxxxxxxxxx
&redirect_uri=https://example-app.com/redirect
&client_id=xxxxxxxxxx
&client_secret=xxxxxxxxxx
```

@nahid_fa

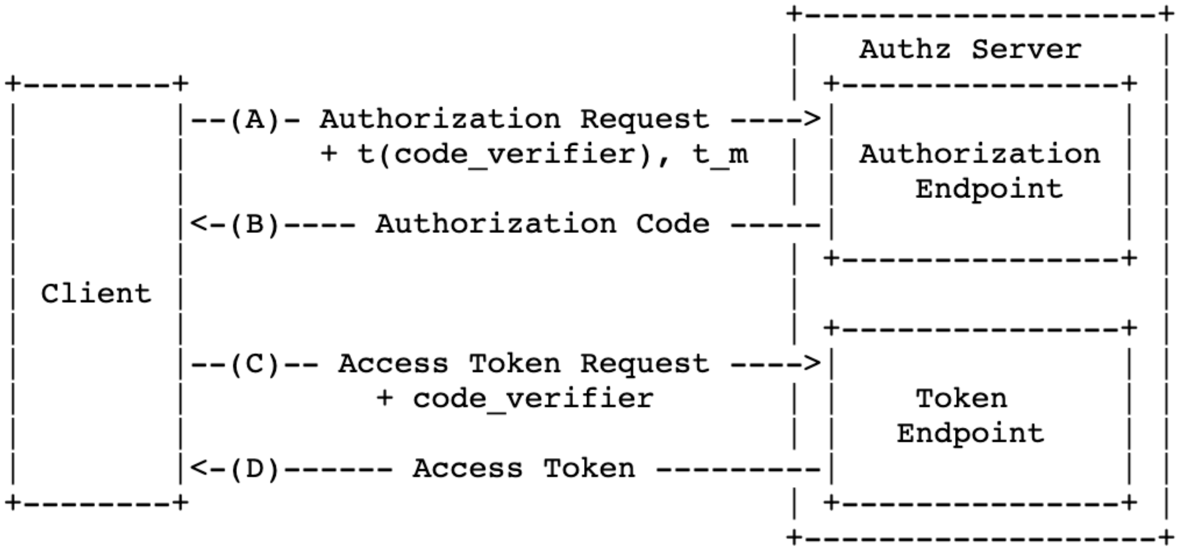
Authorization Code Interception Attack



```
+~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~+
| End Device (e.g., Smartphone)  |
|                                 |
| +-------------+   +----------+  | (6) Access Token  +----------+
| |Legitimate   |   | Malicious|<--------------------|          |
| |OAuth 2.0 App|   | App      |-------------------->|          |
| +-------------+   +----------+  | (5) Authorization |          |
|        |    ^          ^        |        Grant      |          |
|        |     \         |        |                   |          |
|        |      \   (4)  |        |                   |          |
|    (1) |       \  Authz|        |                   |          |
|   Authz|        \ Code |        |                   |  Authz   |
| Request|         \     |        |                   |  Server  |
|        |          \    |        |                   |          |
|        |           \   |        |                   |          |
|        v            \  |        |                   |          |
| +----------------------------+  |                   |          |
| |                            |  | (3) Authz Code    |          |
| |     Operating System/      |<--------------------|          |
| |         Browser            |-------------------->|          |
| |                            |  | (2) Authz Request |          |
| +----------------------------+  |                   +----------+
+~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~+
```

Authorization Code Injection Attack

Proof Key for Code Exchange



```
                                          +-------------------+
                                          |   Authz Server    |
+--------+                                | +---------------+ |
|        |--(A)- Authorization Request ---->|               | |
|        |       + t(code_verifier), t_m  | | Authorization | |
|        |                                | |    Endpoint   | |
|        |<-(B)---- Authorization Code -----|               | |
|        |                                | +---------------+ |
| Client |                                |                   |
|        |                                | +---------------+ |
|        |--(C)-- Access Token Request ---->|               | |
|        |          + code_verifier       | |    Token      | |
|        |                                | |   Endpoint    | |
|        |<-(D)------ Access Token ---------|               | |
+--------+                                | +---------------+ |
                                          +-------------------+
```

Provider + /oauth/redirect?

client_id={client_id} &
redirect_uri={Callback URL} &
scope={Scope} &
response_type=code &
state={random long string} &
code_challenge={code challenge} &
code_challenge_method=SHA256

POST Provider + /oauth/access_token
Request body:

```
{
   client_id:{client_id},
   client_secret:{client_secret},
   redirect_uri:{redirect_uri},
   response_type:token,
   Code:{code}
   code_verifier: {code verifier}
}
```

Redirect URIs must be compared using exact string matching

Return URL:

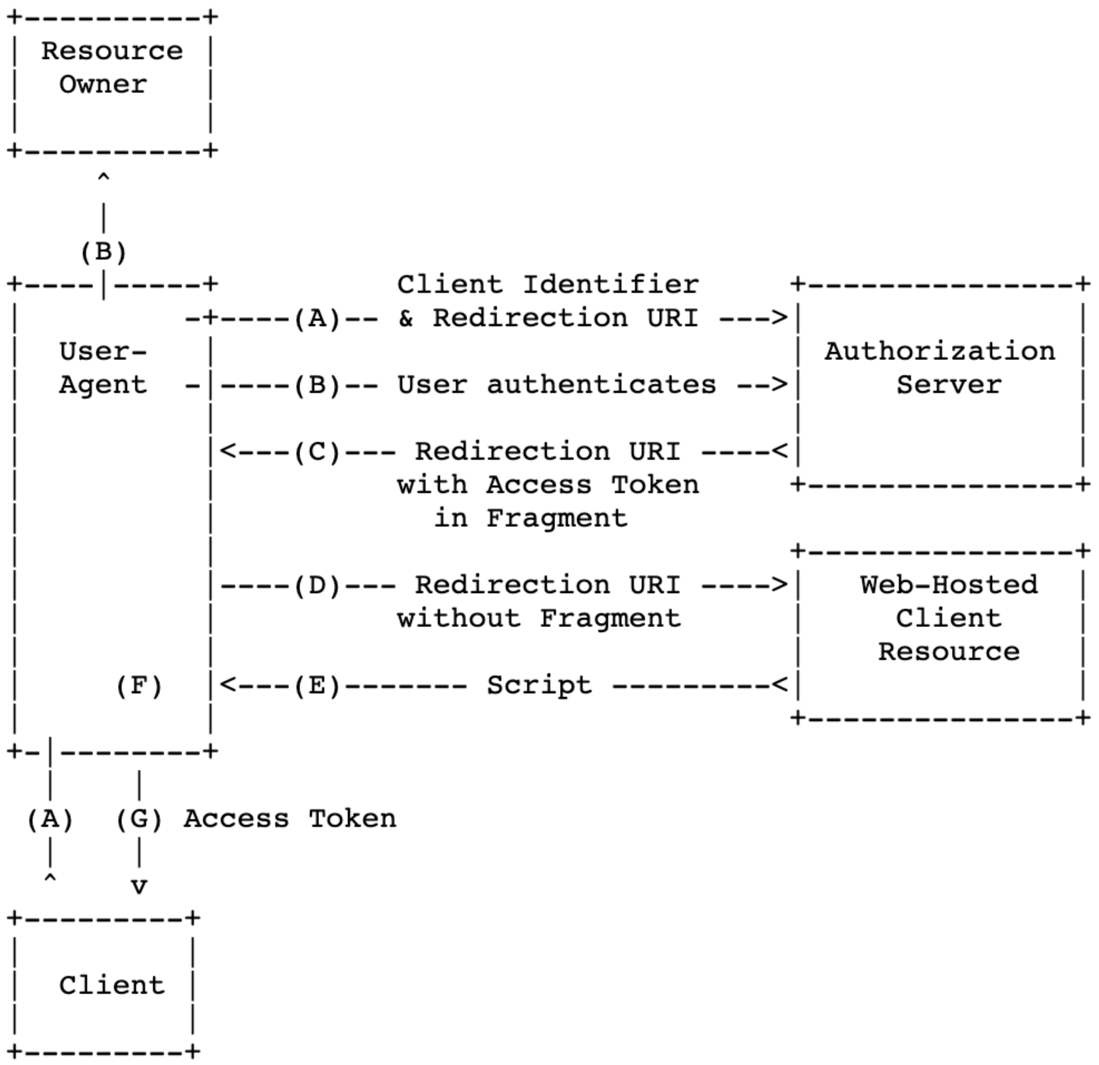
Registered: https://*.somesite.example/*

Valid: https://app1.somesite.example/redirect

Attack: https://attacker.example/.somesite.example

The Implicit grant (response_type=token) is omitted from this specification

Implicit Grant



```
+----------+
| Resource |
|  Owner   |
|          |
+----------+
     ^
     |
    (B)
+----|-----+          Client Identifier     +---------------+
|         -+----(A)-- & Redirection URI --->|               |
|  User-   |                                | Authorization |
|  Agent  -|----(B)-- User authenticates -->|     Server    |
|          |                                |               |
|          |<---(C)--- Redirection URI ----<|               |
|          |          with Access Token     +---------------+
|          |            in Fragment
|          |                                +---------------+
|          |----(D)--- Redirection URI ---->|   Web-Hosted  |
|          |          without Fragment      |     Client    |
|          |                                |    Resource   |
|     (F)  |<---(E)------- Script ---------<|               |
|          |                                +---------------+
+-|--------+
  |    |
 (A)  (G) Access Token
  |    |
  ^    v
+---------+
|         |
|  Client |
|         |
+---------+
```

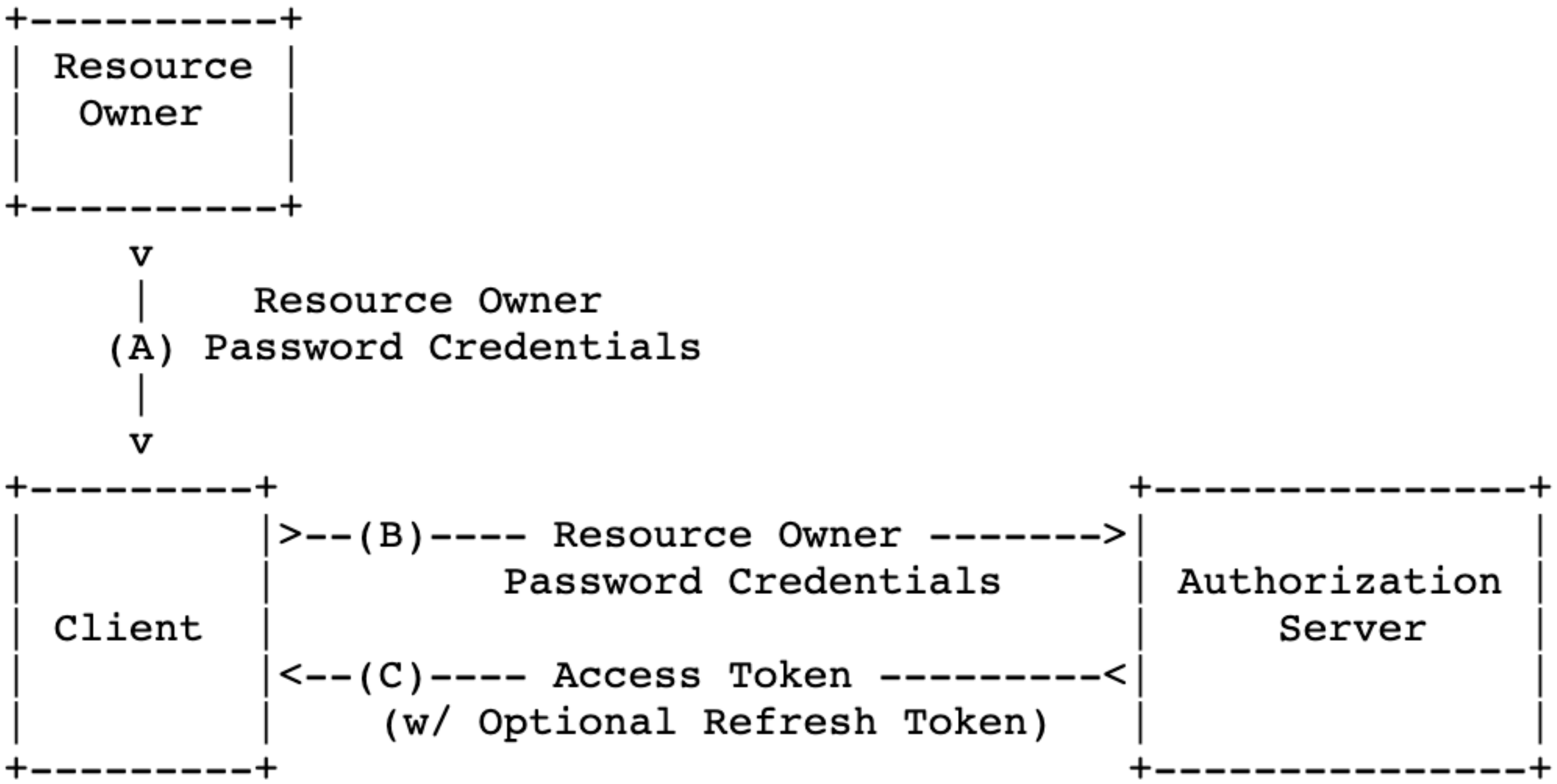
https://authorization-server.com/auth
?response_type=token & client_id= xxxxxxxxxx
&redirect_uri=https://example-app.com/redirect
&scope=create+delete
&state=xcoiv98y2kd22vusuye3kch

https://example-app.com/redirect
#access_token=g0ZGZmNj4mOWIjNTk2Pw1Tk4ZTYyZGI
3 &token_type=Bearer &expires_in=600
&state=xcoVv98y2kd44vuqwye3kcq

@nahid_fa

The Resource Owner Password Credentials grant is omitted from this specification

Password Grant



```
+----------+
| Resource |
|  Owner   |
|          |
+----------+
     v
     |    Resource Owner
    (A) Password Credentials
     |
     v
+---------+                                  +---------------+
|         |>--(B)---- Resource Owner ------->|               |
|         |         Password Credentials     | Authorization |
| Client  |                                  |     Server    |
|         |<--(C)---- Access Token ---------<|               |
|         |    (w/ Optional Refresh Token)   |               |
+---------+                                  +---------------+
```

```
POST /oauth/token HTTP/1.1
Host: authorization-server.com

grant_type=password
&username=user@example.com
&password=123Password
&client_id=xxxxxxxxxx
&client_secret=xxxxxxxxxx
```

@nahid_fa

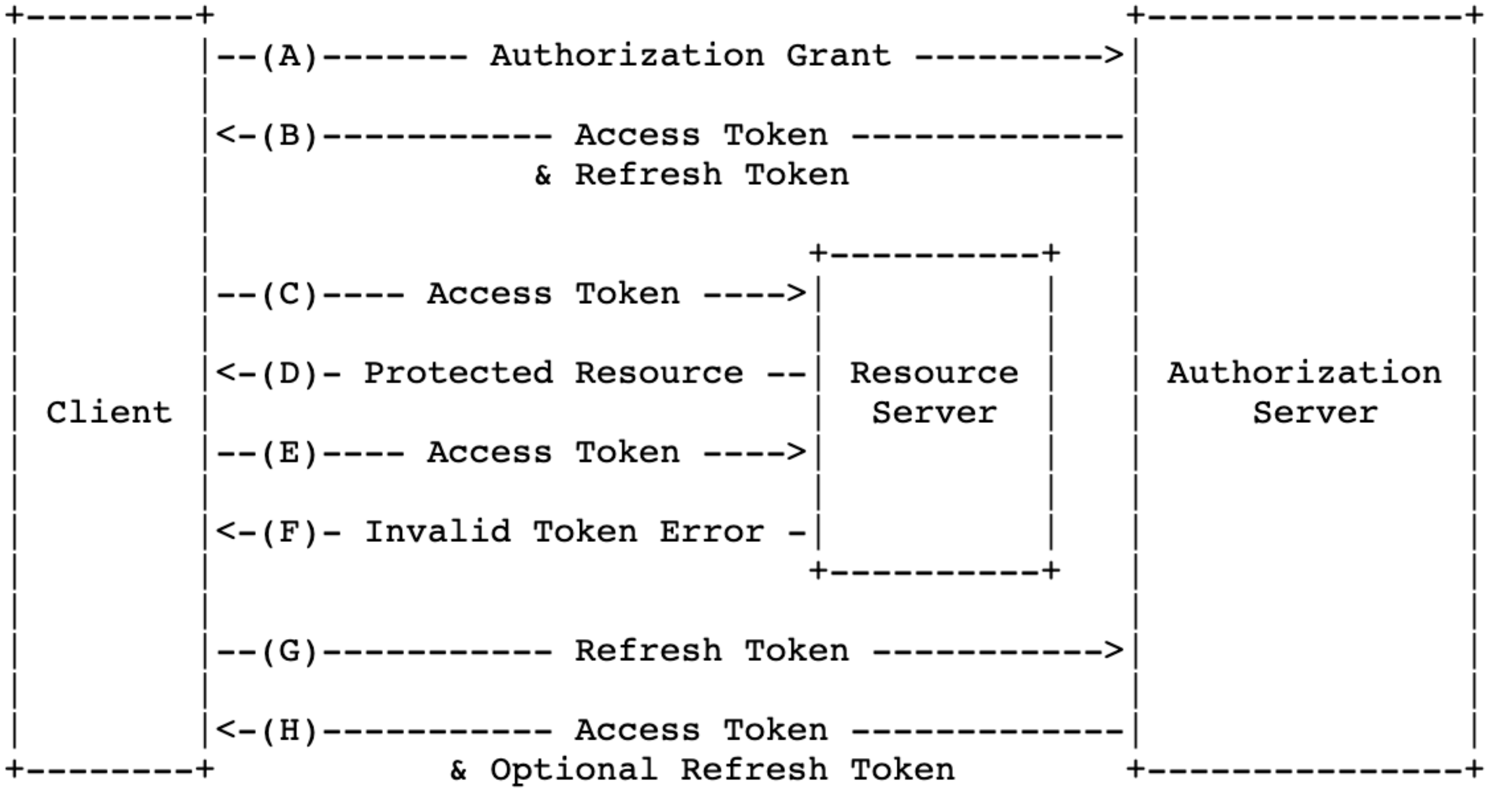
Bearer token usage omits the use of bearer tokens in the query string of URIs

OAuth 2.1 Grant Types

- Client Credentials
- PKCE

Refresh tokens for public clients must either be sender-constrained or one-time use

Refresh Token



```
+--------+                                           +---------------+
|        |--(A)------- Authorization Grant --------->|               |
|        |                                           |               |
|        |<-(B)----------- Access Token -------------|               |
|        |               & Refresh Token             |               |
|        |                                           |               |
|        |                            +----------+   |               |
|        |--(C)---- Access Token ---->|          |   |               |
|        |                            |          |   |               |
|        |<-(D)- Protected Resource --| Resource |   | Authorization |
| Client |                            |  Server  |   |     Server    |
|        |--(E)---- Access Token ---->|          |   |               |
|        |                            |          |   |               |
|        |<-(F)- Invalid Token Error -|          |   |               |
|        |                            +----------+   |               |
|        |                                           |               |
|        |--(G)----------- Refresh Token ----------->|               |
|        |                                           |               |
|        |<-(H)----------- Access Token -------------|               |
+--------+           & Optional Refresh Token        +---------------+
```

```
POST /oauth/token HTTP/1.1
Host: authorization-server.com

grant_type=refresh_token
&refresh_token=xxxxxxxxxxx
&client_id=xxxxxxxxxx
&client_secret=xxxxxxxxxx
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

{
   "access_token": xxxxxxxxxxx,
   "refresh_token":" xxxxxxxxxxx ",
   "token_type":"Bearer",
    "expires_in":3600
}
```

@nahid_fa

1:

```
POST /oauth/token HTTP/1.1
Host: authorization-server.com
Sec-Token-Binding: xxxxxxxxxx

grant_type=authorization_code
&code= xxxxxxxxxx
&code_verifier= xxxxxxxxxx
&client_id=example-native-client-id
```

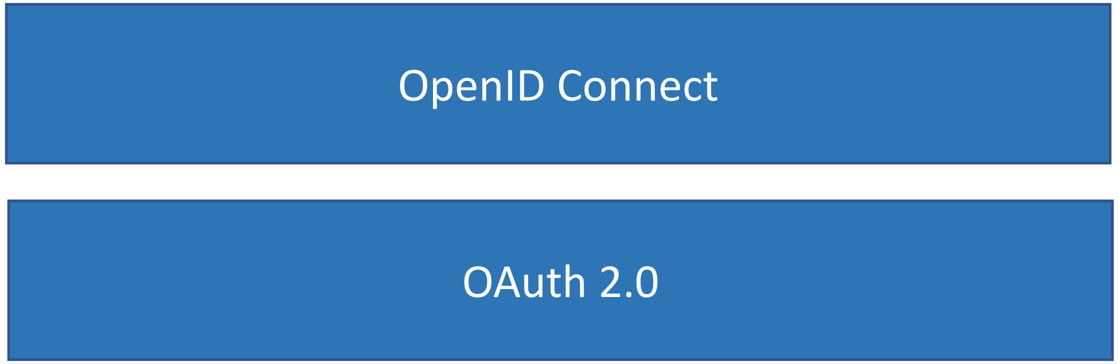
```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

{
    "access_token": xxxxxxxxxxx,
    "refresh_token":" xxxxxxxxxxx ",
    "token_type":"Bearer",
     "expires_in":3600
}
```

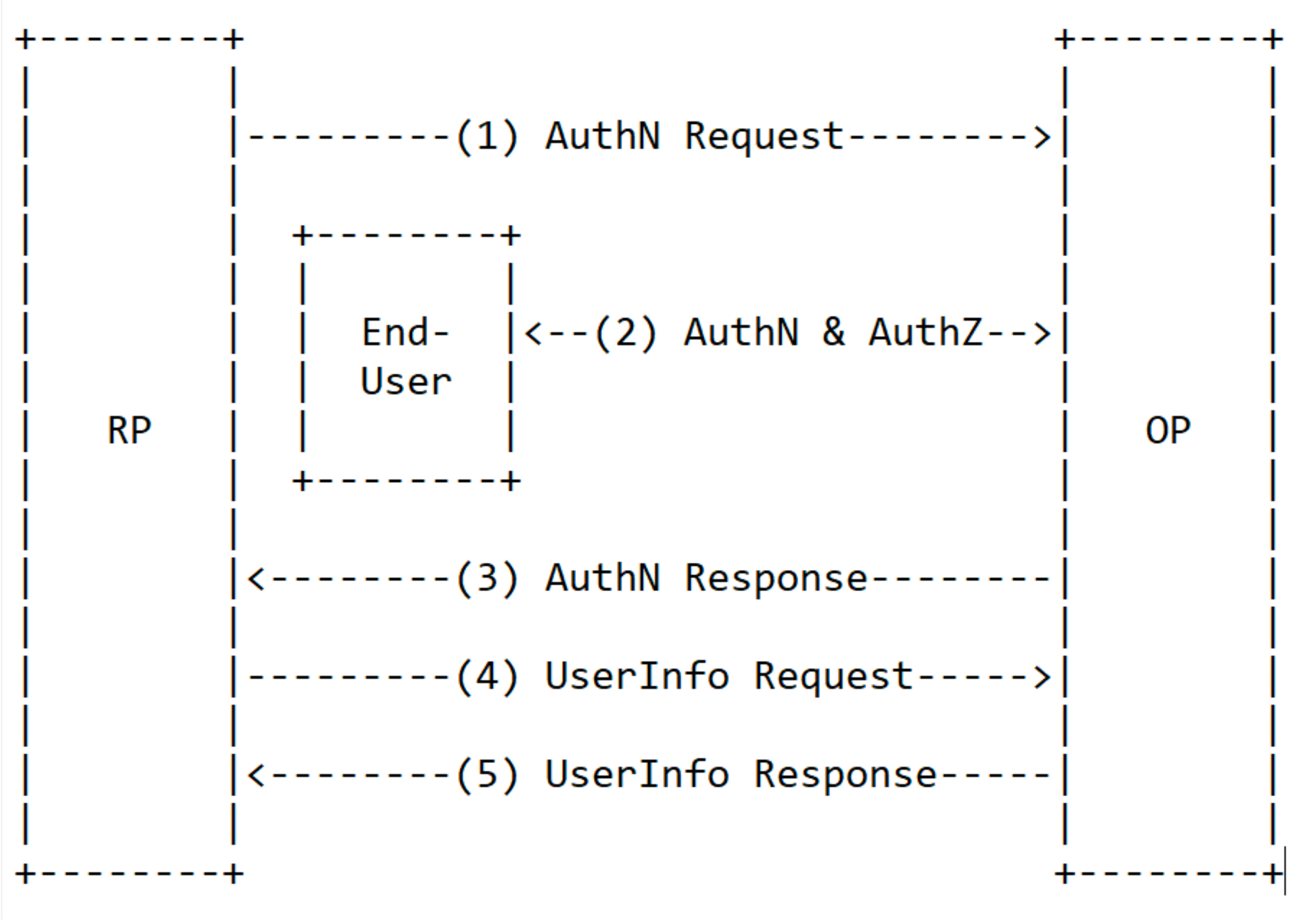
2:

```
POST /oauth/token HTTP/1.1
Host: authorization-server.com
Sec-Token-Binding: xxxxxxxxxx

grant_type=refresh_token
&refresh_token=xxxxxxxxxxx
&client_id=xxxxxxxxxx
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

{
    "access_token": xxxxxxxxxxx,
     "token_type":"Bearer",
     "expires_in":3600
}
```

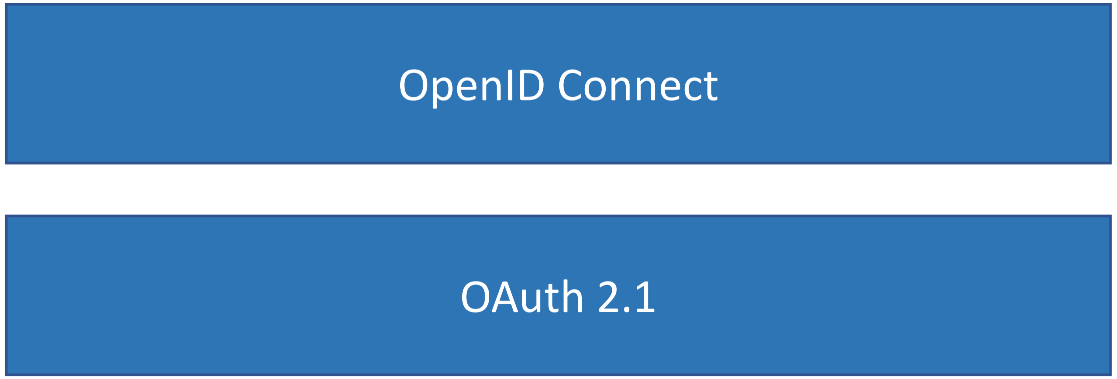
Authentication --> OpenID Connect (OIDC)





```
+--------+                                   +--------+
|        |                                   |        |
|        |---------(1) AuthN Request-------->|        |
|        |                                   |        |
|        |  +--------+                       |        |
|        |  |        |                       |        |
|        |  |  End-  |<--(2) AuthN & AuthZ-->|        |
|        |  |  User  |                       |        |
|   RP   |  |        |                       |   OP   |
|        |  +--------+                       |        |
|        |                                   |        |
|        |<--------(3) AuthN Response--------|        |
|        |                                   |        |
|        |---------(4) UserInfo Request----->|        |
|        |                                   |        |
|        |<--------(5) UserInfo Response-----|        |
|        |                                   |        |
+--------+                                   +--------+
```

@nahid_fa



OpenID Connect
OAuth 2.1

Demo

Question?