



Authentication

Amal Ali
Dana Jayousi

Agenda

1

Authentication and Authorization

2

Basic and Digest Authentication

3

Token Based Authentication and
JWT

4

API Keys

5

OAuth 2.0

6

OpenID

Auth : Authentication and Authorization



Authentication

- Verify that the user are who they claim to be
- Done before Authorization
- “Who are you?”



Authorization

- Detriment authenticated user's permissions
- Done after successful Authentication
- “Are You Allowed to access this resource?”

Basic Authentication

1

Simple and very fast

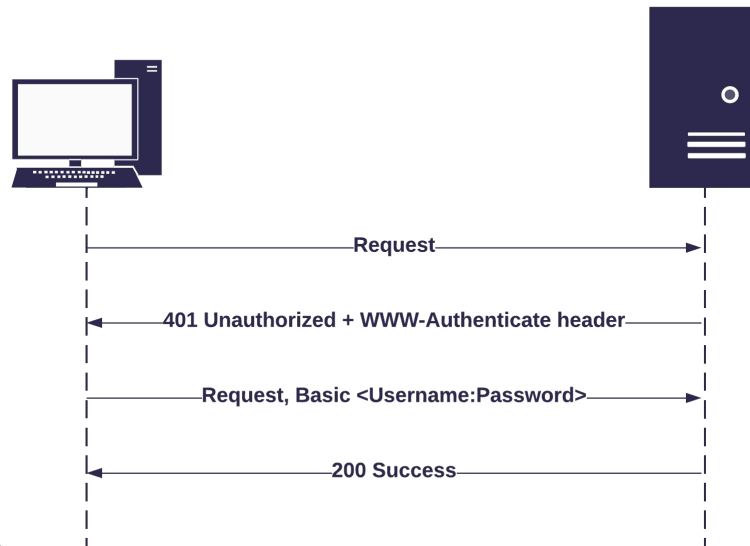
2

Easy to get credentials

3

Must use TLS

Authentication Flow



Digest Authentication

1

No plain text credentials

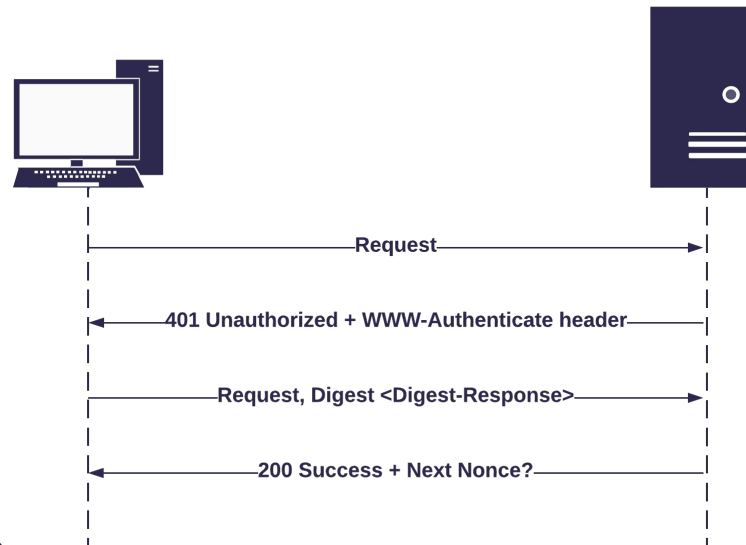
2

Prevents replay attacks

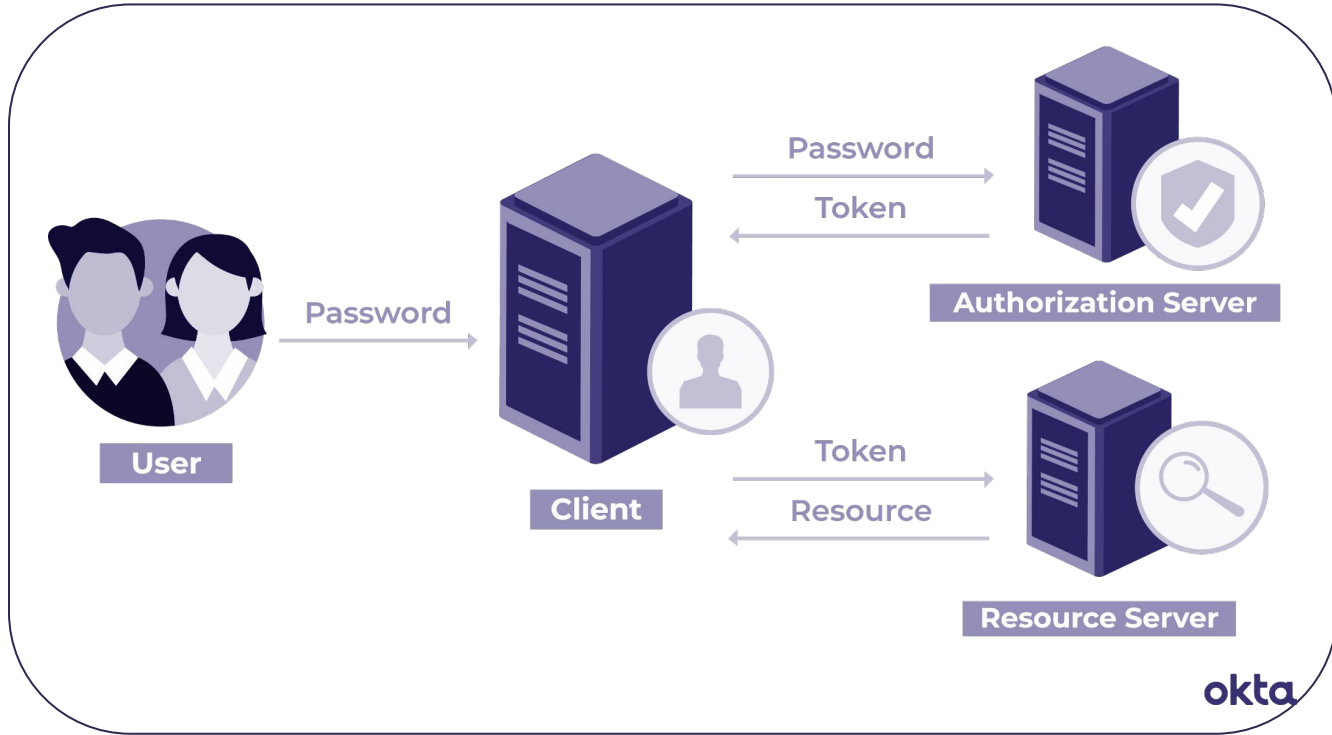
3

Vulnerable to man-in-the-middle attacks

Authentication Flow



Token Based Authentication



JWT: JSON Web Token

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI3NzciLCJuYW1lIjoiaRGFuYSAmIEFtYWwiLCJhZG1pbil6dHJ1ZSviaWF0IjoxNjYzMDY2NDExfQ.MEsuu7ltpRXNgeeSTVd0ZjVeGLlPr5HvgVRQImZ3n7E

Header

Signing algorithm
Token type

Payload

Claims
Info about user

Signature

[JWT Debugger](#)

Token Based Authentication Using JWT

1

Expires, and can be refreshed

2

Stateless

3

No tampering

Authentication Flow



Credentials

JWT

Request, JWT

200 Success

API Keys

1

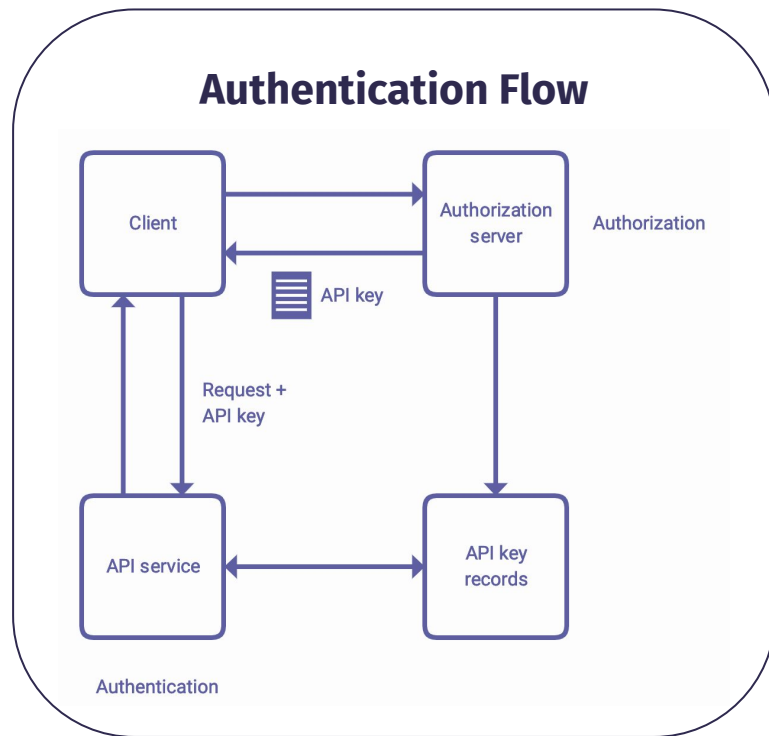
Unique for every user

2

Valid until it's revoked

3

Better to not send it as query parameter



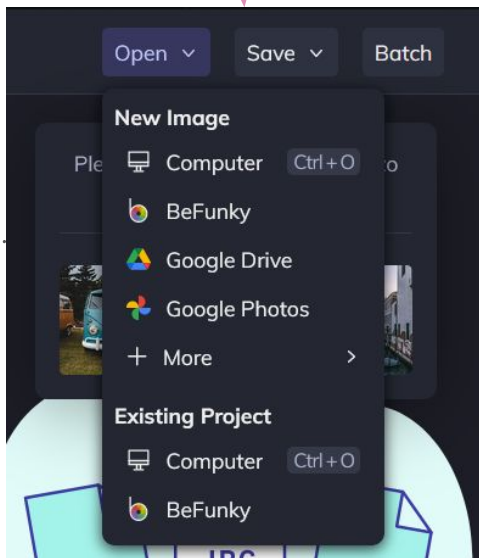
OAuth

OAuth is Short for Open - Authorization, which is an Authorization protocol that allows a third party to gain limited access to another HTTP service, such as Google, Facebook, and GitHub, on behalf of a user, once the user grants permission to access their credentials.

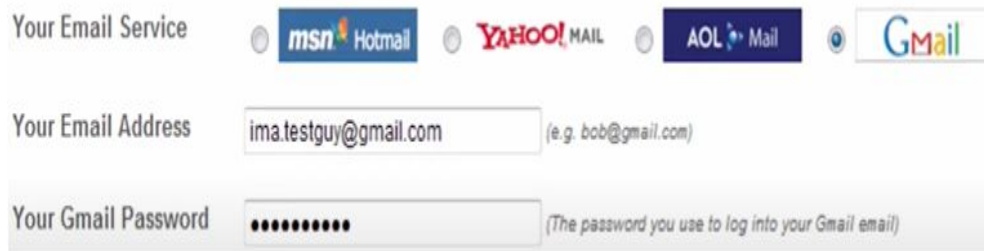


Why OAuth?

To do this

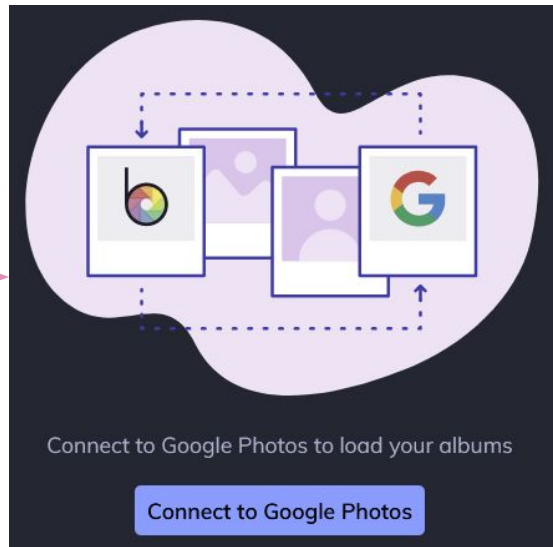
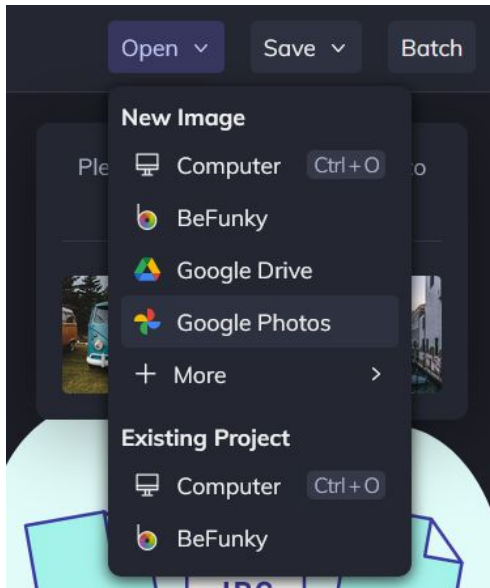


We had to do this

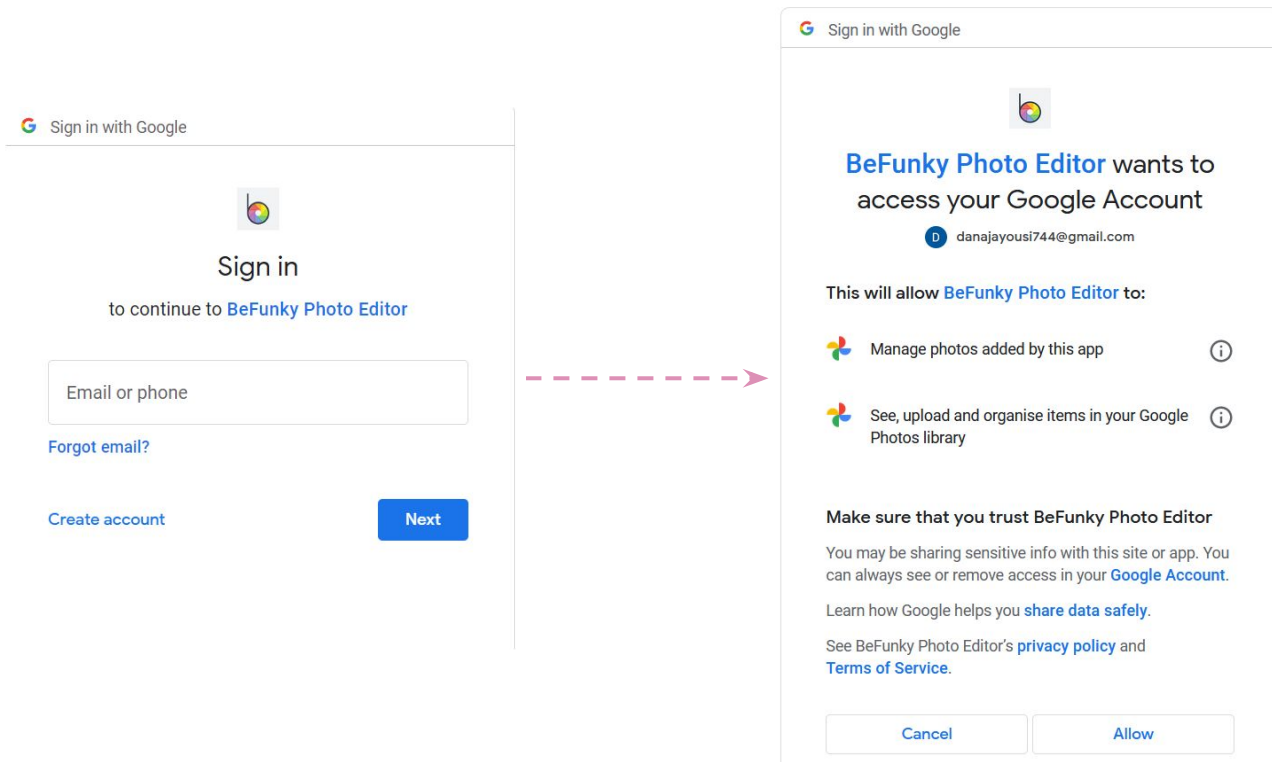


A screenshot of a login form for Gmail. It has three sections: 'Your Email Service' with radio buttons for 'msn Hotmail', 'YAHOO! MAIL', 'AOL Mail', and 'Gmail'; 'Your Email Address' with a text input field containing 'ima.testguy@gmail.com' and a placeholder '(e.g. bob@gmail.com)'; and 'Your Gmail Password' with a password input field containing ten dots and a placeholder '(The password you use to log into your Gmail email)'. A pink dashed arrow points from the text 'We had to do this' to the 'YAHOO! MAIL' radio button.

After OAuth



After OAuth



OAuth

OAuth is about **Access Delegation**



Access Delegation

To give a person
permission to act on
your behalf.

Components Of OAuth

1

Actors



Resource owner



Client



Resource Server

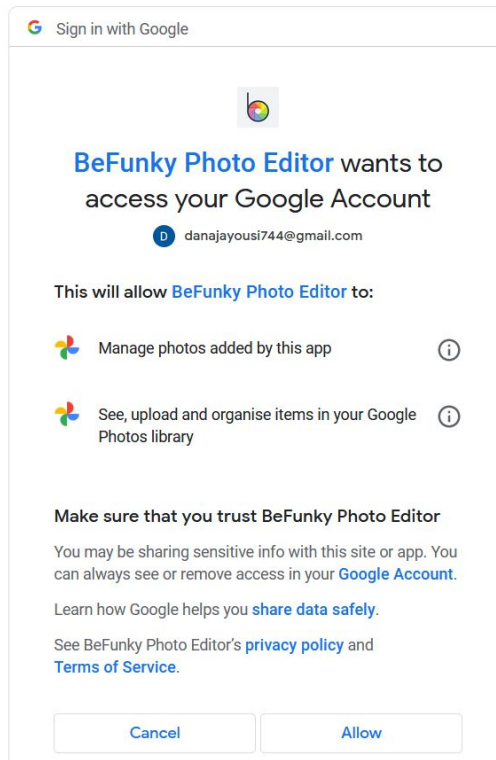


Auth server

Components Of OAuth

2

Scopes and Consents



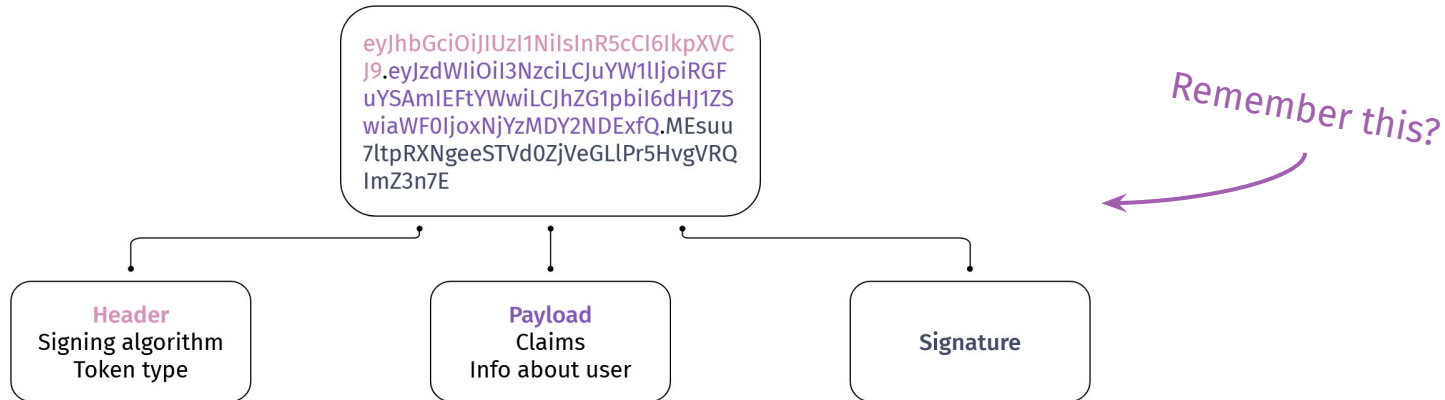
Components Of OAuth

3

Access Token

A token is a piece of data containing just enough information to be able to verify a user's identity or authorize them to perform a certain action.

There is no specific format to use in OAuth but JWT is the most-often used token.



OAuth Workflows

➤ Authorization Code

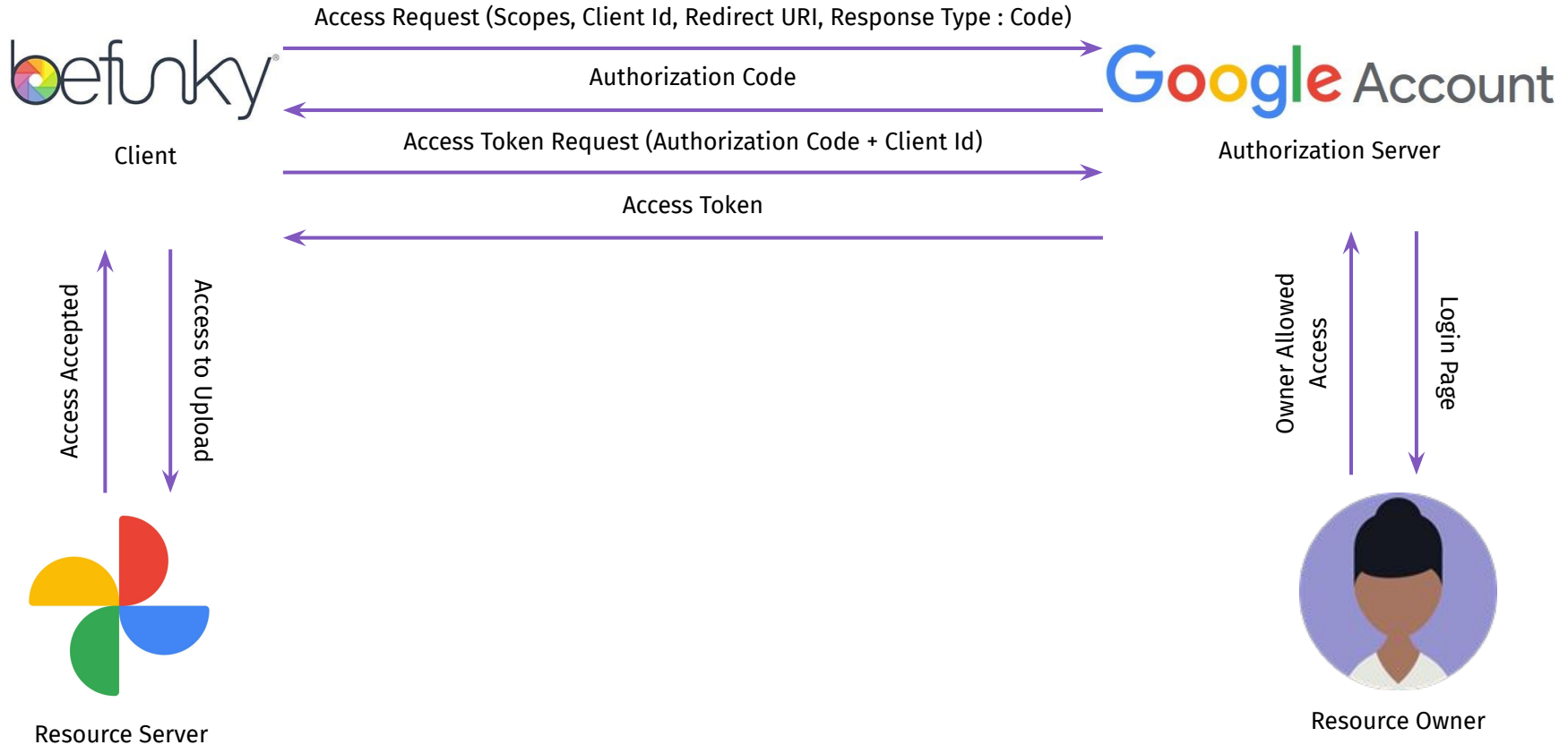
➤ Implicit

➤ Client Credentials

➤ Resource Owner Password Credentials



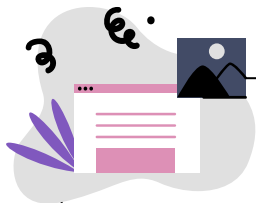
Authorization Code Flow



Implicit Flow



Back Channel & Front Channel



Front Channel

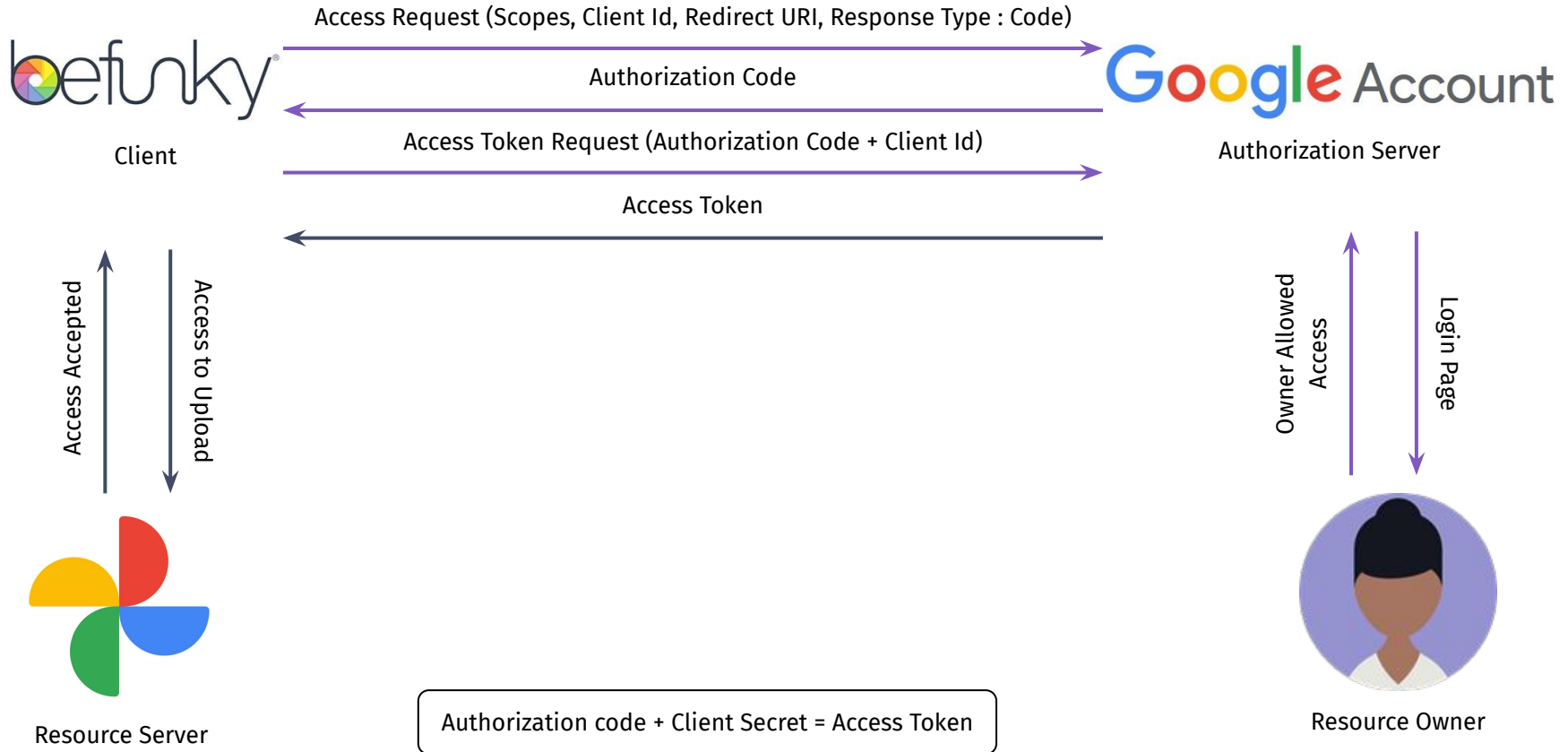
The front channel is a slightly less secure communication channel such as browsers. Anyone can open the developer tool and check out our javascript.



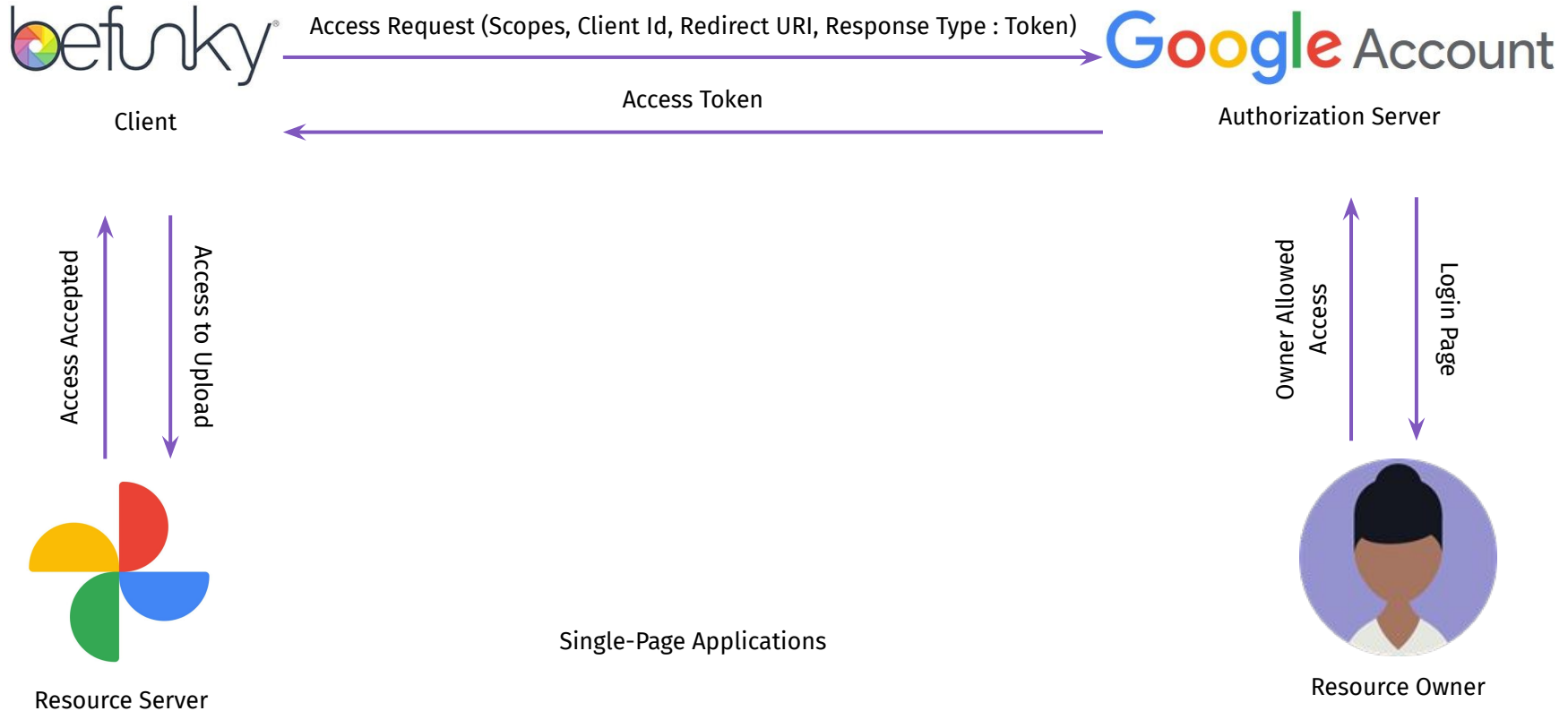
Back Channel

The back channel is a highly secure communication channel. The API request to another server happens using HTTPS.

Authorization Code Flow



Implicit Flow



Client Credentials Flow

1

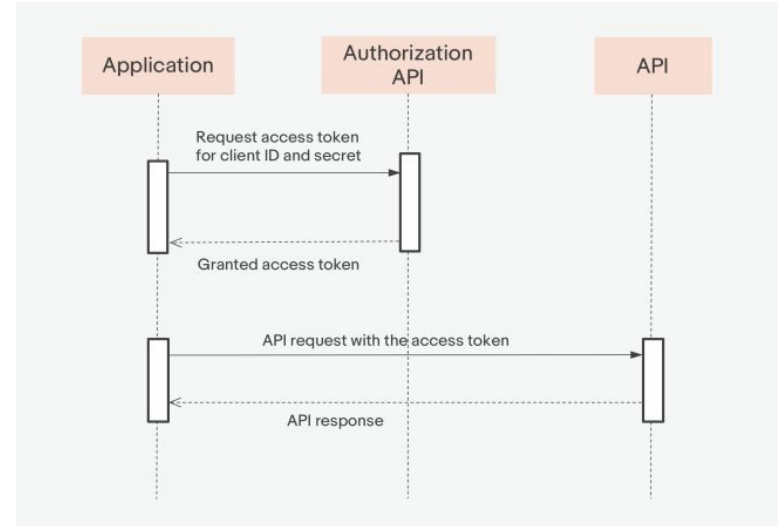
Used in machine-to-machine applications.

2

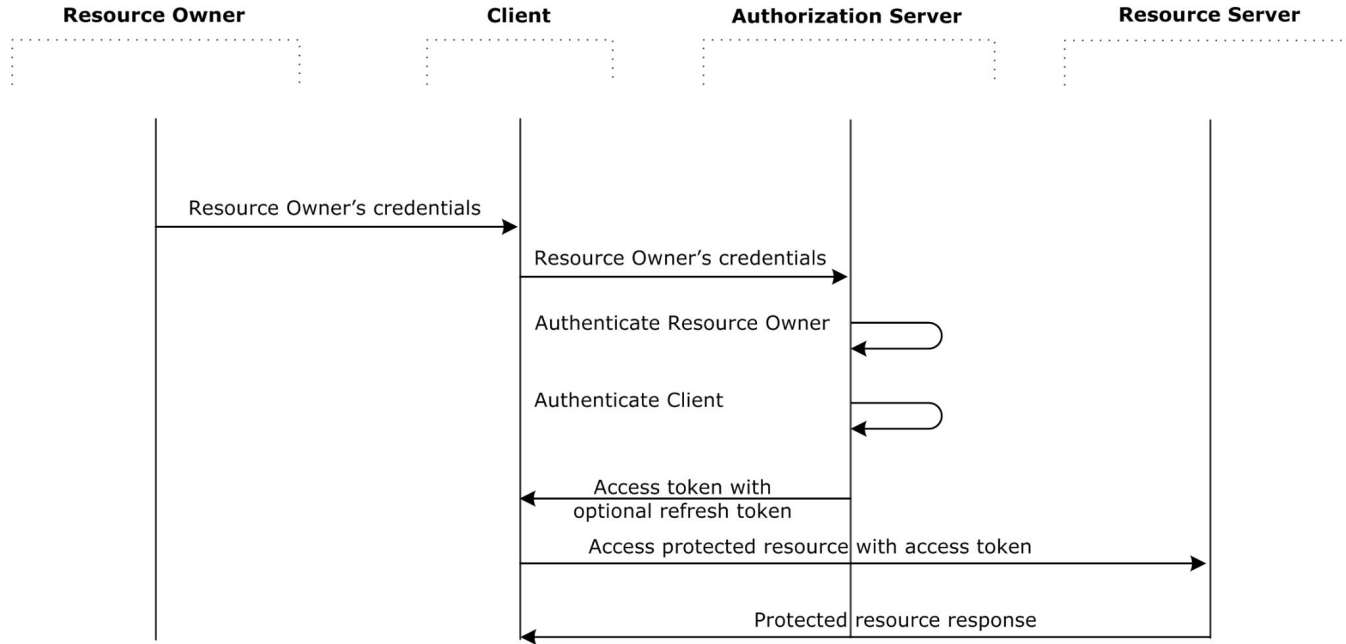
Done in the back channel

3

The system authenticates and authorizes the app rather than a user

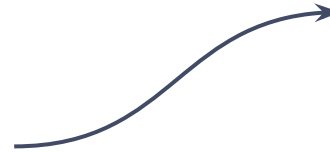
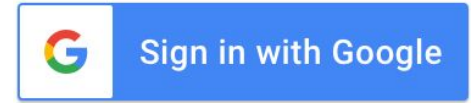


Resource Owner Password Credentials Flow



OAuth in Authentication

- OAuth was invented to make access delegation.
- Now OAuth Is being used in more Purposes. Such as Login and Sign up process.
- But as OAuth is an authorization protocol it can't provide the data needed in such cases. Such as username or email.



OpenID



OpenID

Extension of OAuth which came to solve what OAuth couldn't.

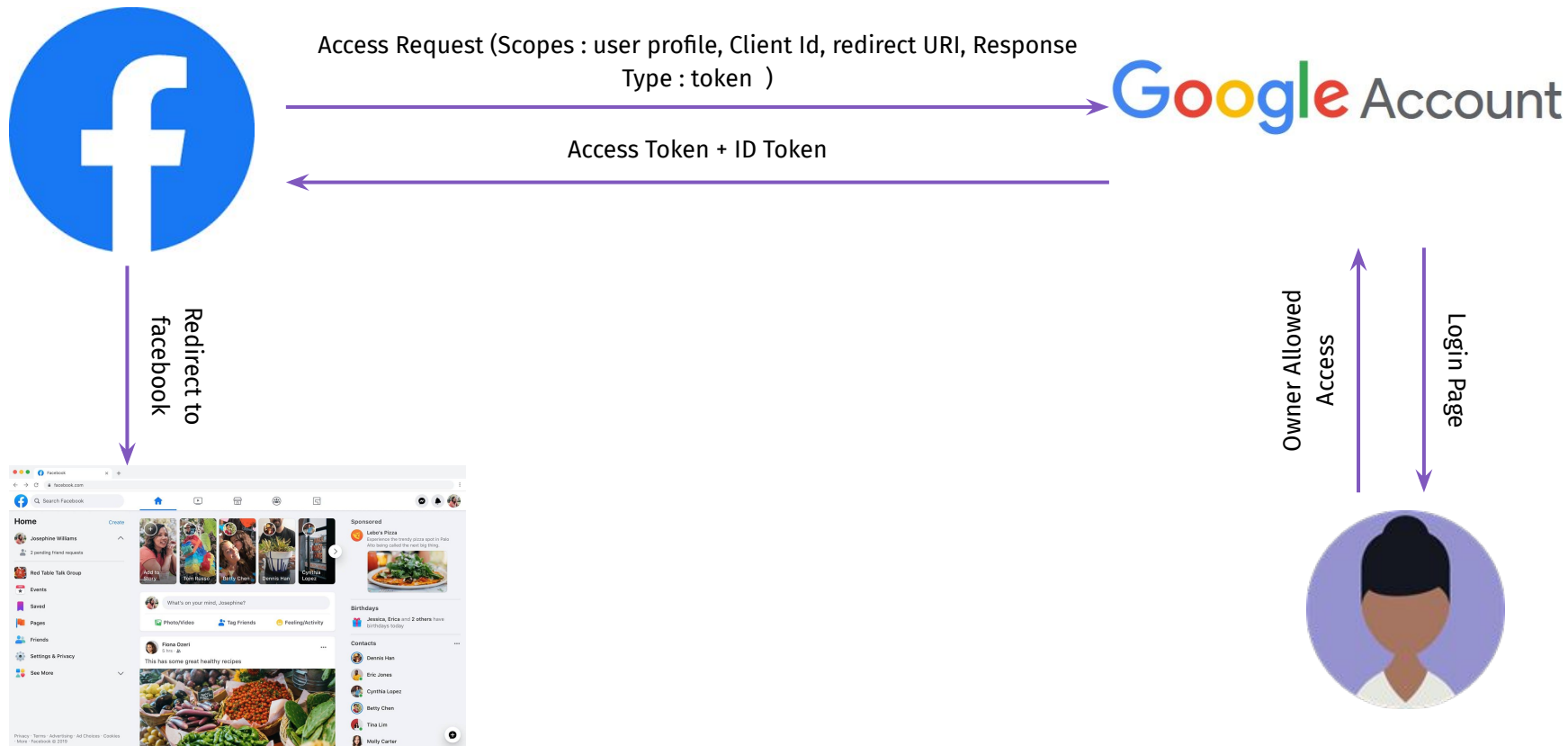
Uses ID token which adds some user information.



OpenID

ID Token is always a JWT token.

OpenID WorkFlow



Resources



[Authentication vs. Authorization](#)

[Authentication on the Web](#)

[HTTP Authentication: Basic and Digest Access Authentication](#)

[Digest access authentication](#)

[What Is Token-Based Authentication?](#)

[Learn what an API key is, how it's used, and how it provides security | Algolia Blog](#)

[What is OAUTH?](#)

- [OAuth & OpenID Connect](#)

Thank You!



Template Credits: [Slidesgo.com](https://www.slidesgo.com)