Understanding Authorization with OAuth2 and OpenID Connect

Kevin Dockx

ARCHITECT

@KevinDockx https://www.kevindockx.com

How OAuth2 Works

authorization request

Authorization Server

Client application
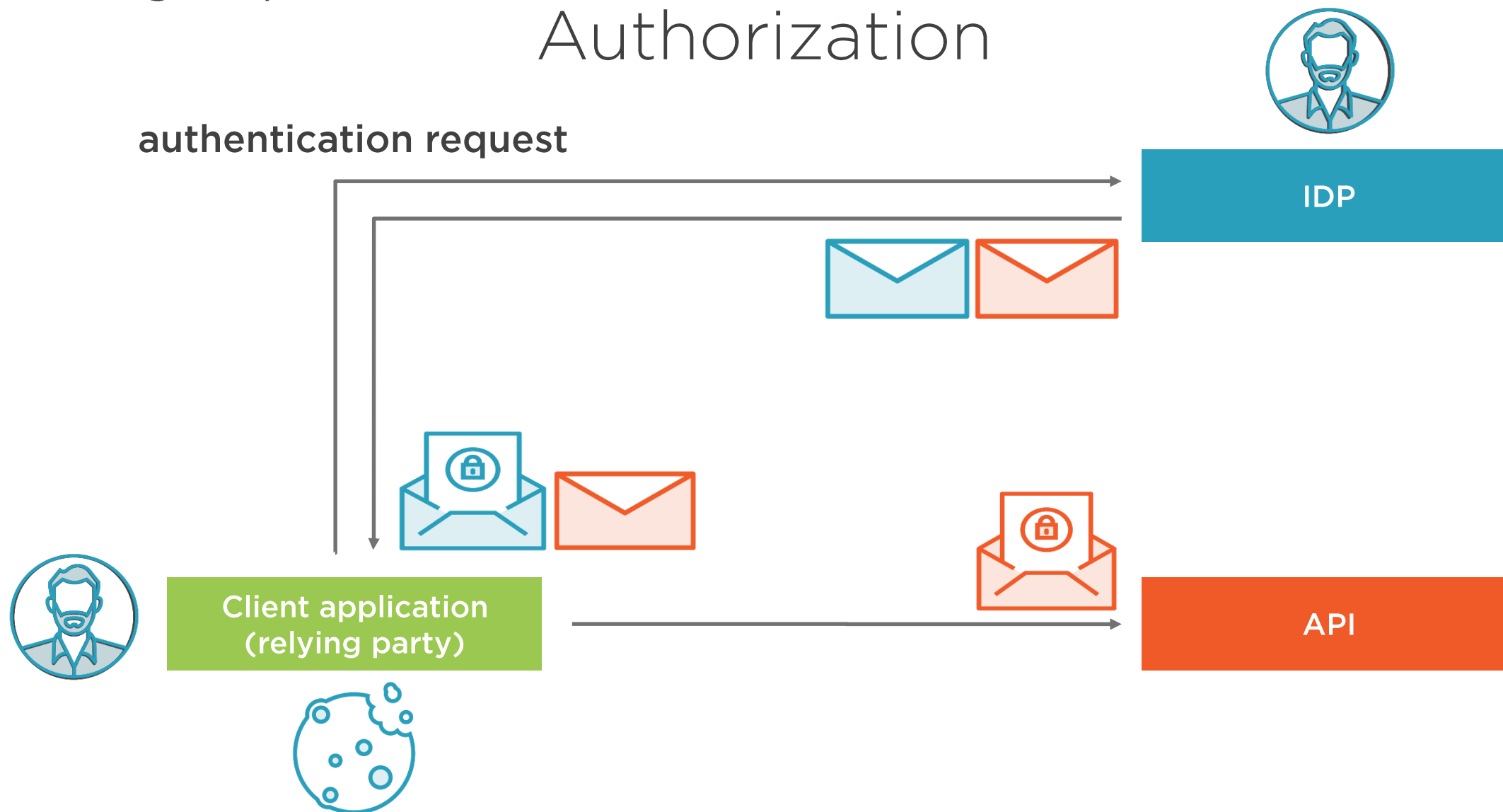(relying party)

API

Why OpenID Connect Is Preferred Over OAuth2
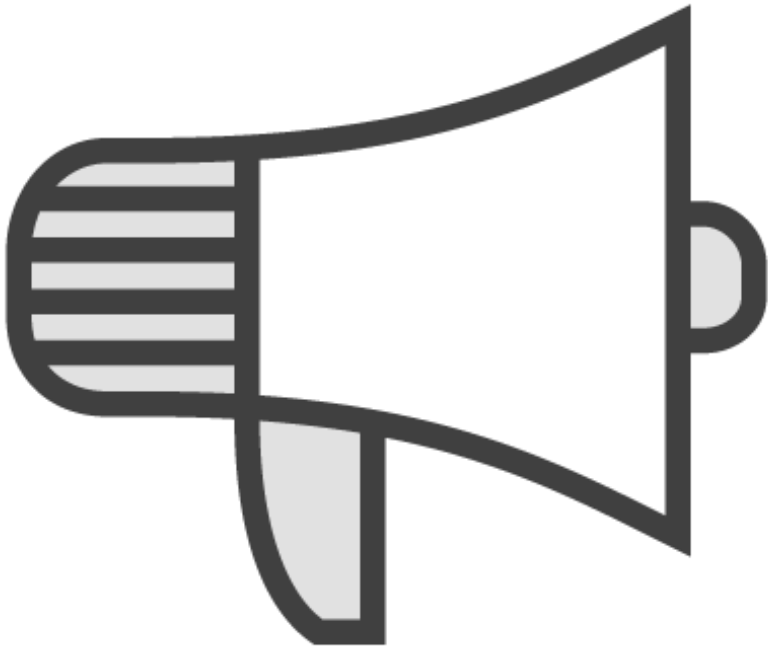
Identity token can be linked to access token (at_hash)

Identity token can be verified first

Using OpenID Connect for Authentication and Authorization

authentication request

IDP

Client application
(relying party)

API

OAuth2 and OpenID Connect Flows

Authorization Code

Tokens from token endpoint

Confidential clients

Long-lived access

Implicit

Tokens from authorization endpoint

Public clients

No long-lived access

Hybrid (OIDC only)

Tokens from authorization endpoint & token endpoint

Confidential clients

Long-lived access

OAuth2 and OpenID Connect Flows

**Resource Owner
Password Credentials
(OAuth2 only)**

In-app login screen

Only for trusted applications

Should be avoided

**Client Credentials
(OAuth2 only)**

No user involvement

Confidential clients

For machine to machine
communication

```
{
  "sub": "b7539694-97e7-4dfe-84da-b4256e1ff5c7",
  "iss": "https://localhost:44303",
  "aud": [
    "imagegalleryapi",
    "https://localhost:44303/resources"],
  …
}
```

Inspecting an Access Token

Access tokens are often JWTs, but don't have to be (eg: reference tokens)

```
{
  "sub": "b7539694-97e7-4dfe-84da-b4256e1ff5c7",
  "iss": "https://localhost:44303",
  "aud": [
    "imagegalleryapi",
    "https://localhost:44303/resources"],
  …
}
```

Inspecting an Access Token

The intended audience

- Our image gallery API
- Resources at level of the IDP (eg when calling the UserInfo endpoint)

```
{ …
  "client_id": "imagegalleryclient",
  "nbf": 1491235799,
  "exp": 1491235869,
  "auth_time": 1491235794,

  …
}
```

Inspecting an Access Token

The client identifier signifies the client application that requested the access token

```
{ …
  "scope": [
    "openid",
    "imagegalleryapi",
    "profile"],
  "amr": ["pwd"]
}
```

Inspecting an Access Token

The scopes in this token give access to API resources and Identity resources

Summary

Use OIDC for authentication and authorization, as it's the superior protocol

The Hybrid Flow is advised for confidential applications

OAuth2-only flows

ROPC should be avoided

Client Credentials is for machine to machine communication