Understanding Authorization with OpenID Connect

Kevin Dockx
Architect

@KevinDockx https://www.kevindockx.com

Coming Up

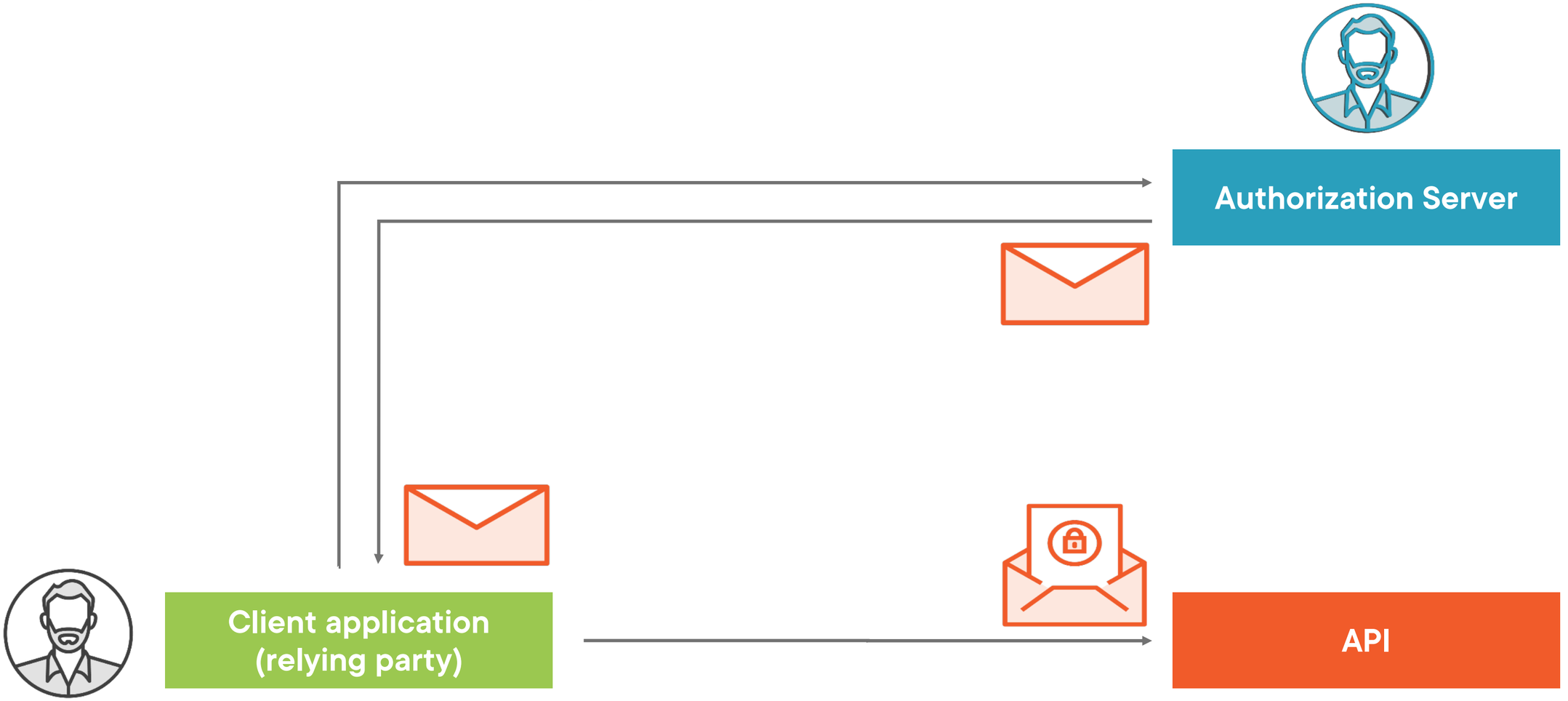
Learning how OAuth2 works

Using OpenID Connect for authentication and authorization

OIDC/OAuth2 flows

Inspecting an access token

Learning How OAuth2 Works

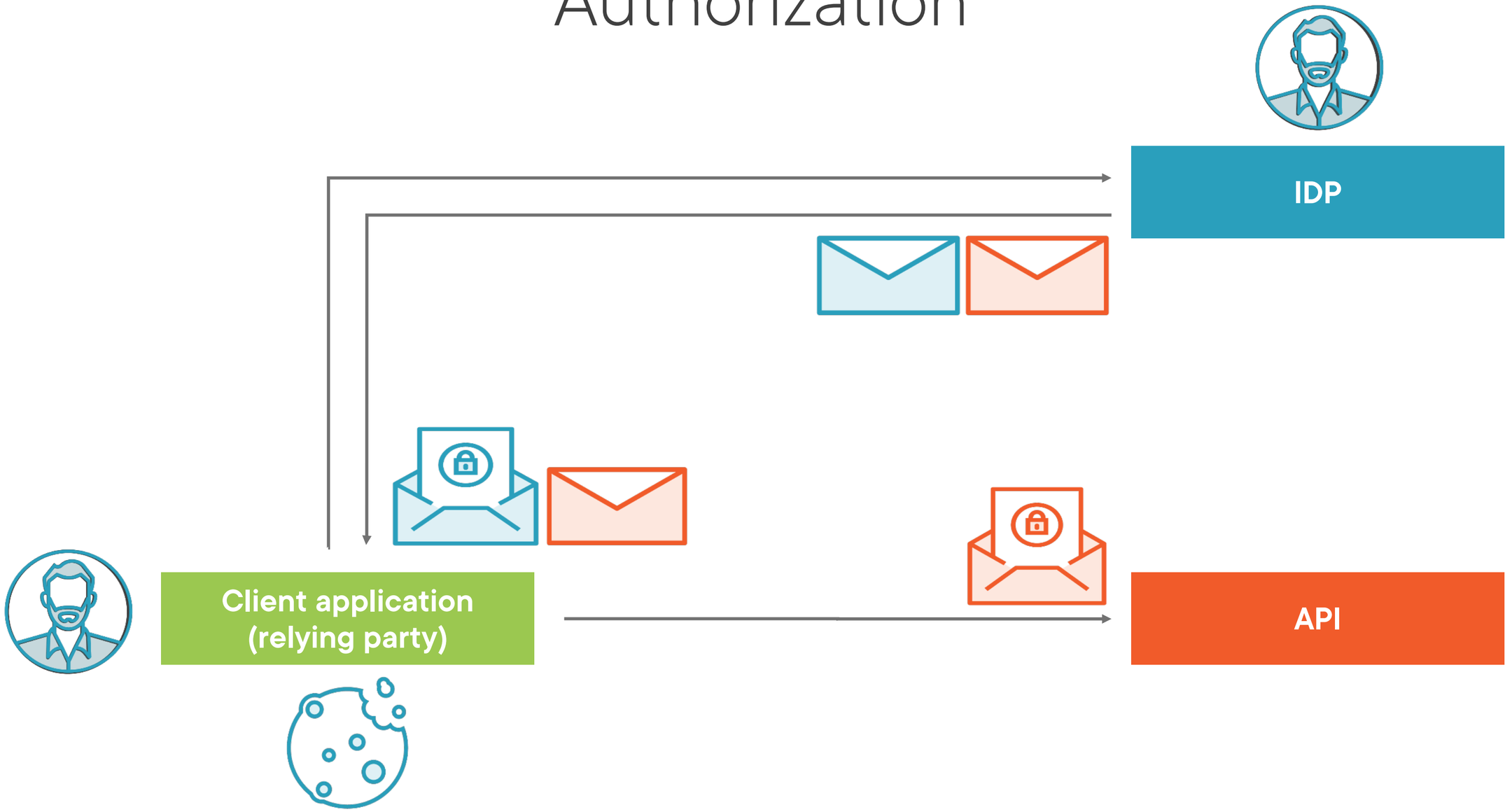


Learning How OAuth2 Works

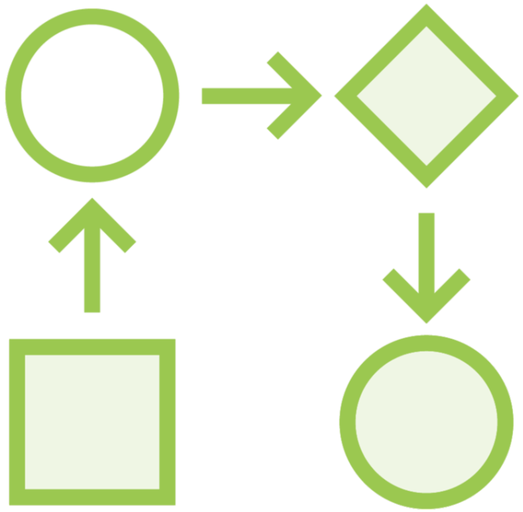
OpenID Connect standardized claims & verification methods

- You're often using OpenID Connect, even when you only require an access token

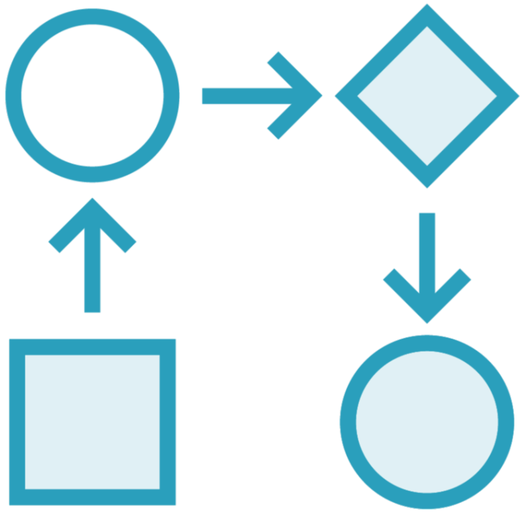
Using OpenID Connect for Authentication and Authorization



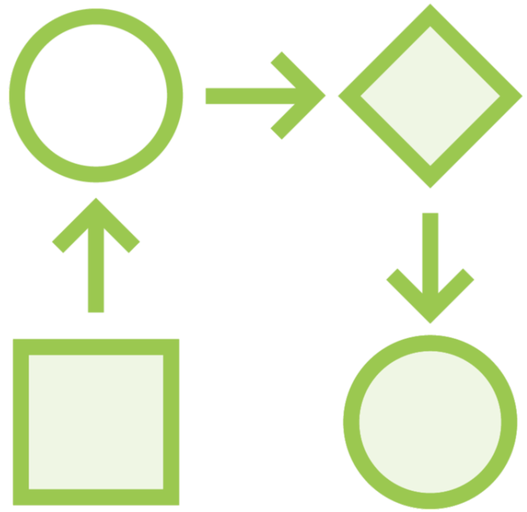
OAuth2 and OpenID Connect Flows



Authorization code

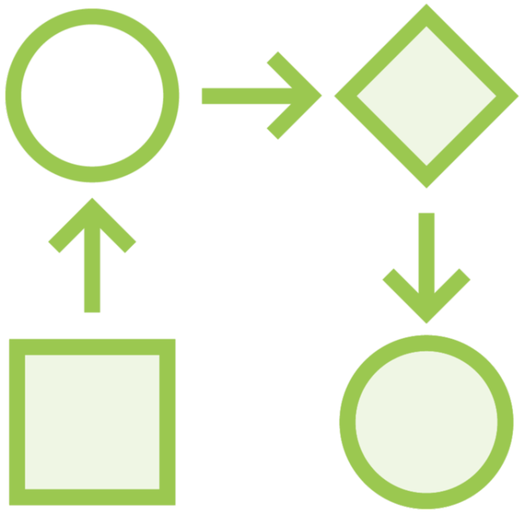


Implicit



Hybrid (OIDC only)

OAuth2 and OpenID Connect Flows

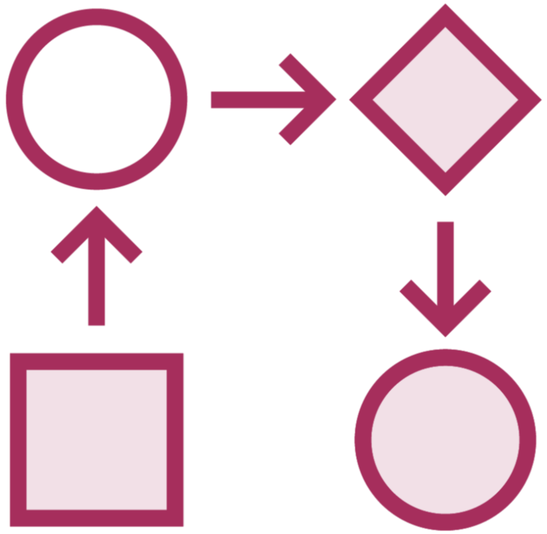


Authorization code

Implicit

Hybrid (OIDC only)

OAuth2 and OpenID Connect Flows

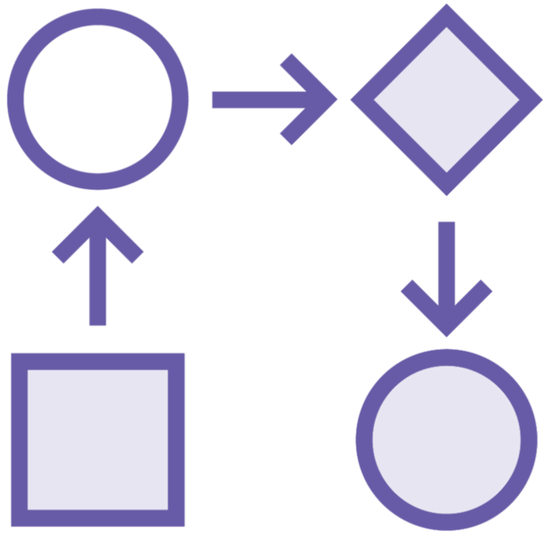


Resource Owner Password Credentials (OAuth2 only)

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:5001",
  "aud": [
    "imagegalleryapi“,
    "https://localhost:5001/resources"],
  …
}
```

Inspecting an Access Token

Access tokens are often JWTs, but don’t have to be (e.g.: reference tokens)

```
{
  "sub": "b7539694-97e7-4dfe-84da-b4256e1ff5c7",
  "iss": "https://localhost:5001",
  "aud": [
    "imagegalleryapi“,
    "https://localhost:5001/resources"],
  …
}
```

Inspecting an Access Token

The intended audience

- Our image gallery API
- Resources at level of the IDP (e.g. 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 (it extends & improves on OAuth2)

The advised flow is the authorization code flow with PKCE protection

Summary

OAuth2-only flows

- ROPC must be avoided
- Client credentials is for machine to machine communication

Up Next:
Securing Your API