Securing Your API

Kevin Dockx
ARCHITECT

@KevinDockx https://www.kevindockx.com

Coming Up

The authorization code flow with PKCE protection

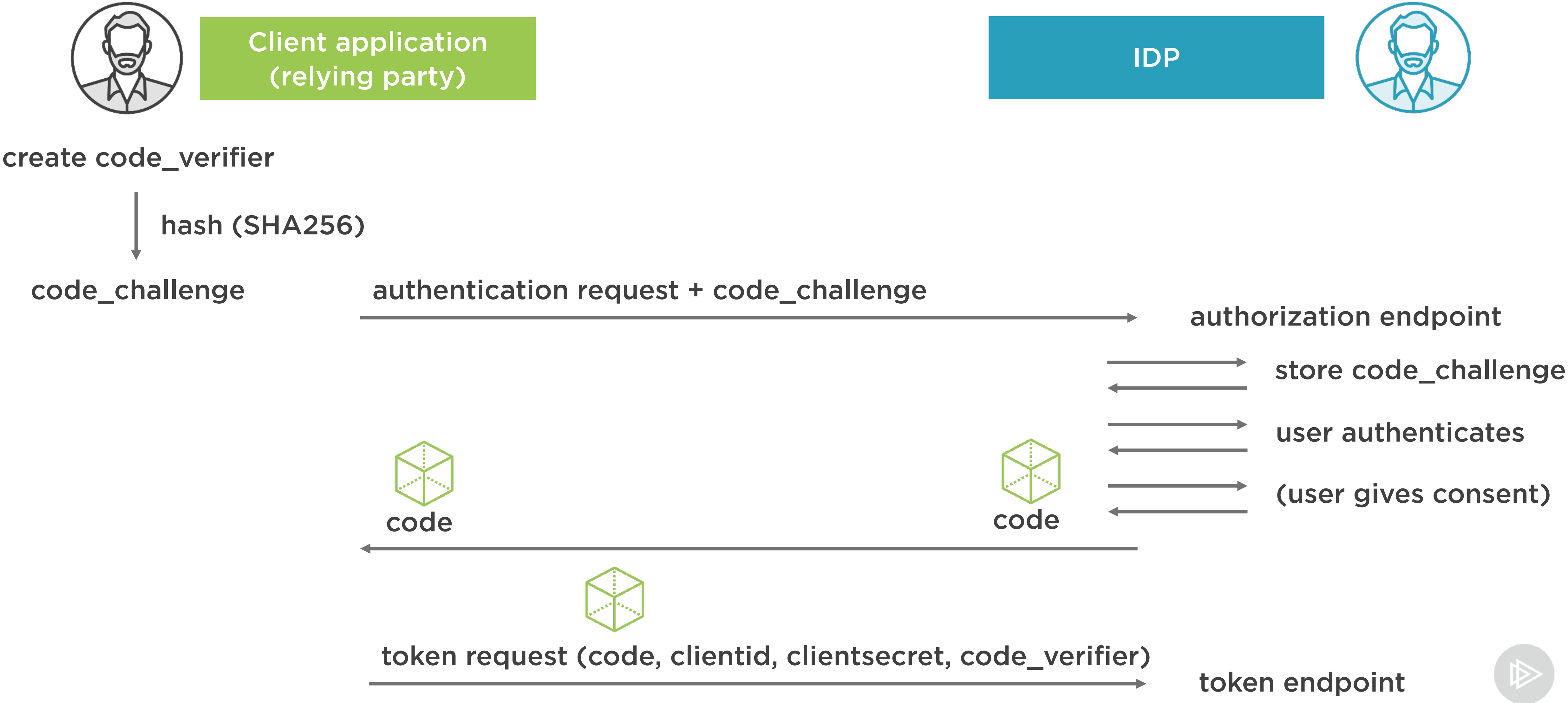
Passing an access token to the API and validating it

Using access token claims

Including additional identity claims in an access token

Role-based authorization

The Authorization Code Flow + PKCE



Client application (relying party)

IDP

create code_verifier

hash (SHA256)

code_challenge

authentication request + code_challenge

authorization endpoint

store code_challenge

user authenticates

(user gives consent)

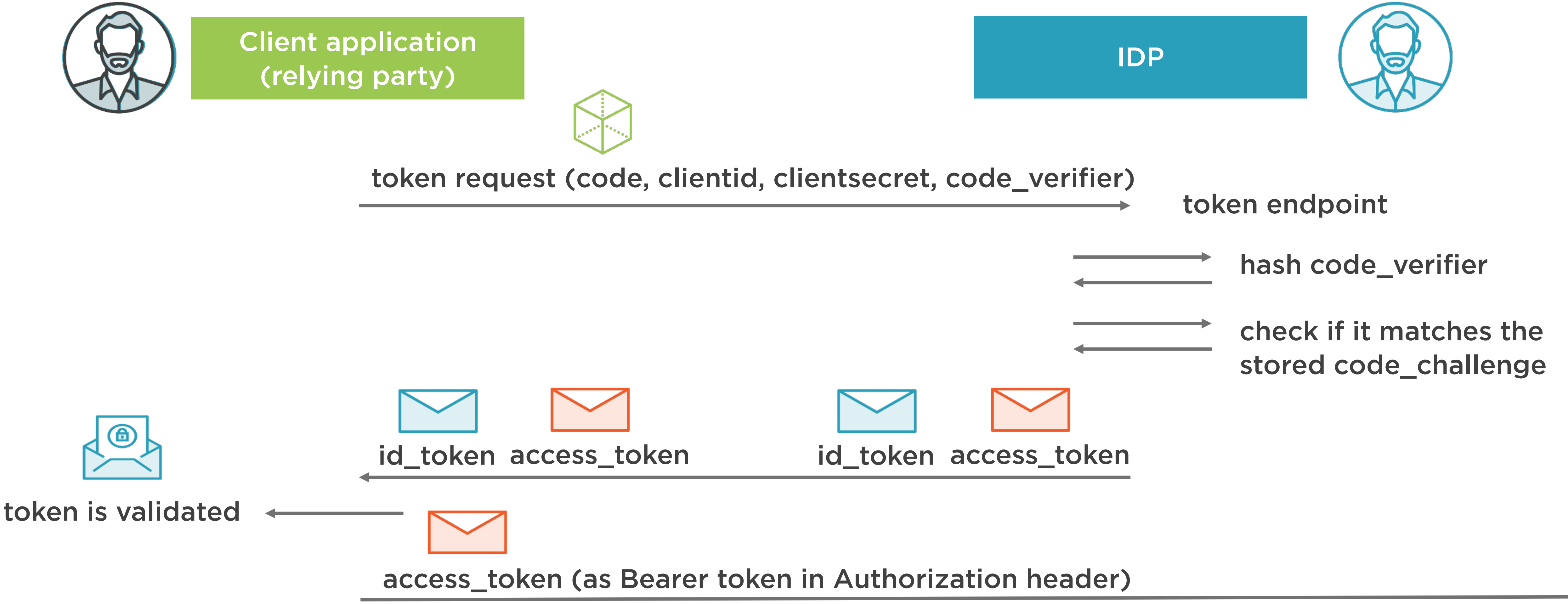
code

code

token request (code, clientid, clientsecret, code_verifier)

token endpoint

The Authorization Code Flow + PKCE



Client application (relying party)

IDP

token request (code, clientid, clientsecret, code_verifier)

token endpoint

hash code_verifier

check if it matches the stored code_challenge

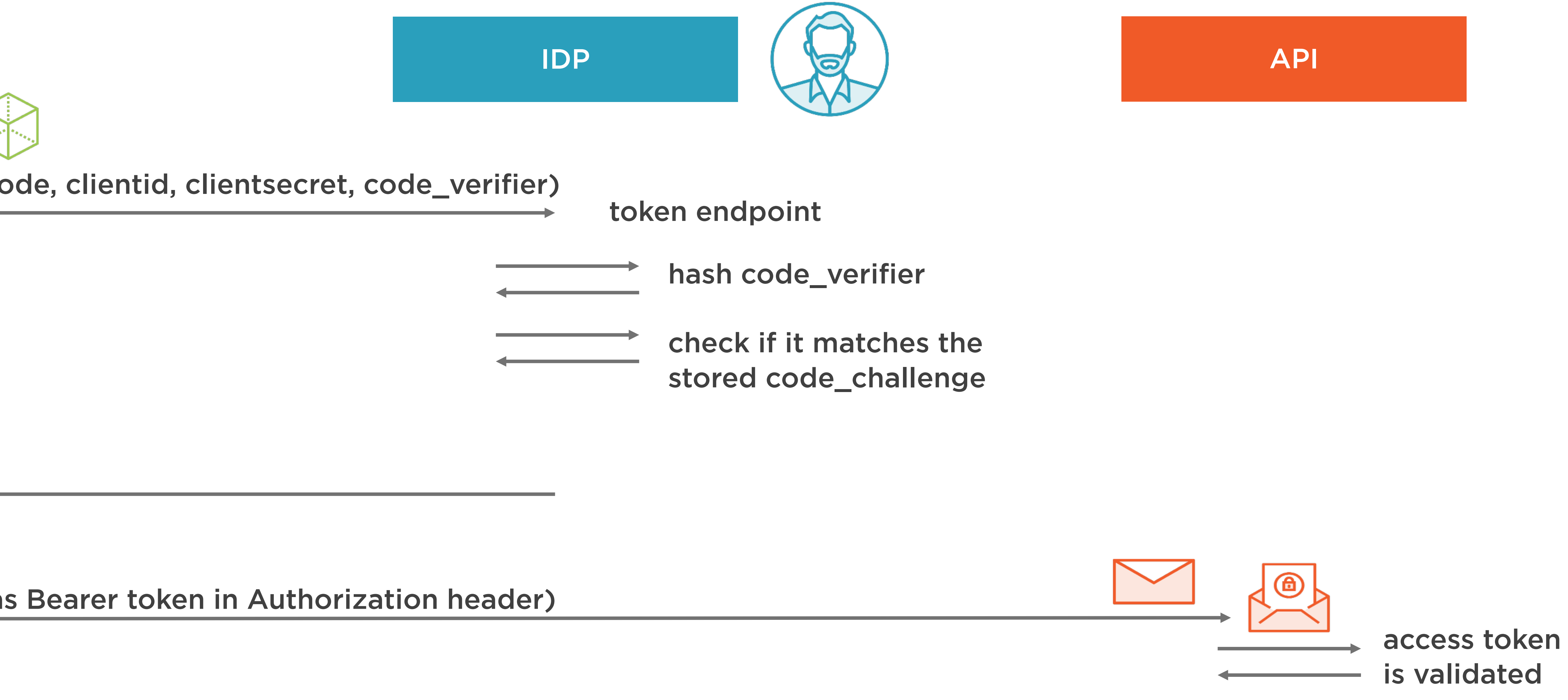
id_token access_token

id_token access_token

token is validated

access_token (as Bearer token in Authorization header)

The Authorization Code Flow + PKCE



IDP

API

ode, clientid, clientsecret, code_verifier)

token endpoint

hash code_verifier

check if it matches the stored code_challenge

s Bearer token in Authorization header)

access token is validated

Demo

Securing access to our API

Demo

Passing an access token to our API

Demo

Showing an access denied page

Demo

Using access token claims when getting a resource collection

Including Identity Claims in an Access Token

Sometimes an API needs access to identity claims

When defining a resource scope (API resource), include the required claims in the claims list

Demo

Including identity claims in an access token

Demo

Protecting the API when creating a resource (with roles)

Summary

Access tokens are passed to the API as Bearer tokens

AccessTokenValidation middleware can be used to validate an access token at level of the API

Summary

Configure the ApiResource to include additional identity claims in the access token

Role-based authorization is achievable through the Authorize attribute