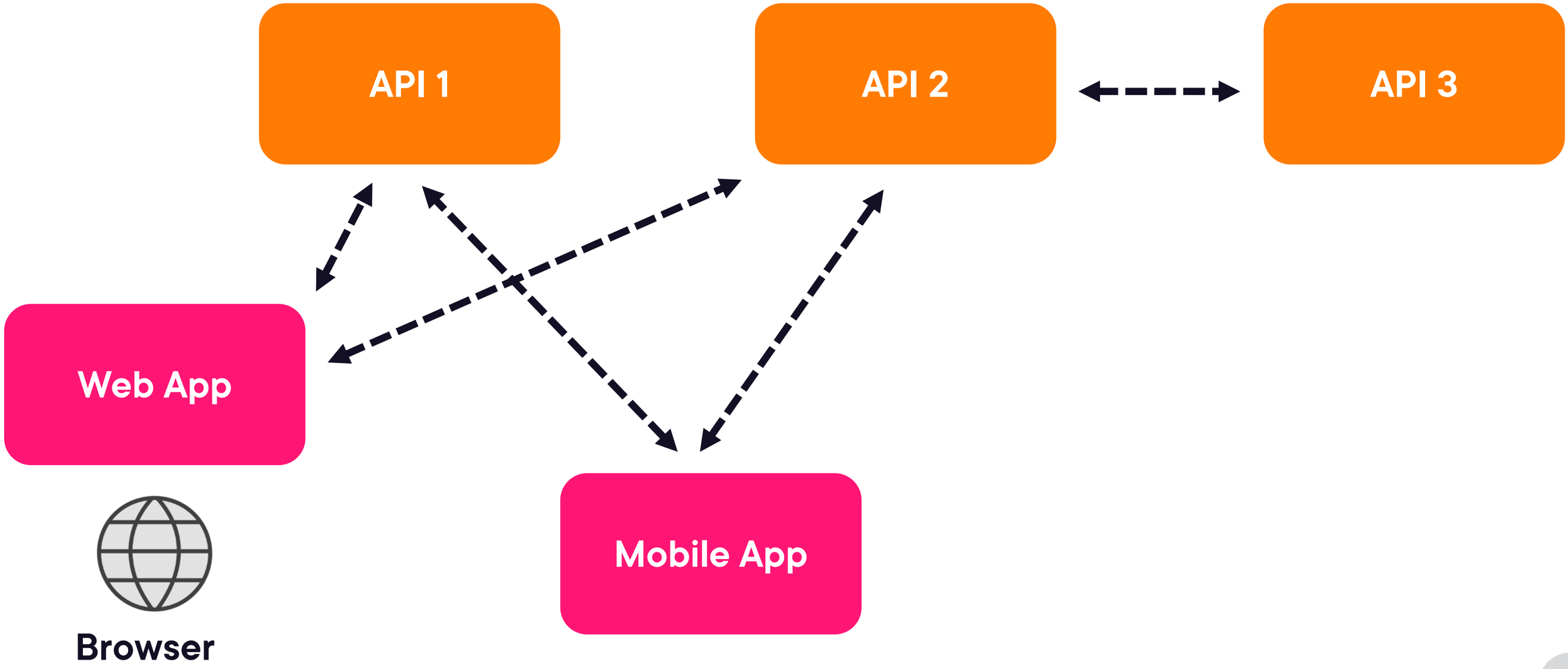
Multi-Application Authentication with OpenID Connect

Roland Guijt

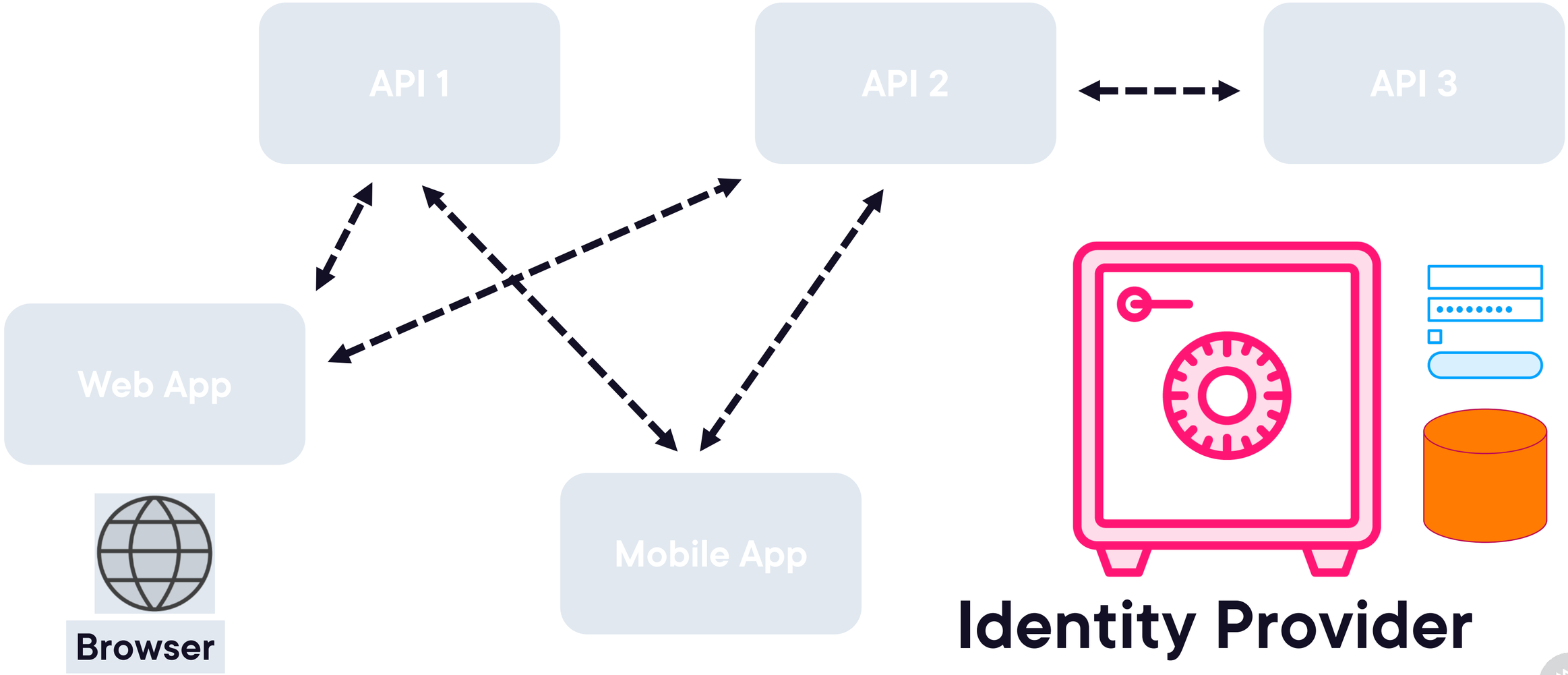
Freelance Trainer and Consultant | Microsoft MVP

@rolandguijt | roland.guijt@gmail.com

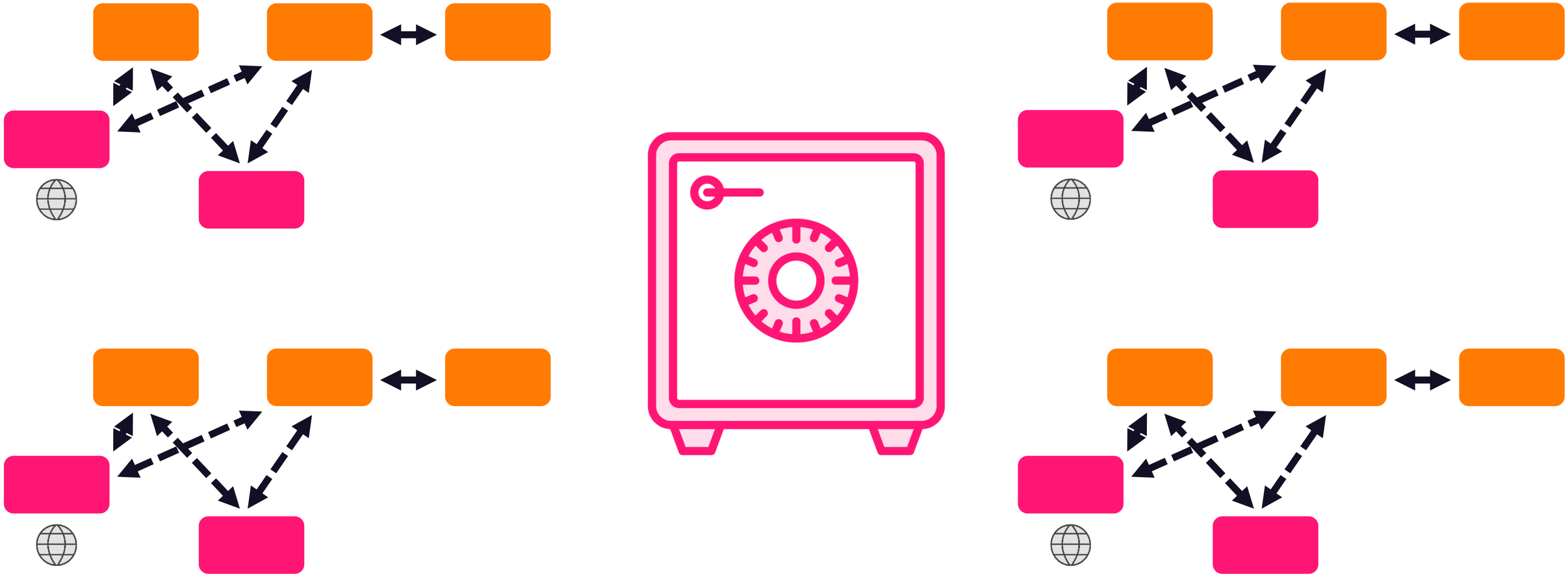
A Typical Application Landscape



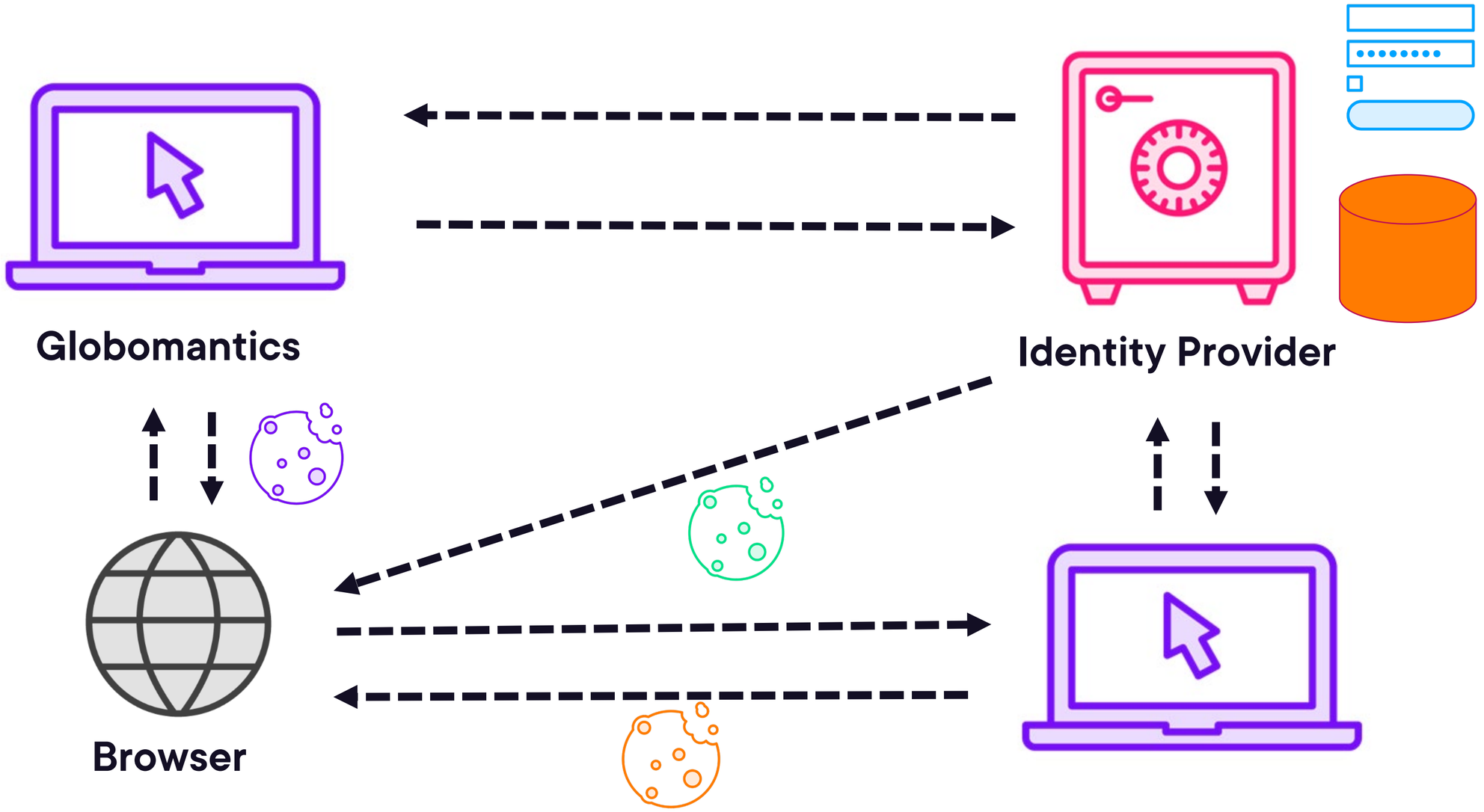
The Identity Provider



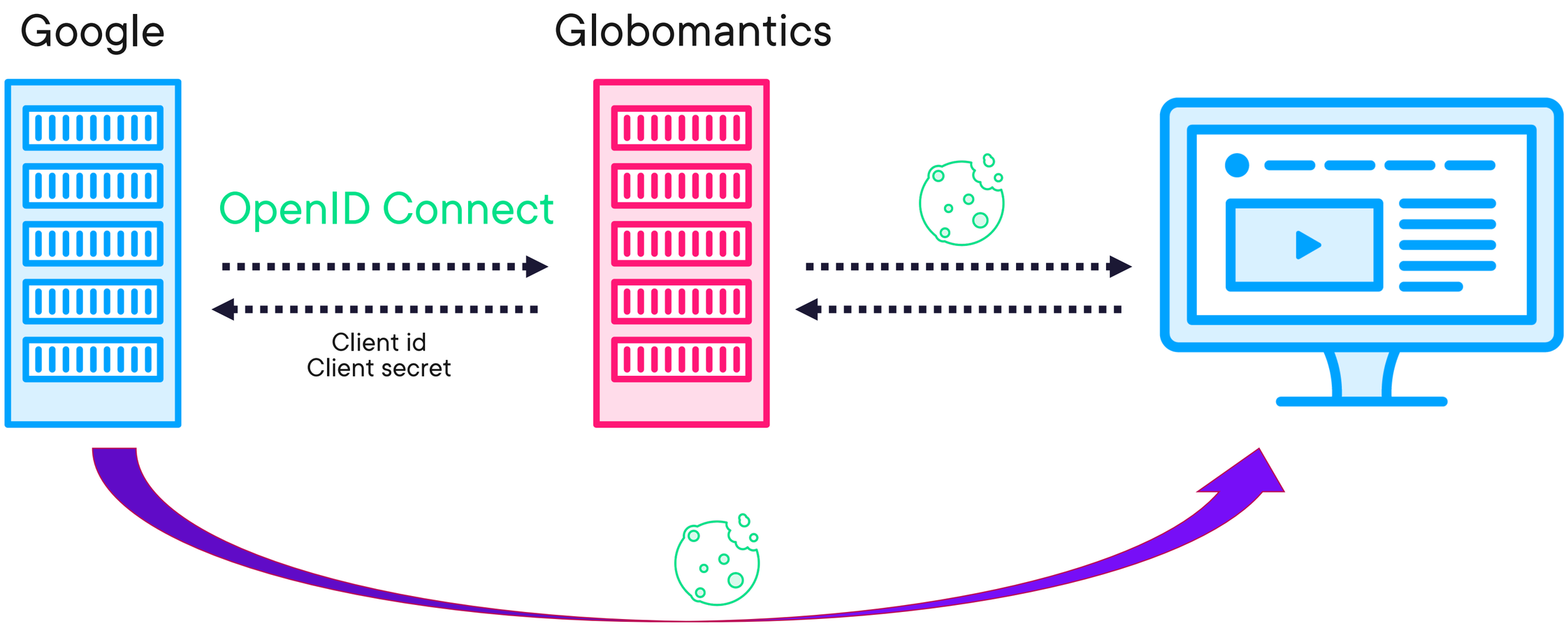
One Identity Provider to Rule Them All



Delegating Authentication to an Identity Provider



External Identity Providers



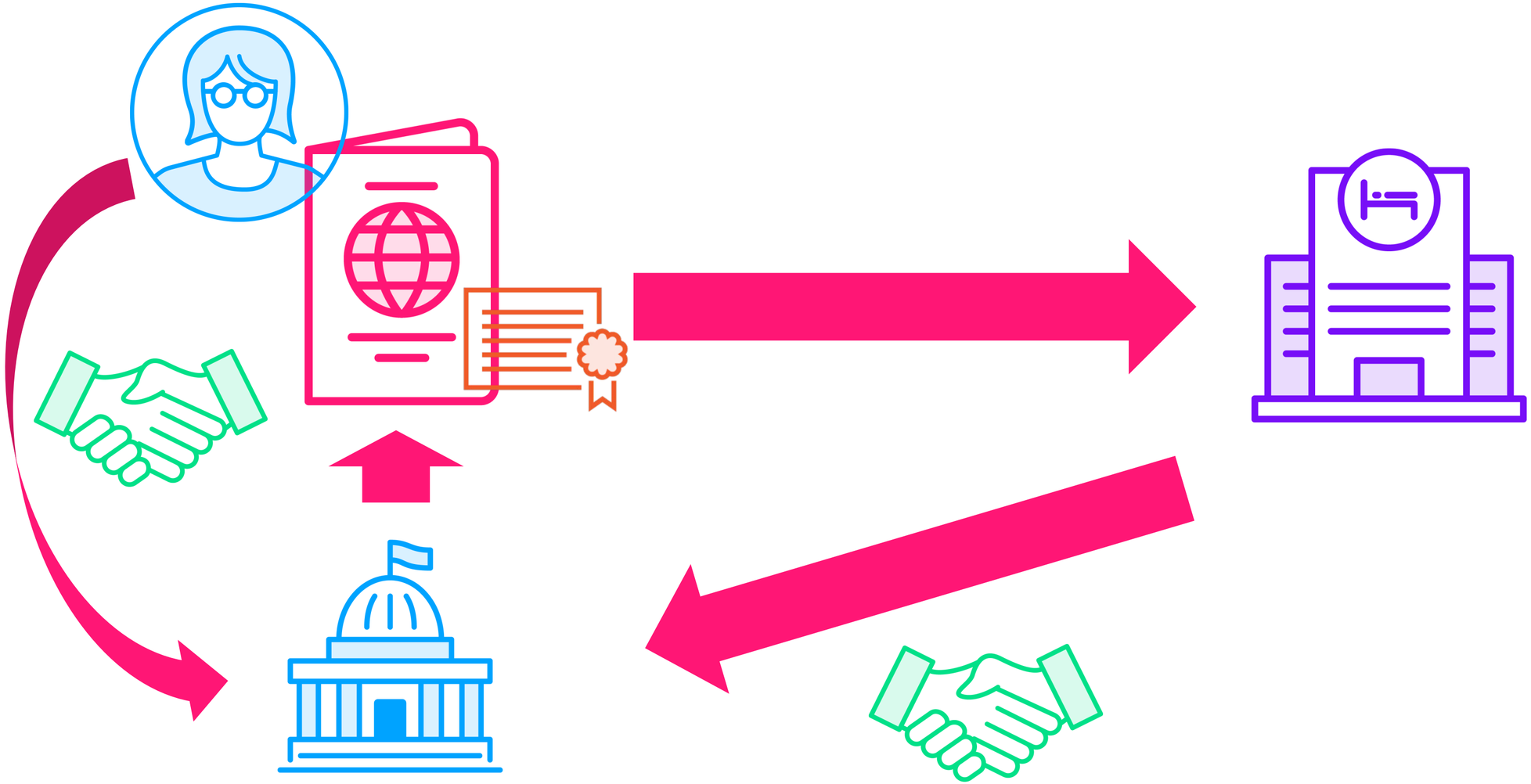
Running Two Applications

Both the web application and the identity provider are running

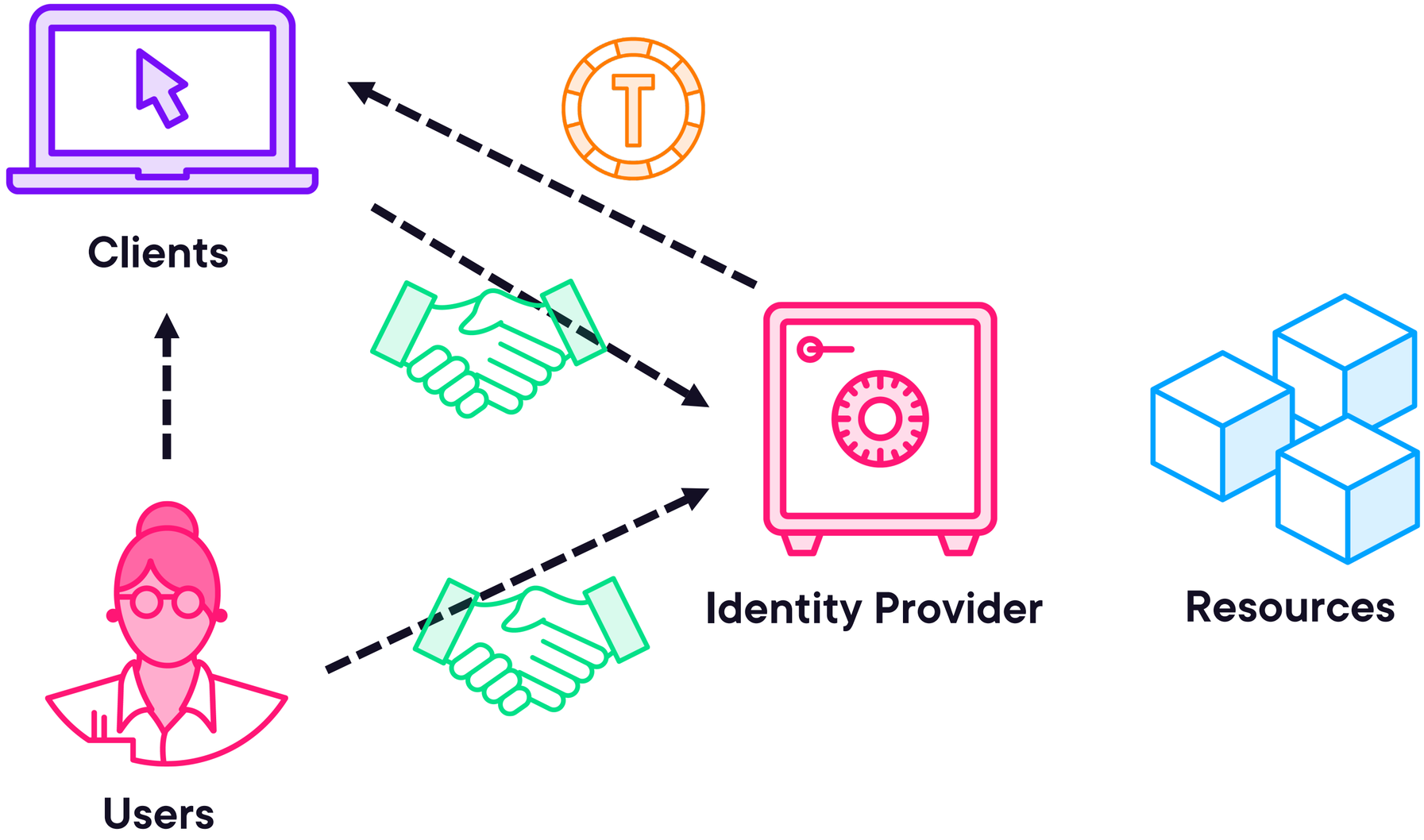
The web application has the [Authorize] attribute on both controllers

The web application is running on https://localhost:5001, the identity provider on https://localhost:5000.

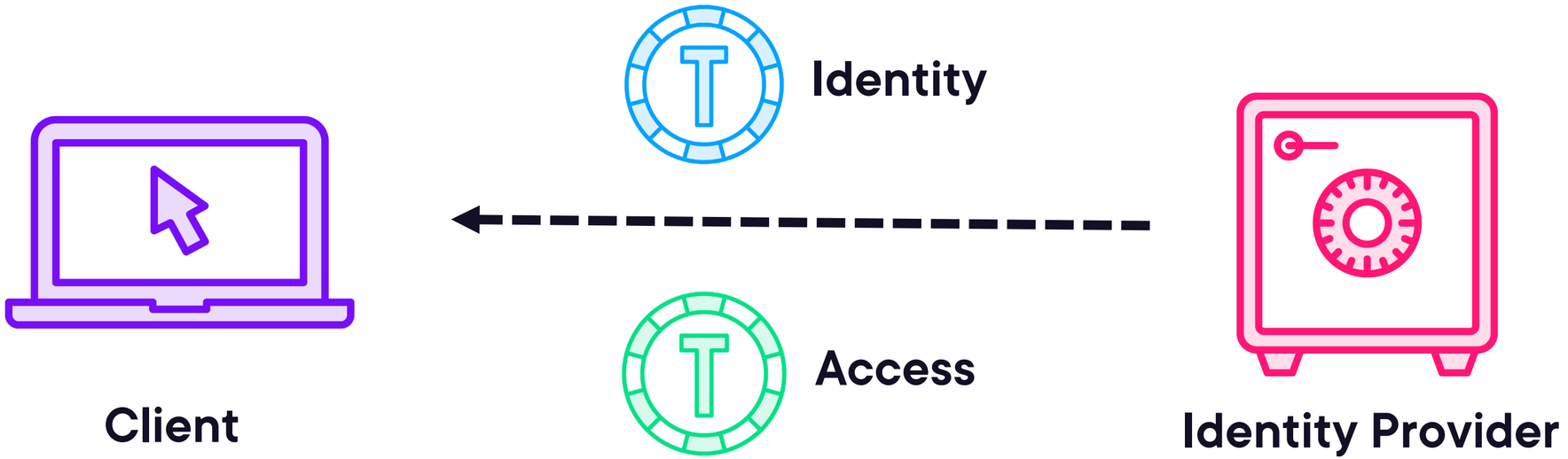
The Process of Authentication Enhanced



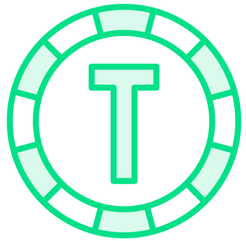
OpenID Connect Concepts



Tokens

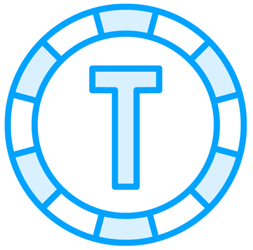


Standards



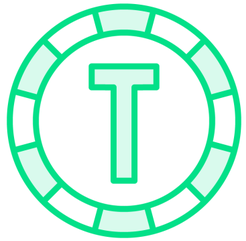
Access

OAuth2



Identity

+

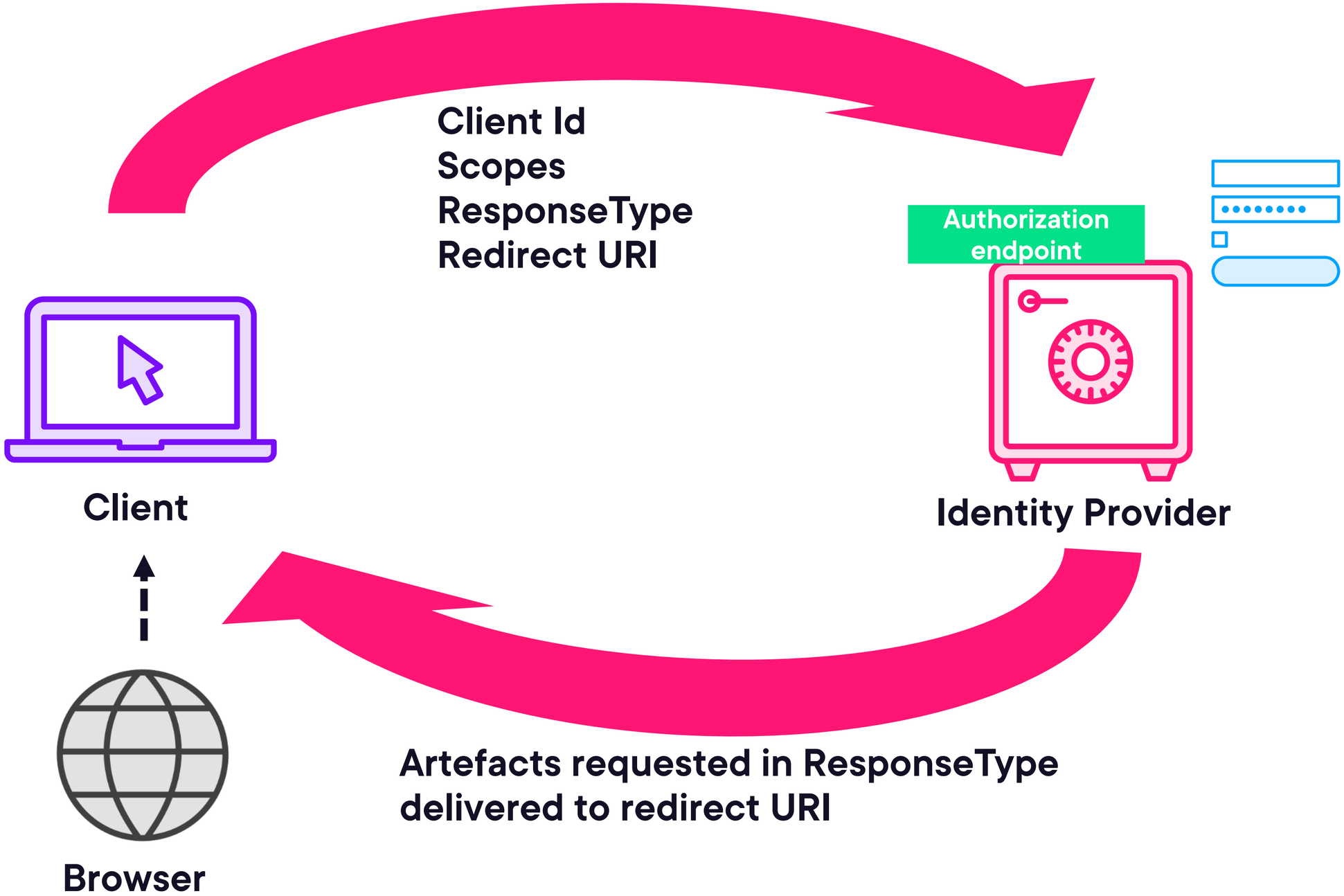


Access

OpenId Connect (OIDC)

Course recommendation:

Authentication and Authorization in ASP.NET Core Web API


Client Id
Scopes
ResponseType
Redirect URI
Authorization endpoint
Client
Identity Provider
Browser
Artefacts requested in ResponseType
delivered to redirect URI

Scopes

Identity

API

Many cloud-based identity providers use extension methods that call AddOpenIdConnect

Claims in the Profile Scope

name
family_name
given_name
middle_name
nickname
preferred_username
picture
website
gender
birthdate
zoneinfo
locale
updated_at

Authorization Code Flow

A way to get tokens

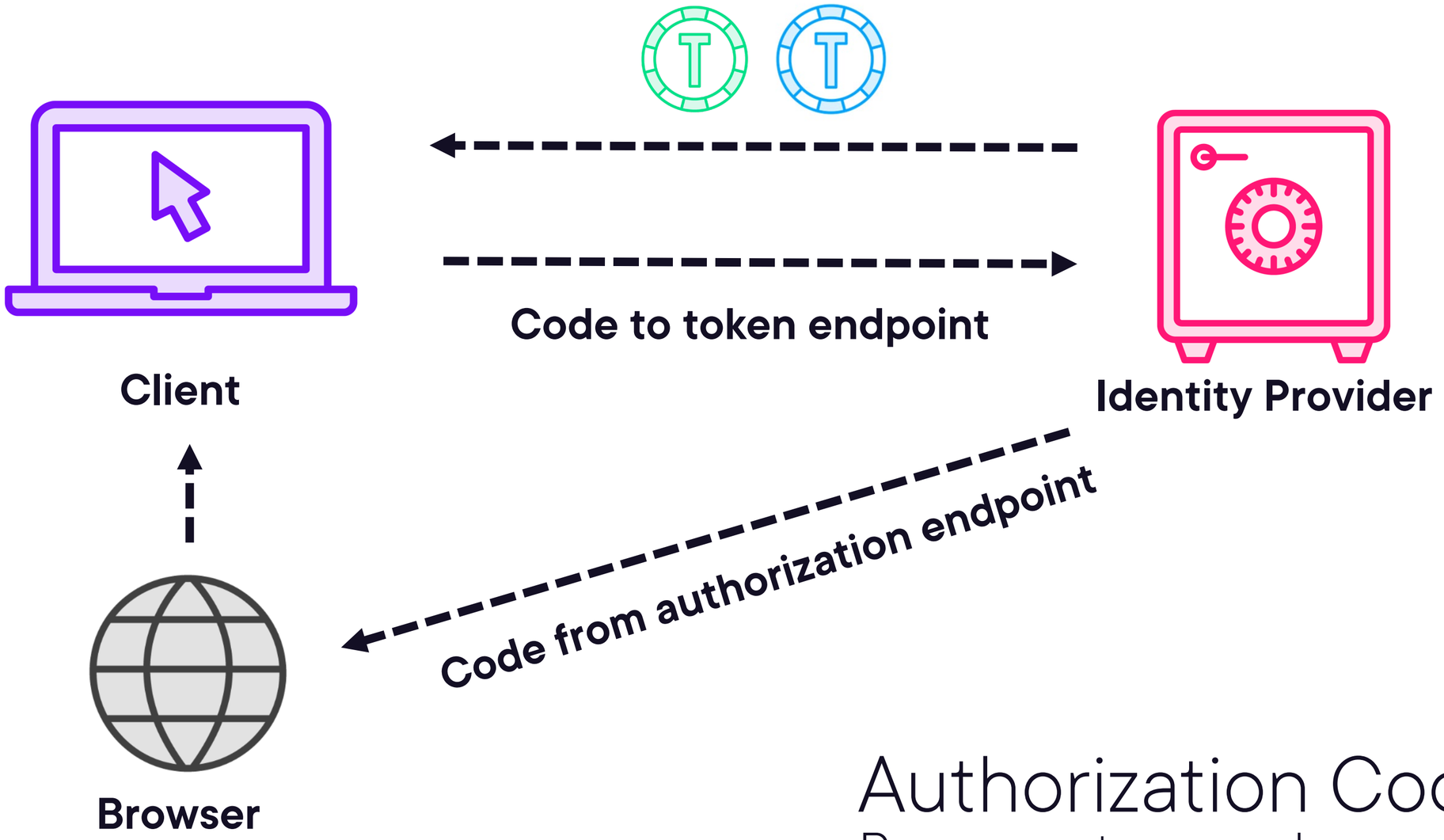
Client will initially get a code

Browser redirects to send tokens

Browser = Front channel

Front channel = unsafe

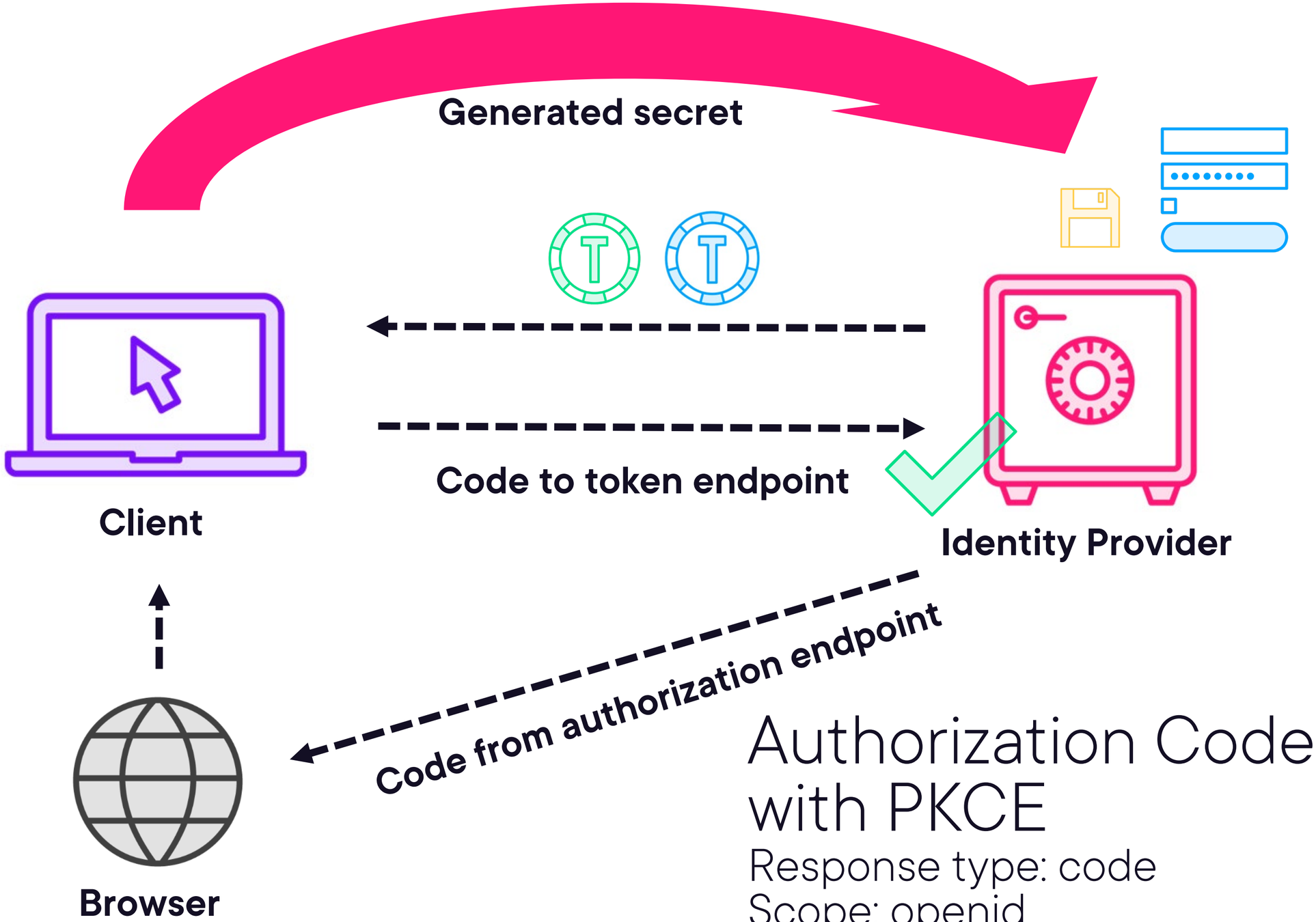
Authorization Code Flow helps



Authorization Code

Response type: code
Scope: openid

https://4sh.nl/PkceSpec



Authorization Code with PKCE

Response type: code
Scope: openid

PKCE

Enabled by default by middleware when using Authorization Code Flow

Only up-to-date identity providers will be able to use it

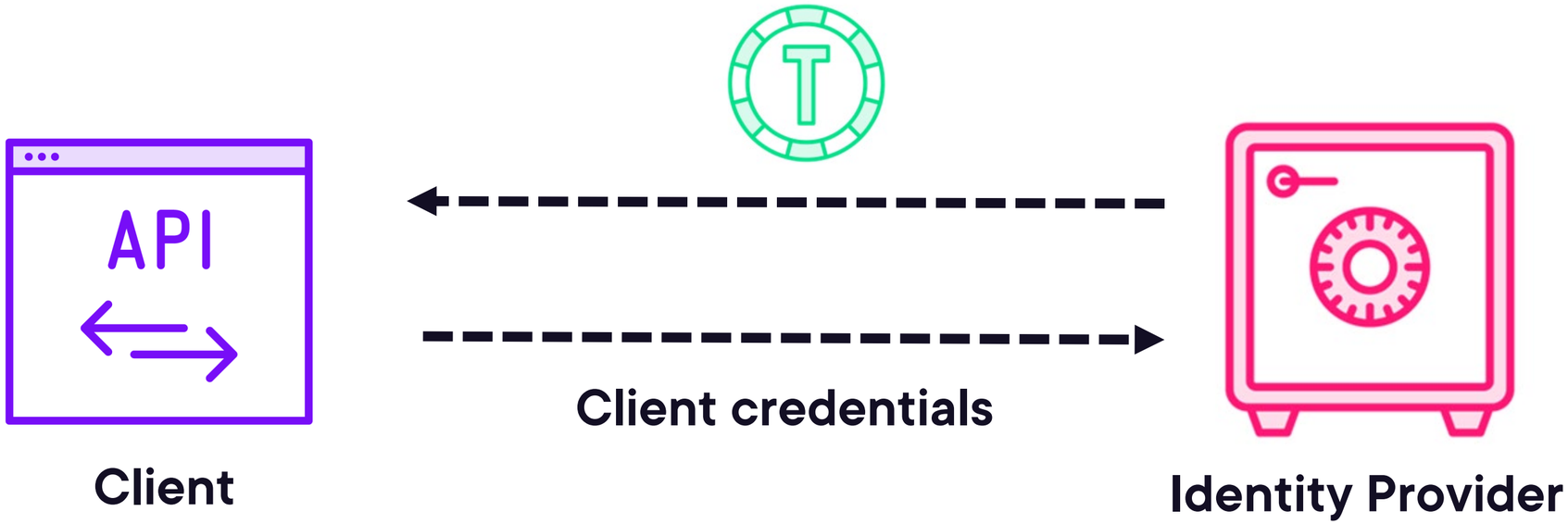
Flows for Front-End Applications

There are more flows than Authorization Code Flow

Considered unsafe

SPAs can also use Authorization Code Flow

Client Credentials



Either build your own identity provider or use one in the cloud

Duende IdentityServer

Adds identity provider endpoints to an ASP.NET Core application

Duende is supporting company

Open source

Free for testing and personal use

In production: license needed

https://4sh.nl/idsvrlicense

IdentityServer and Users

Leaves user store and functionality like password resets, 2FA etc. to you

Focuses on the OpenID Connect part

IdentityServer and Identity ideal combination

https://4sh.nl/idsvrtemplates

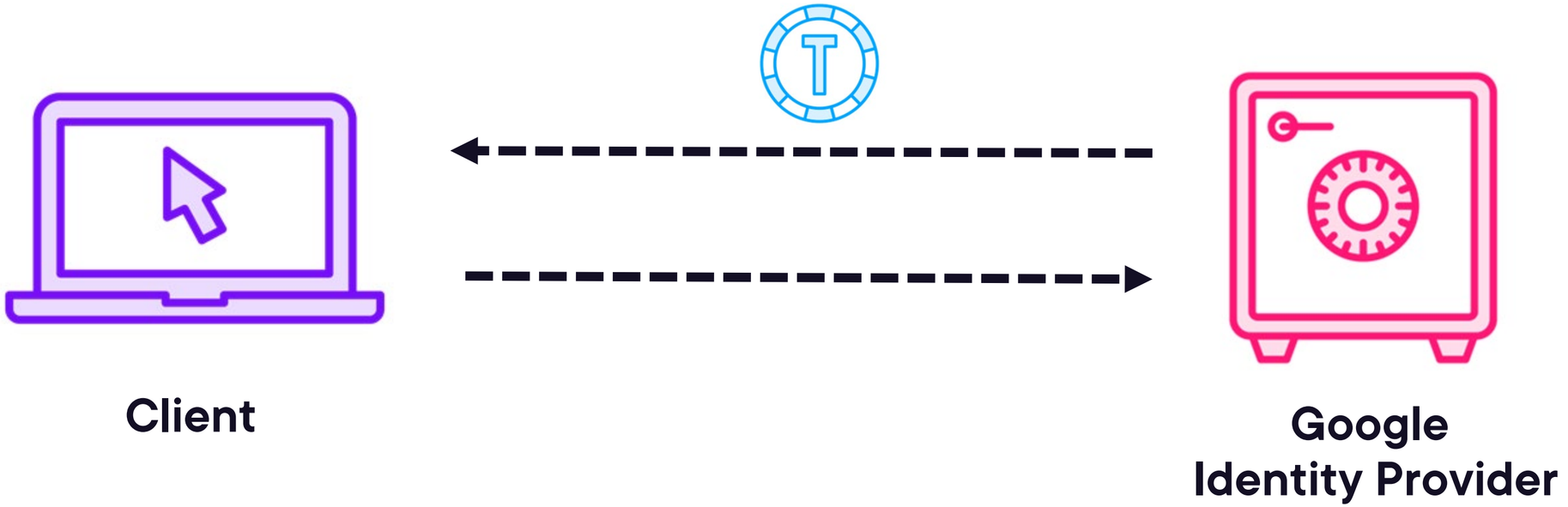
Accounts in Included Database

roland.guijt@gmail.com - Secret123!

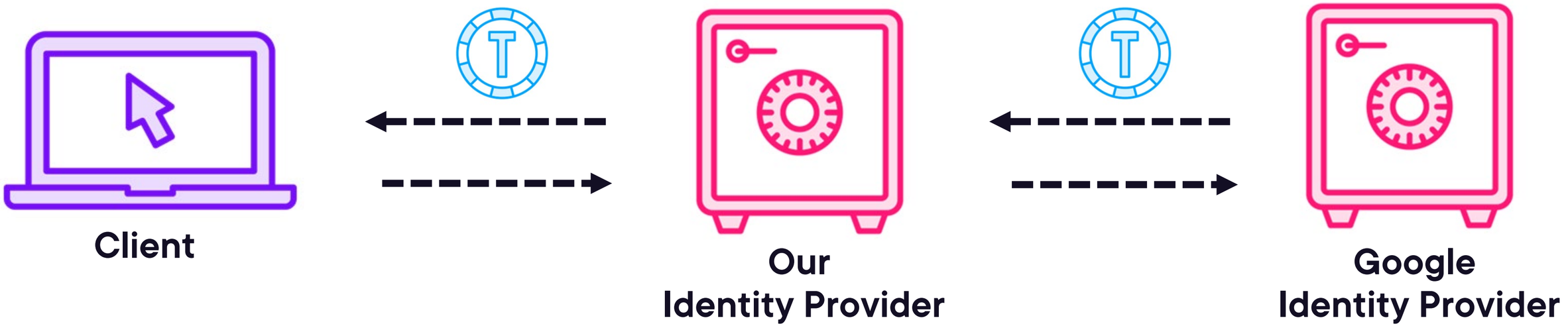
bobsmith@email.com - Pass123$

alicesmith@email.com - Pass123$

Adding Google's Identity Provider



Adding Google's Identity Provider



Identity Server's ProfileService is responsible for adding user claims.

Token Verification by Client or API

1. Identity Provider creates hash of contents
2. Hash is encrypted using private key
3. Attaches result (== signature) to token
4. Client uses public key to decrypt hash
5. Readable contents is hashed
6. Compares own hash with decrypted hash

Successful Verification Conclusions

The token came from the trusted authority

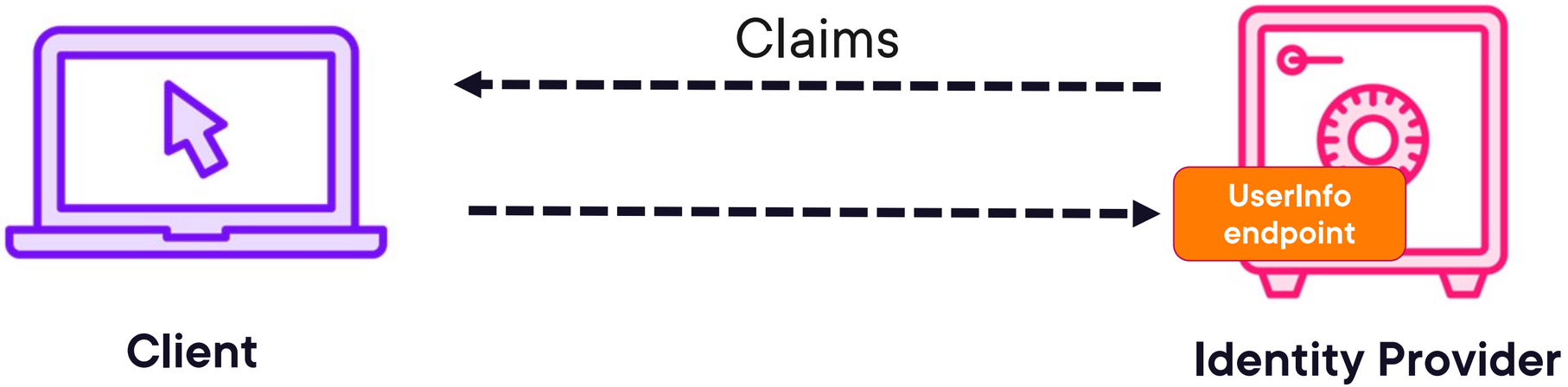
The contents is as the authority issued it

Key-Value List of Claim Mappings

Key	Value
role	http://schemas.microsoft.com/ws/2008/06/identity/claims/role
birthdate	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth

Bloated tokens can cause problems

The UserInfo Endpoint



When is a Claim a Claim?

It should be relevant for the whole application landscape

Not for one individual client

Example: UI-related settings

Store on client-level using subject id claim

Evaluate the "role" claim

Cloud Based Identity Providers

Most use OpenID Connect

Less complex to setup and run

Less flexible

Other Cloud Identity Providers

Auth0

Okta

Azure Active Directory (AAD)

Things Named Identity

ASP.NET Core Identity

Identity provider

Duende IdentityServer

Microsoft Identity Platform

Windows Authentication

Authenticate against user store of OS

Or domain controller

Not usable for public facing applications

Just on local network

Up Next:

Single-Page Application Authentication with BFF