Authentication and Authorization in ASP.NET Core 6

Authentication Basics

Roland Guijt

Freelance Trainer and Consultant | Microsoft MVP

@rolandguijt | roland.guijt@gmail.com

Version Check

This version was created by using:

- ASP.NET Core 6

Version Check

This course is 100% applicable to:

- ASP.NET Core 5
- ASP.NET Core 7

Authentication

Name: Roland Guijt

Address: 2001 Clarke Avenue

City: New York

Birth date: 12/22/1980

Authentication

Needs proof

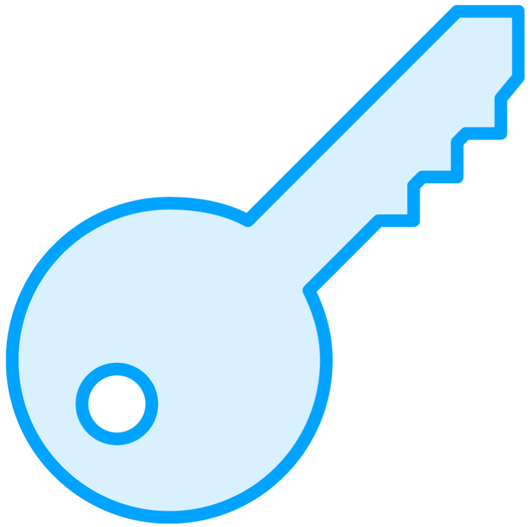
Proof for application is password

Authentication is verifying an identity

Authentication and Authorization in ASP.NET Core

Authentication (AuthN)

Identity cookies
ASP.NET Core Identity
Identity Provider



Authorization (AuthZ)

ASP.NET Core Authorization


Hotel

Authorization

Limited access

What a user can do

Needs data

Coming directly or indirectly from claims

Examples of Claims

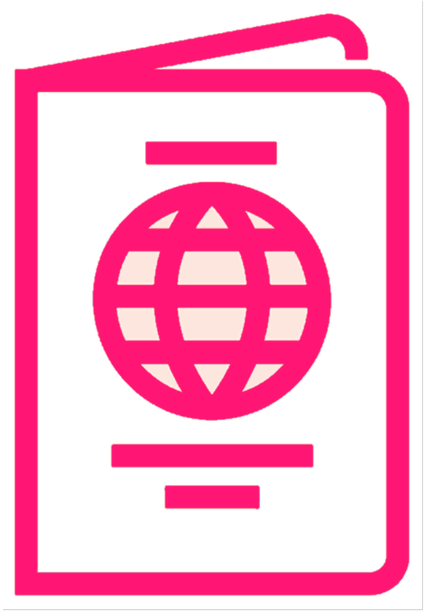
Name	Address	Date of Birth
Role	EmployeeNo	Department

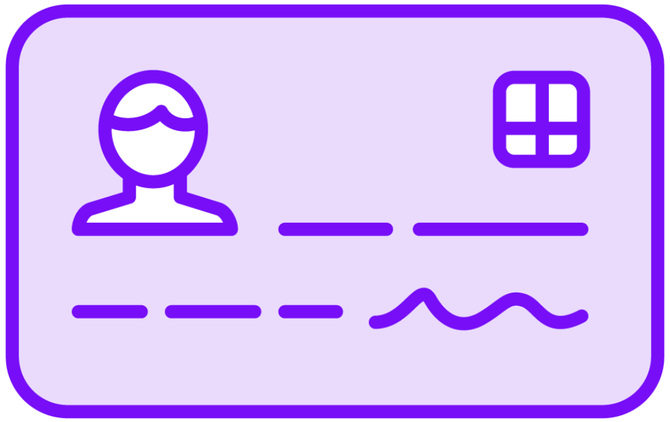
ASP.NET Core 6: Big Picture

All ASP.NET Core application types use the same building blocks

An authentication scheme is a way to authenticate

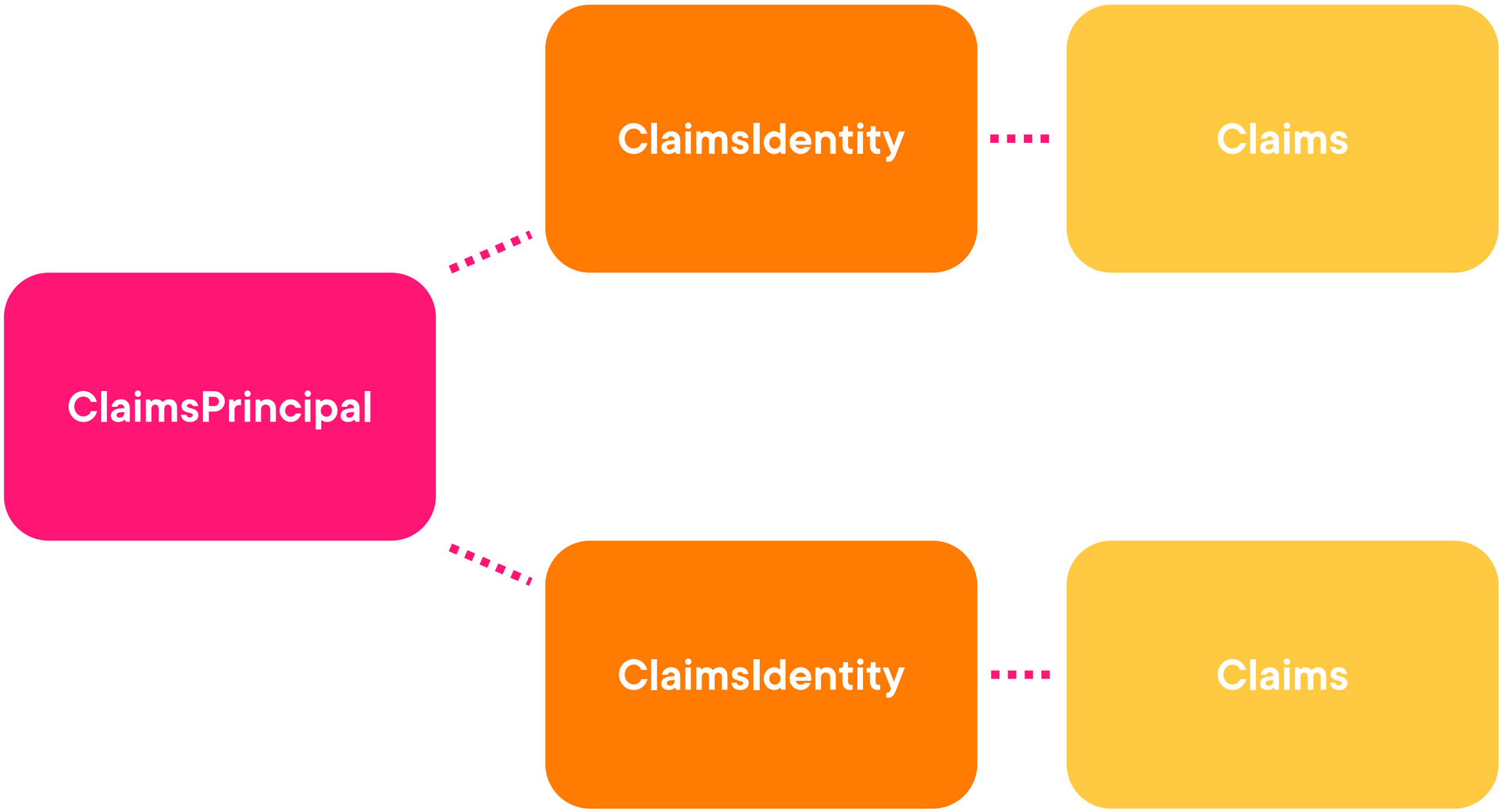
Authentication Schemes





A hash is a cryptographic function that transforms data into a string of a fixed length.

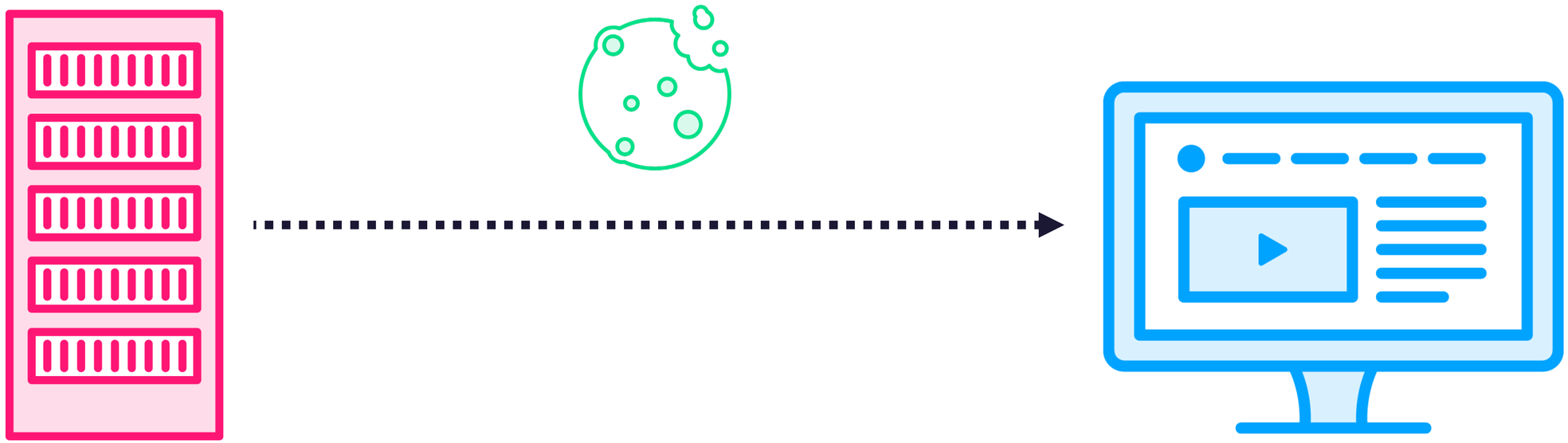
Claims-based Identity



Use a local redirect to protect against open redirection attacks

The Web is Stateless

Identity Cookie



Identity Cookie

When the Application Receives an Identity Cookie

The user information is decrypted

The ClaimsPrincipal object is reconstructed

ClaimsPrincipal is made available

Secured by ASP.NET Core Data Protection

ClaimsPrincipal and Claims

Use Claims property to access all claims

Could be used to do authorization

But use centralized authorization instead

Problem with Identity Cookies

Persistent cookies lifetime

User has access to application as long as cookie lives

Solution: handle event that fires upon each incoming request

Examples of External Identity Providers

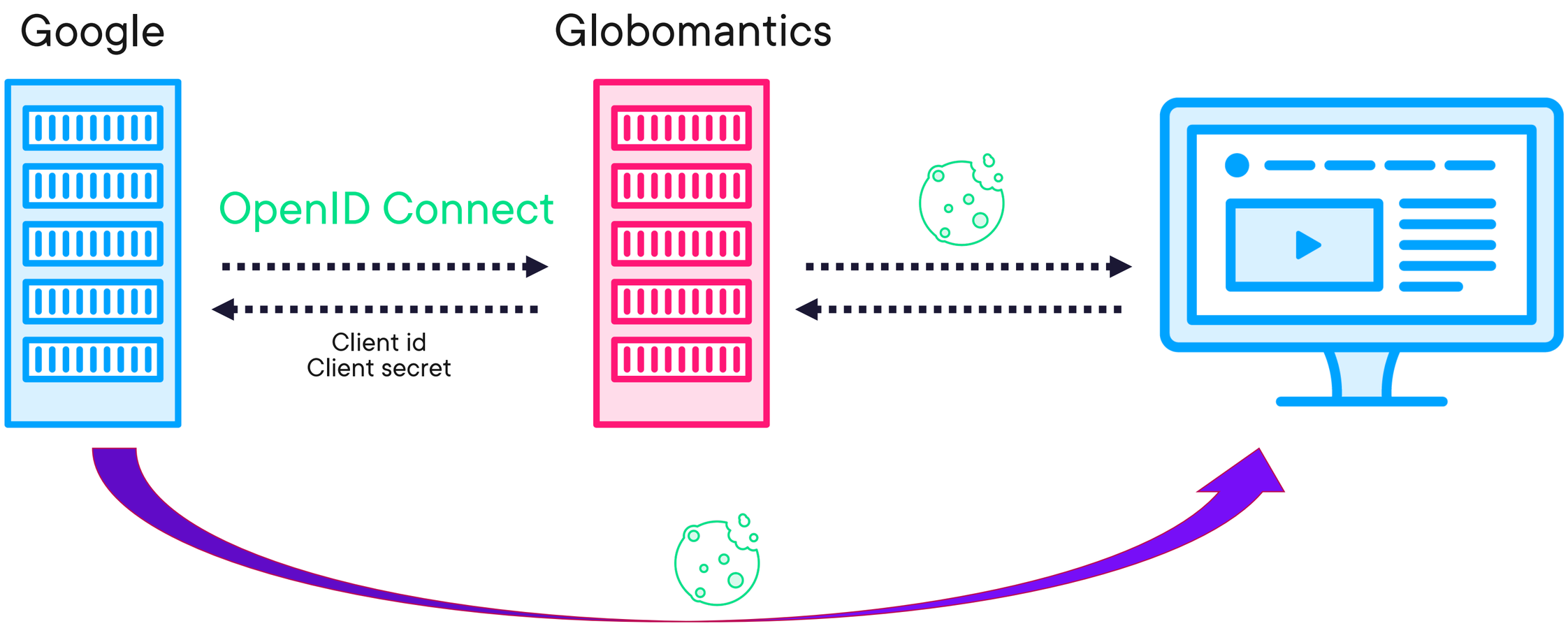
Google

Facebook

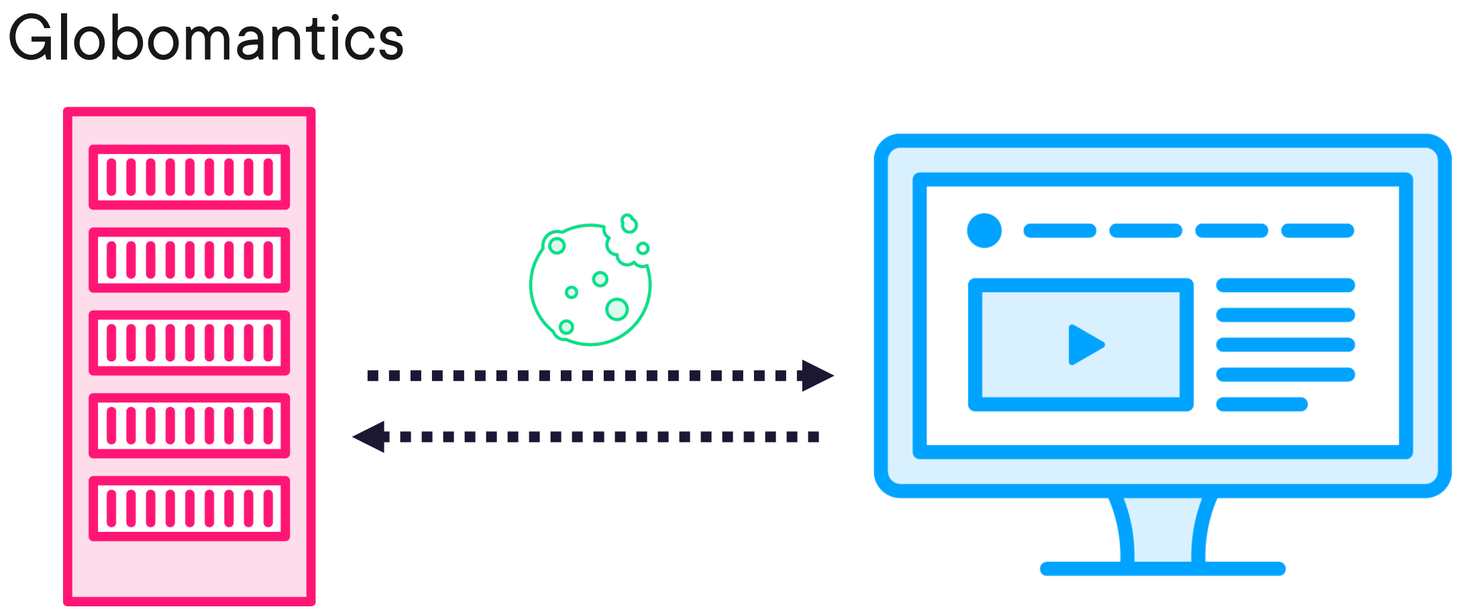
Microsoft

Twitter

External Identity Providers



External Identity Providers



https://4sh.nl/googleclient

Secrets

Not in source code

Use configuration object

Not in JSON files

Secret manager

https://4sh.nl/secrets

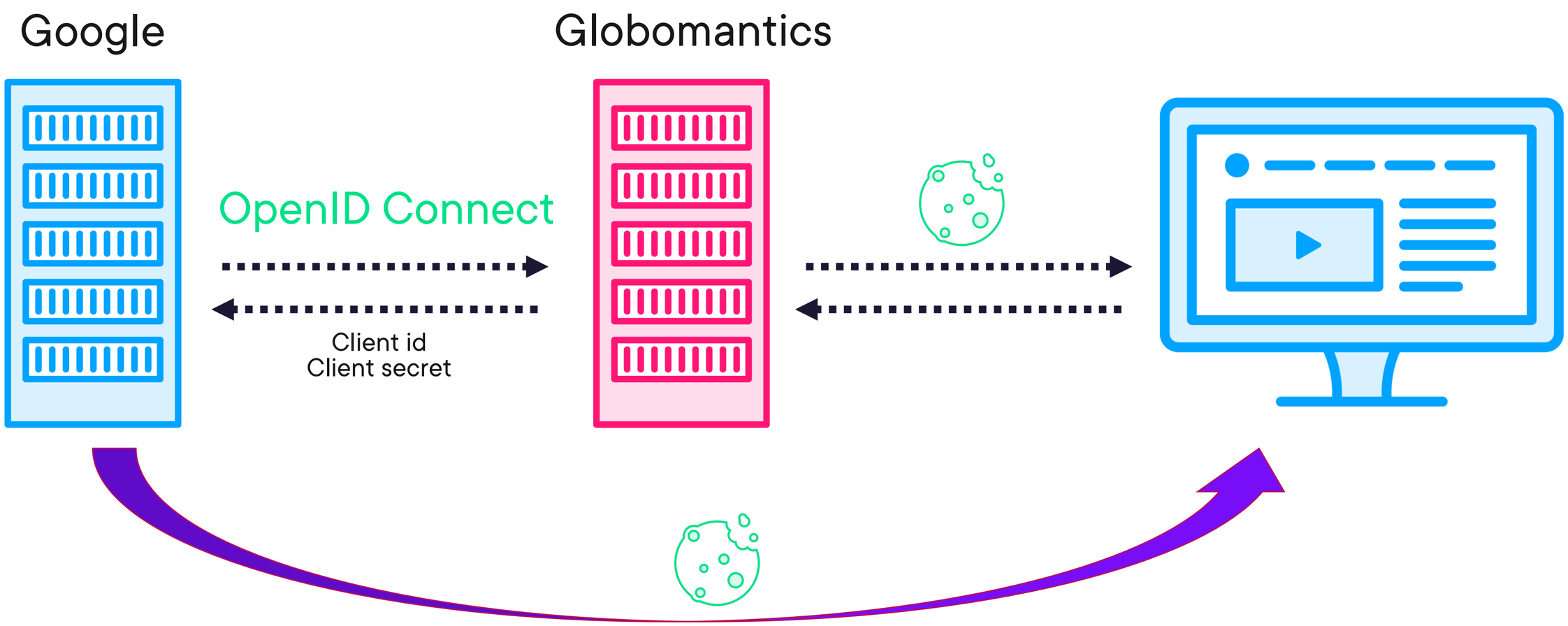
Scheme Actions

Authenticate

Challenge

Forbid

External Identity Providers



SigninAsync versus AuthenticateAsync

SignInAsync

Returns the ClaimsPrincipal and persists it.

AuthenticateAsync

Returns the ClaimsPrincipal without persisting.

Up Next:

Authentication with ASP.NET Core Identity