Centralized Authentication with a Token Service

Roland Guijt
CONSULTANT | TRAINER | AUTHOR

@rolandguijt www.rmgsolutions.nl

Overview

What is a token service?

OAuth2 and OpenIdConnect

Setting up a token service using IdentityServer

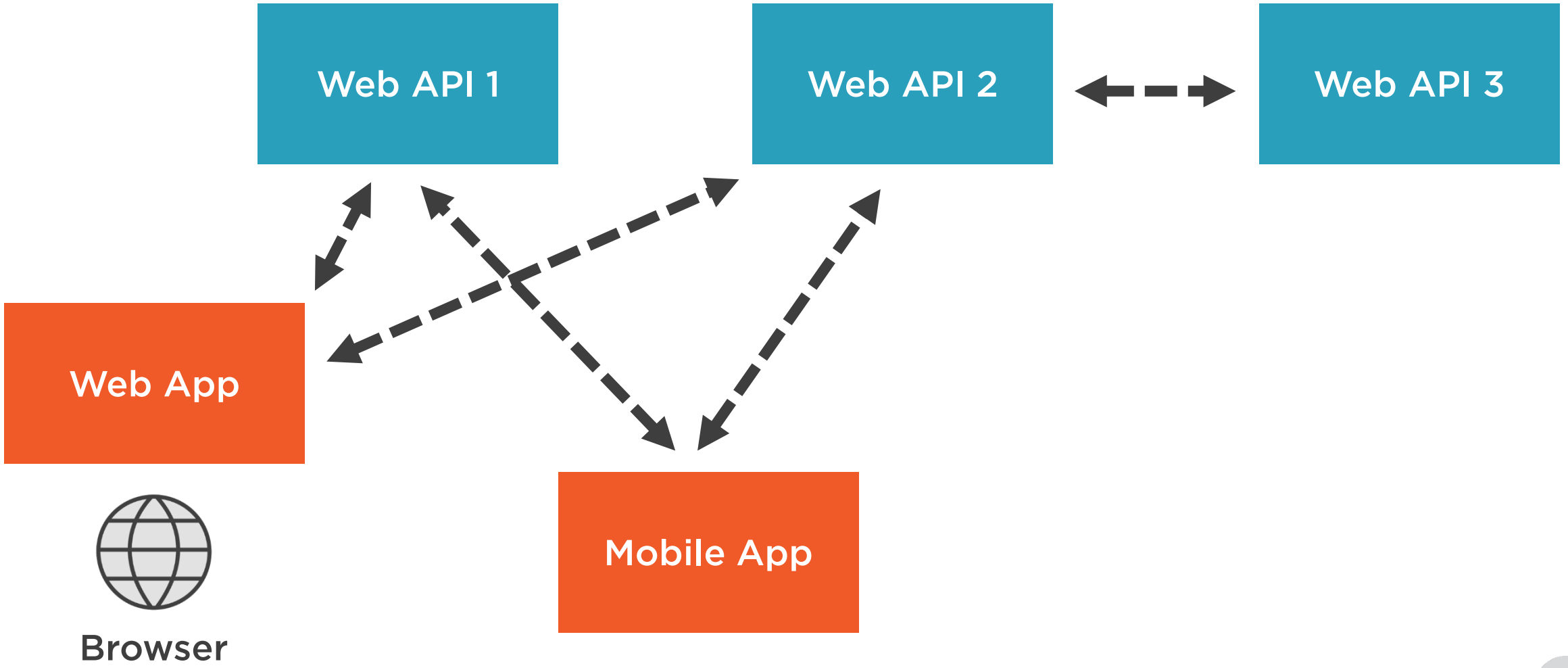
Configuring different kinds of clients to use the token service

Using different kinds of tokens

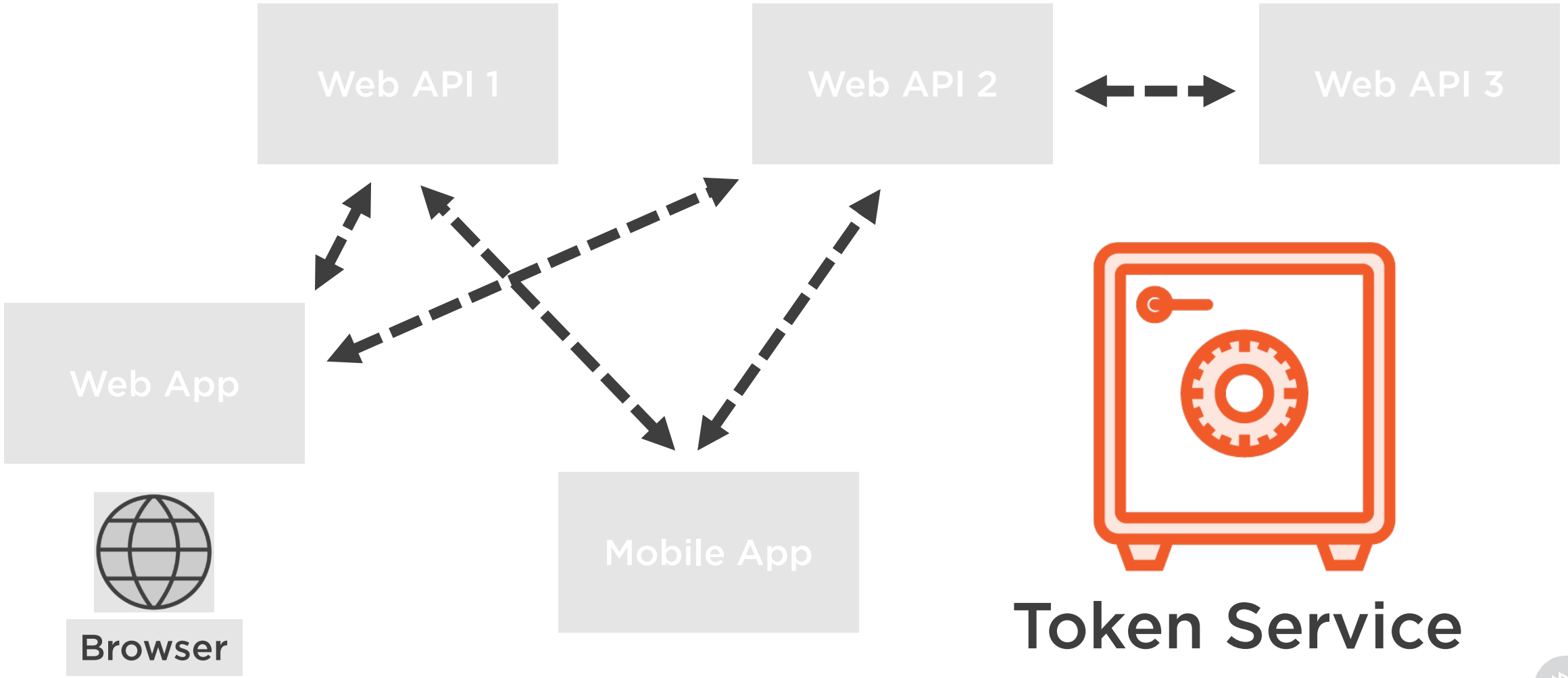
Utilizing IdentityServer endpoints

Using external authentication providers

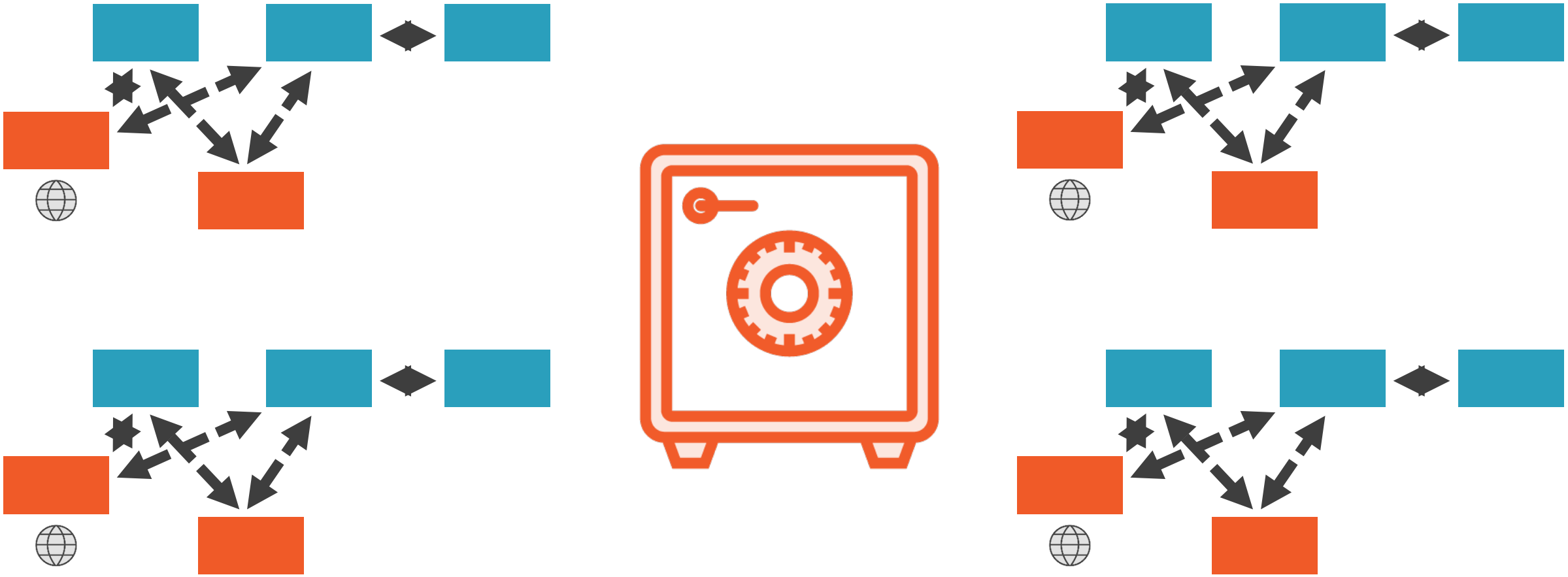
A Typical Modern Application



The Token Service



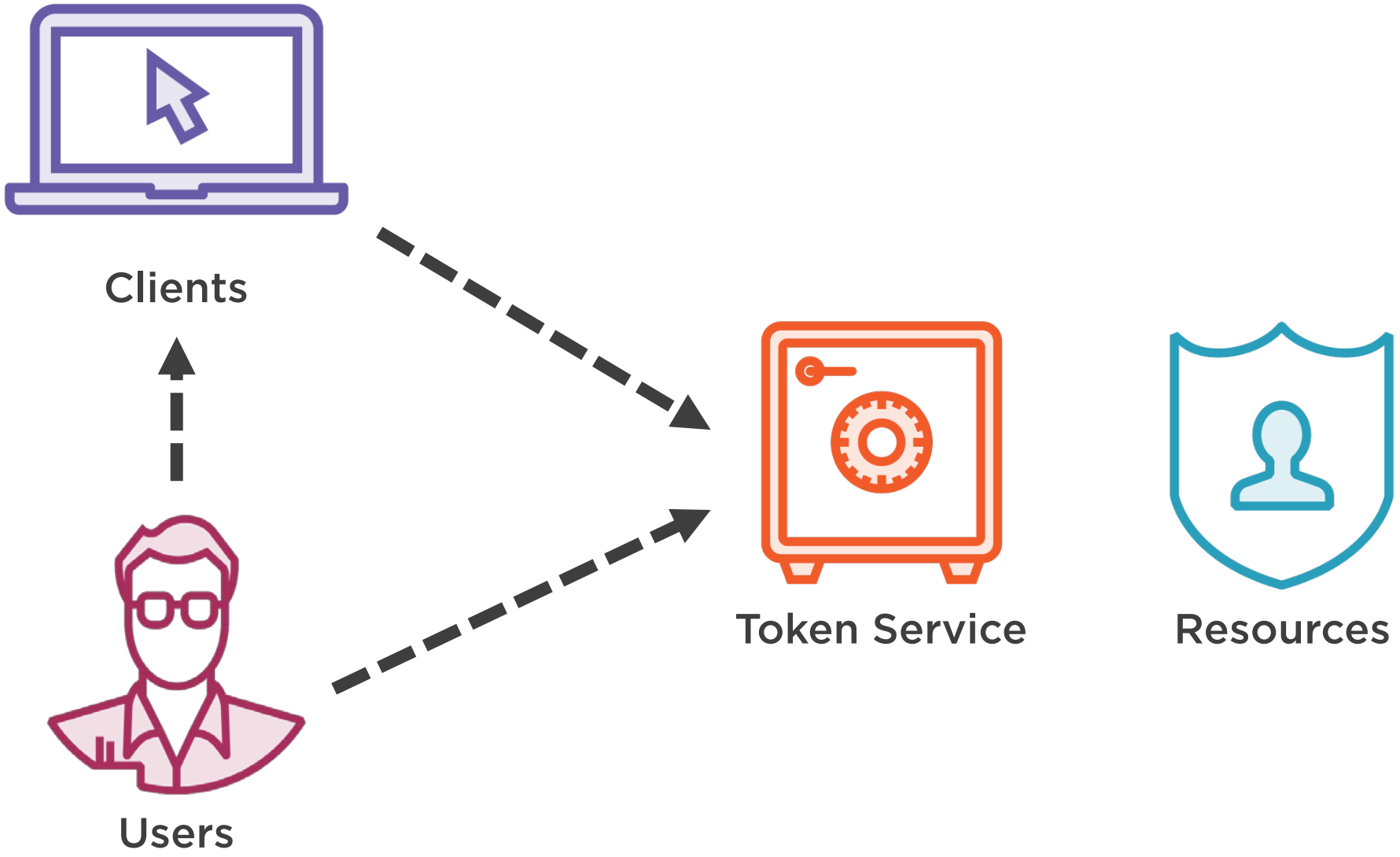
One Token Service to Rule Them All



IdentityServer

A framework that helps you to build a token service

Concepts



Example Implicit Client Application is requesting your permission

Uncheck the permissions you do not wish to grant.

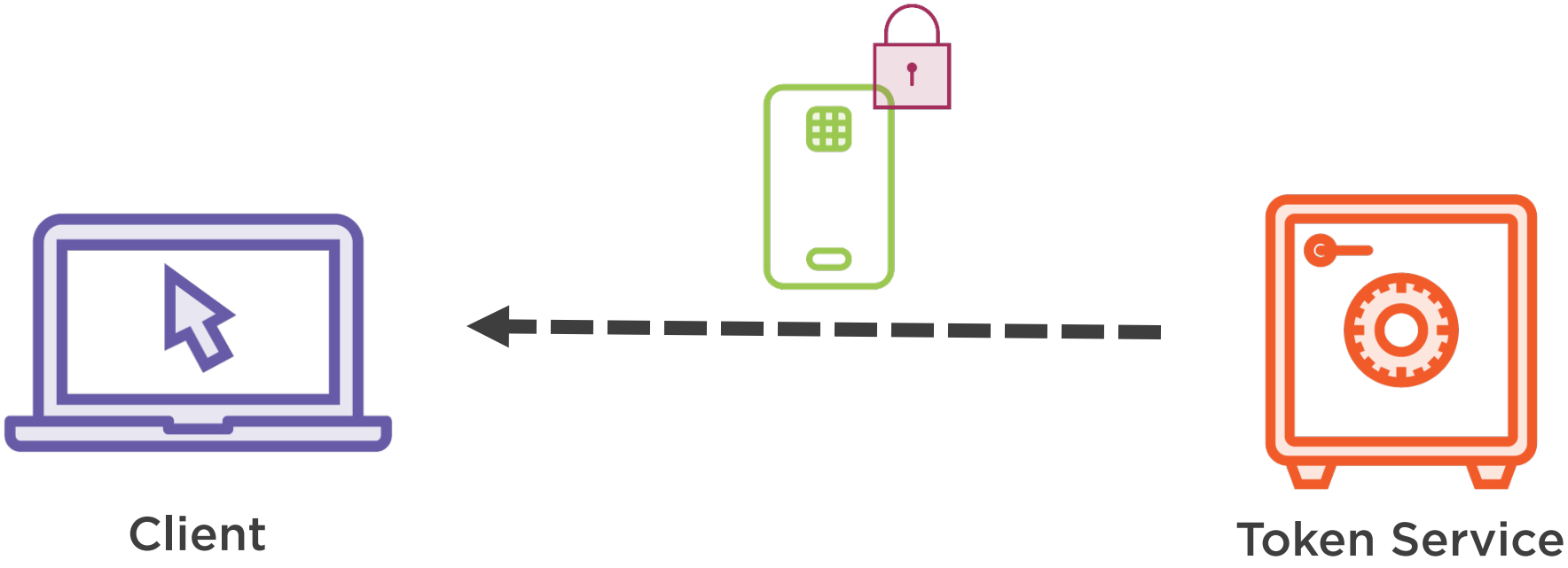
Personal Information

- **Your user identifier** *(required)*
- **User profile**
  Your user profile information (first name, last name, etc.)

Remember My Decision

Yes, Allow | No, Do Not Allow

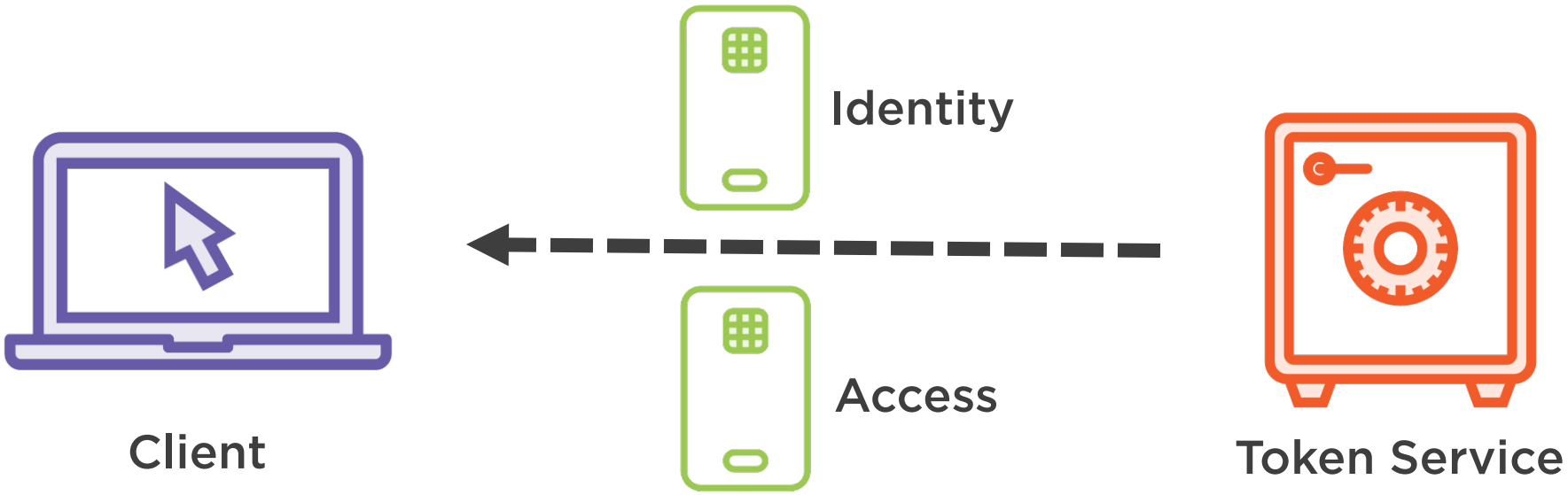
Tokens



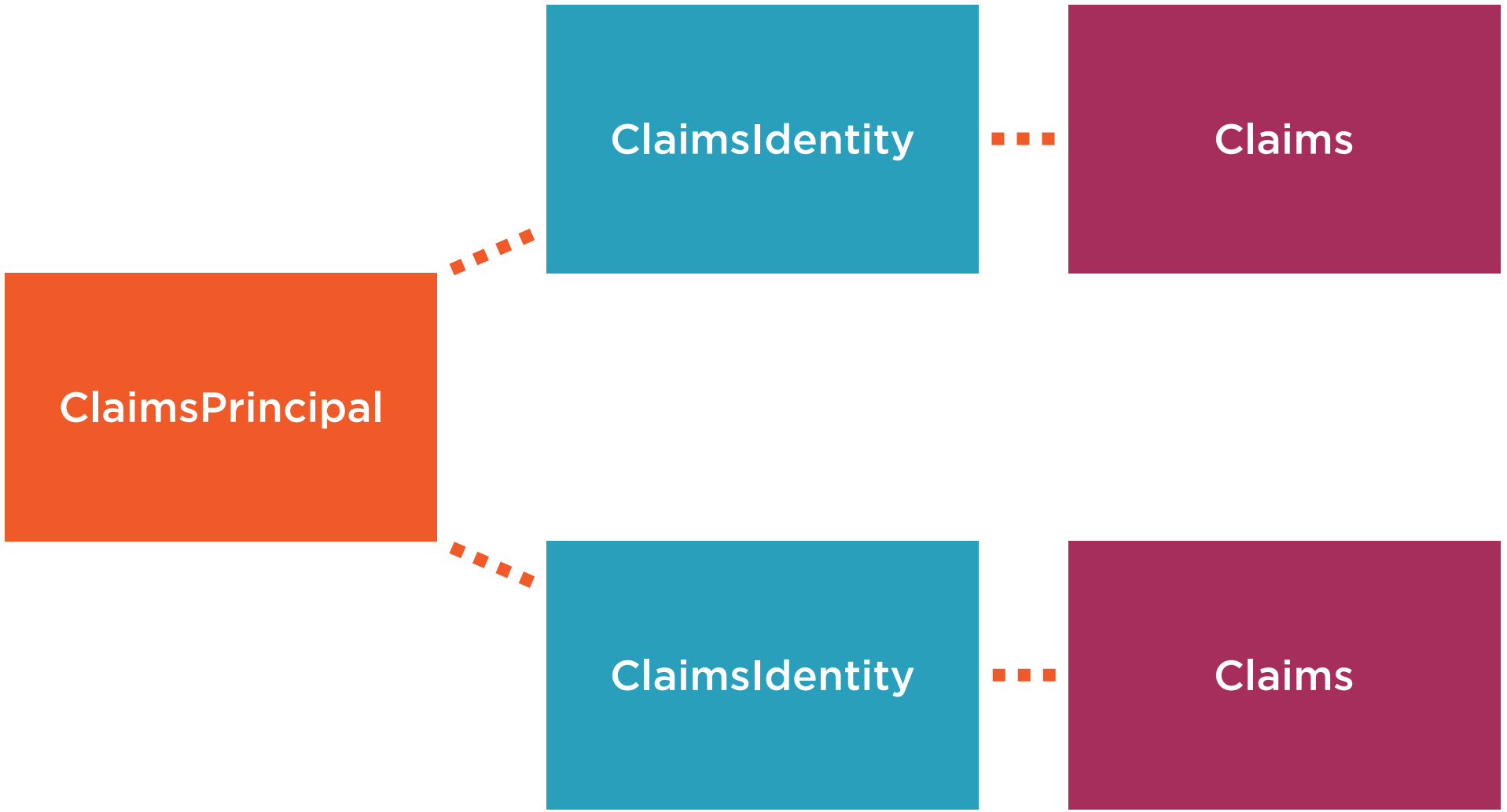
The JWT Token

```
{
  "typ": "JWT",
  "alg": "HS256"
}
{
  "iss": "tokenservice.com",
  "exp": 1300819380,
  “sub": “fd22zzx59ed",
  "name": "Roland Guijt",
  "role": "Admin"
}
```

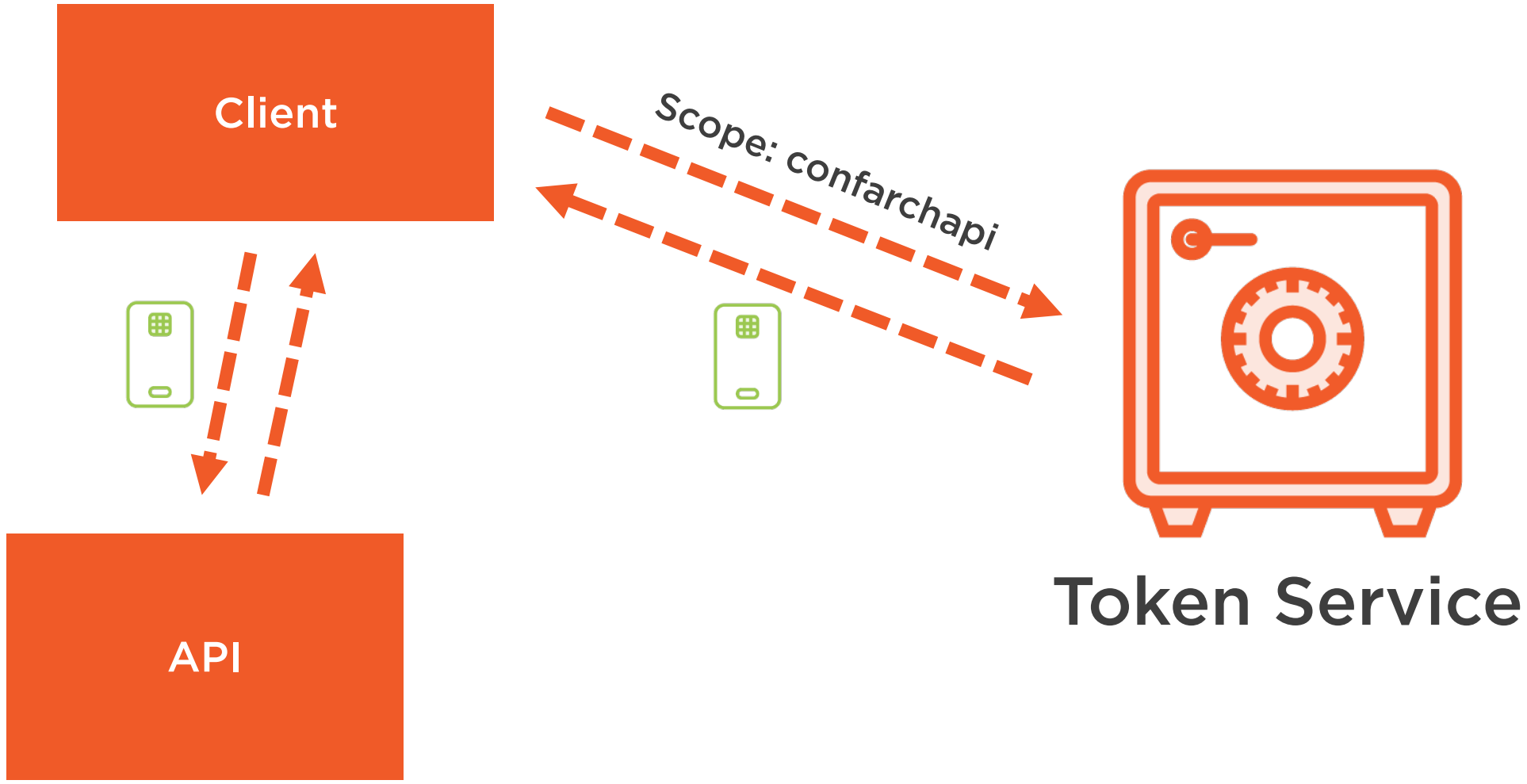
Tokens



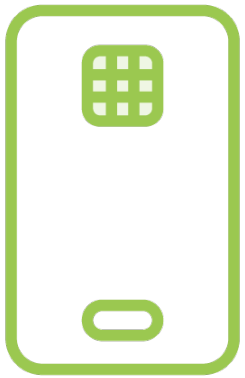
Claims-based Identity



Access Token Usage

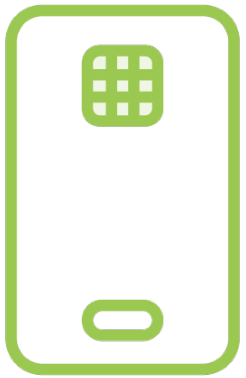


Standards



Identity

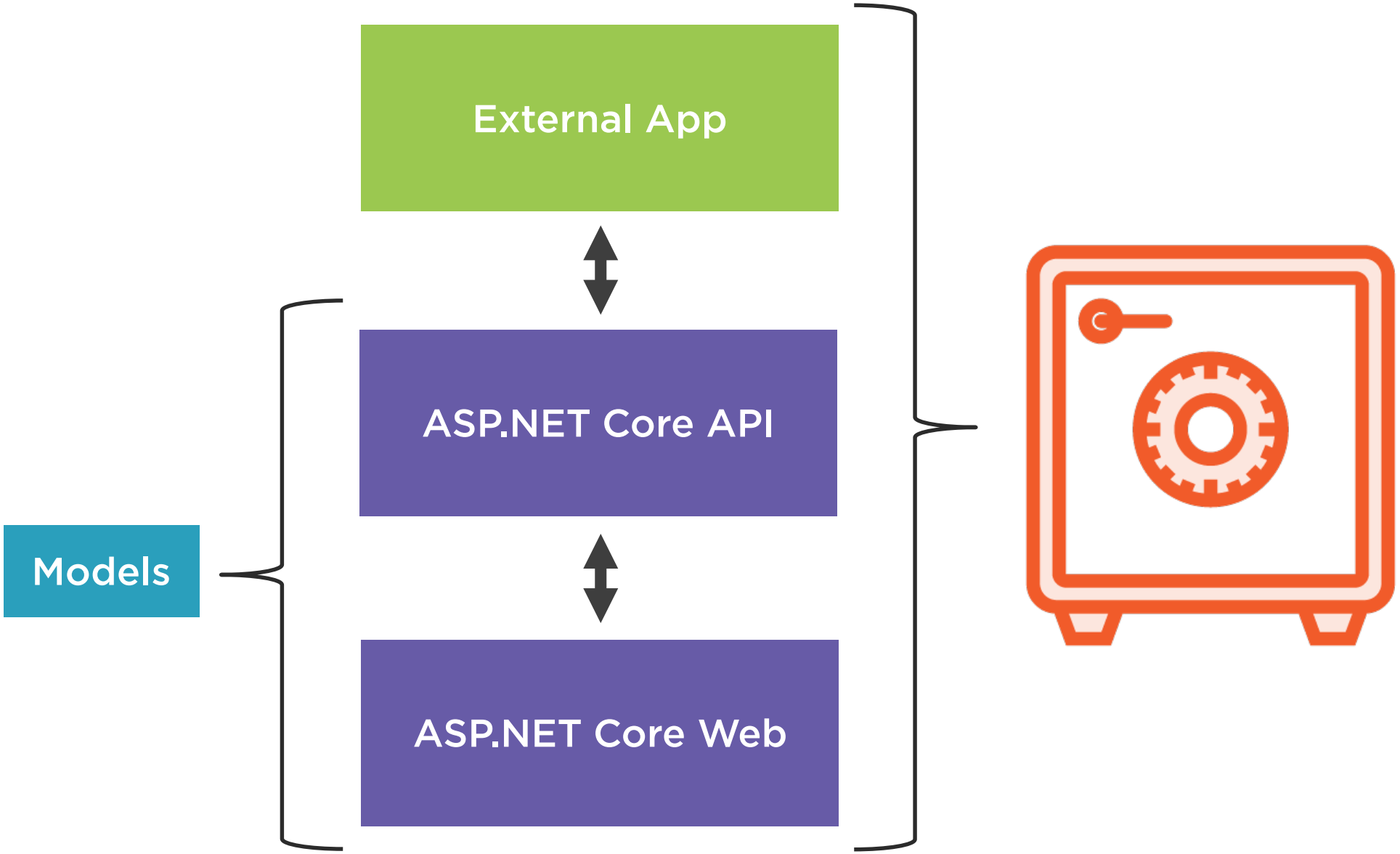
OpenID Connect (OIDC)



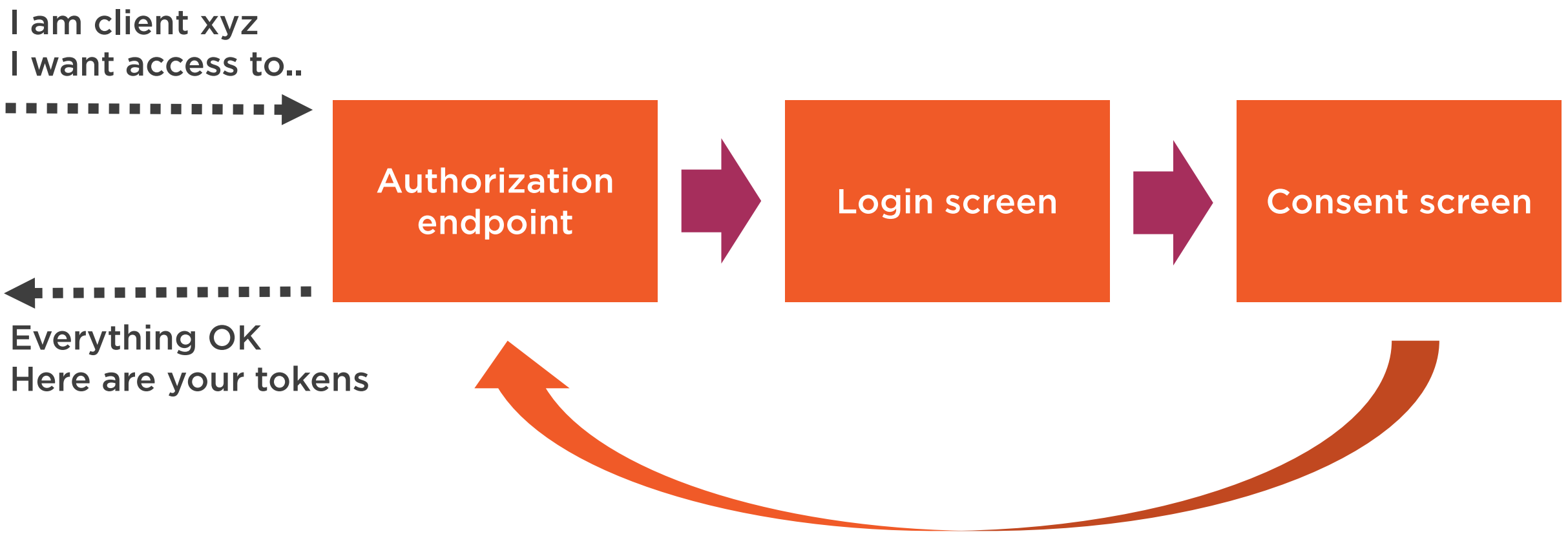
Access

OAuth2

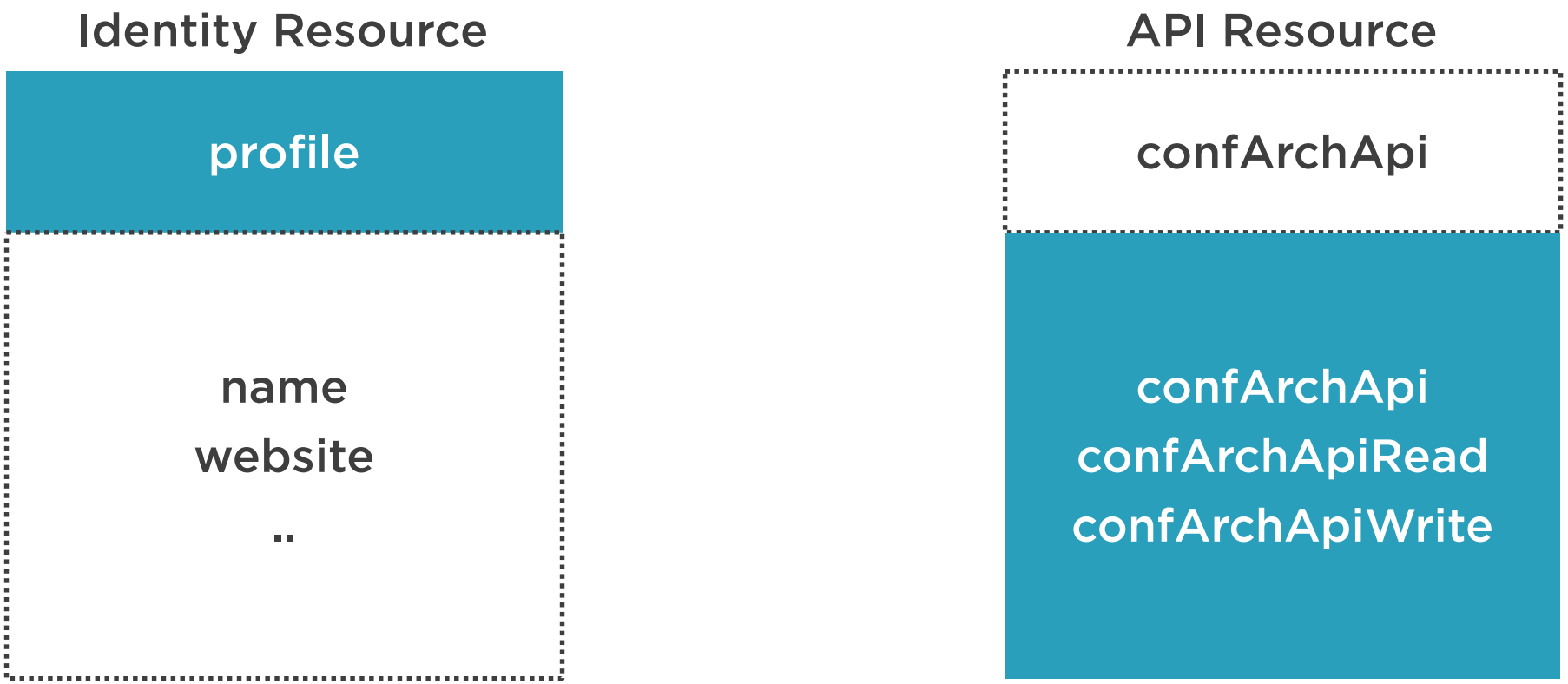
New ConfArch Architecture



Authenticating with a Token Service



Resources and Scopes



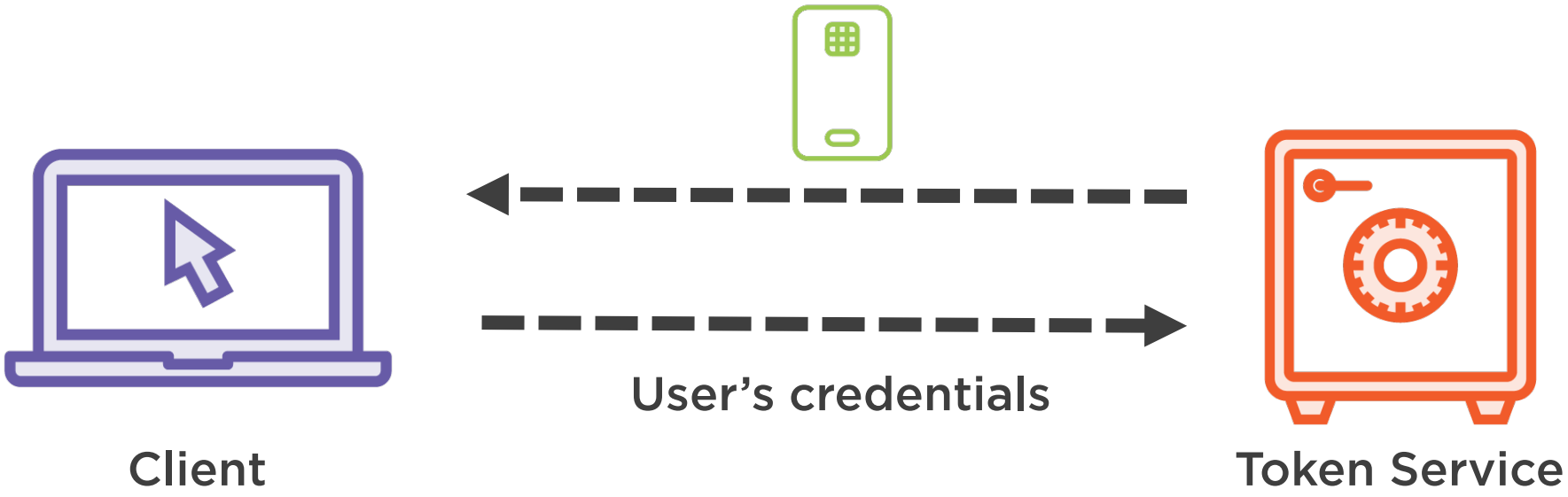
The blue is what a client requests

Grant

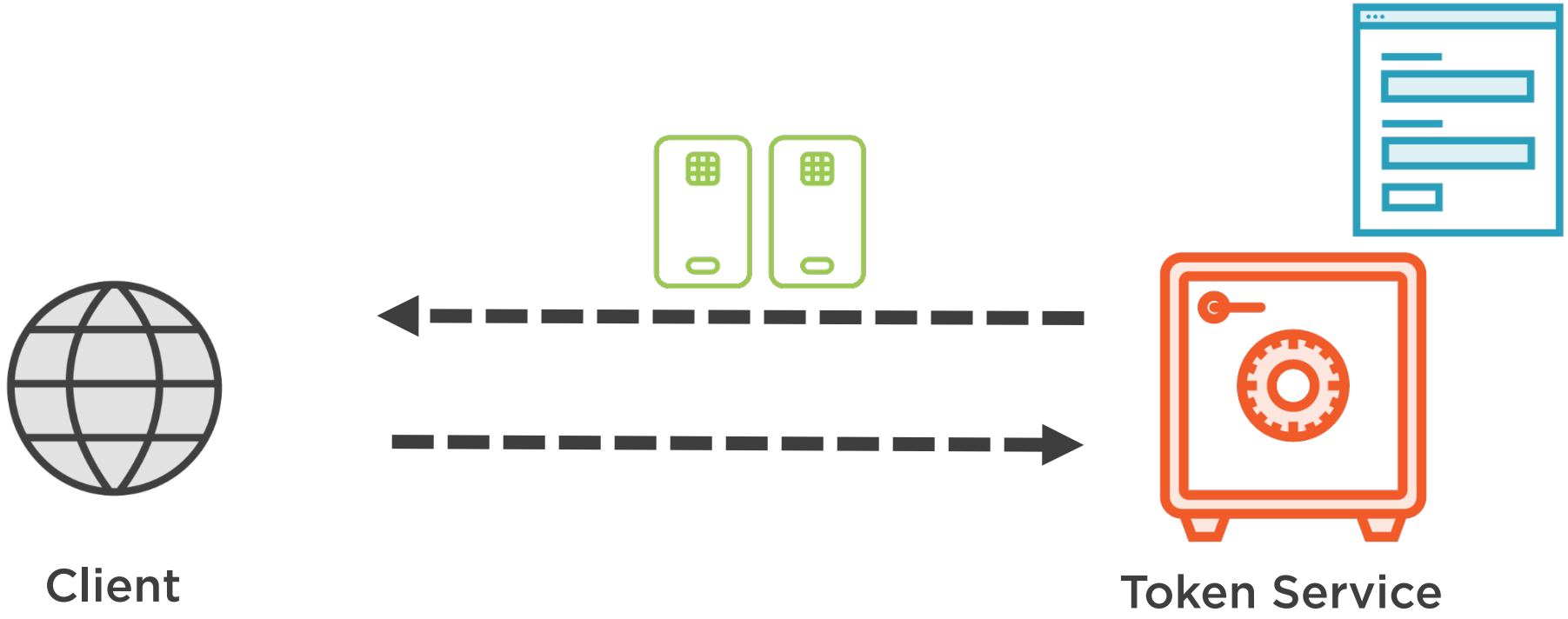
A way to get the tokens from the token service.

It uses a workflow.

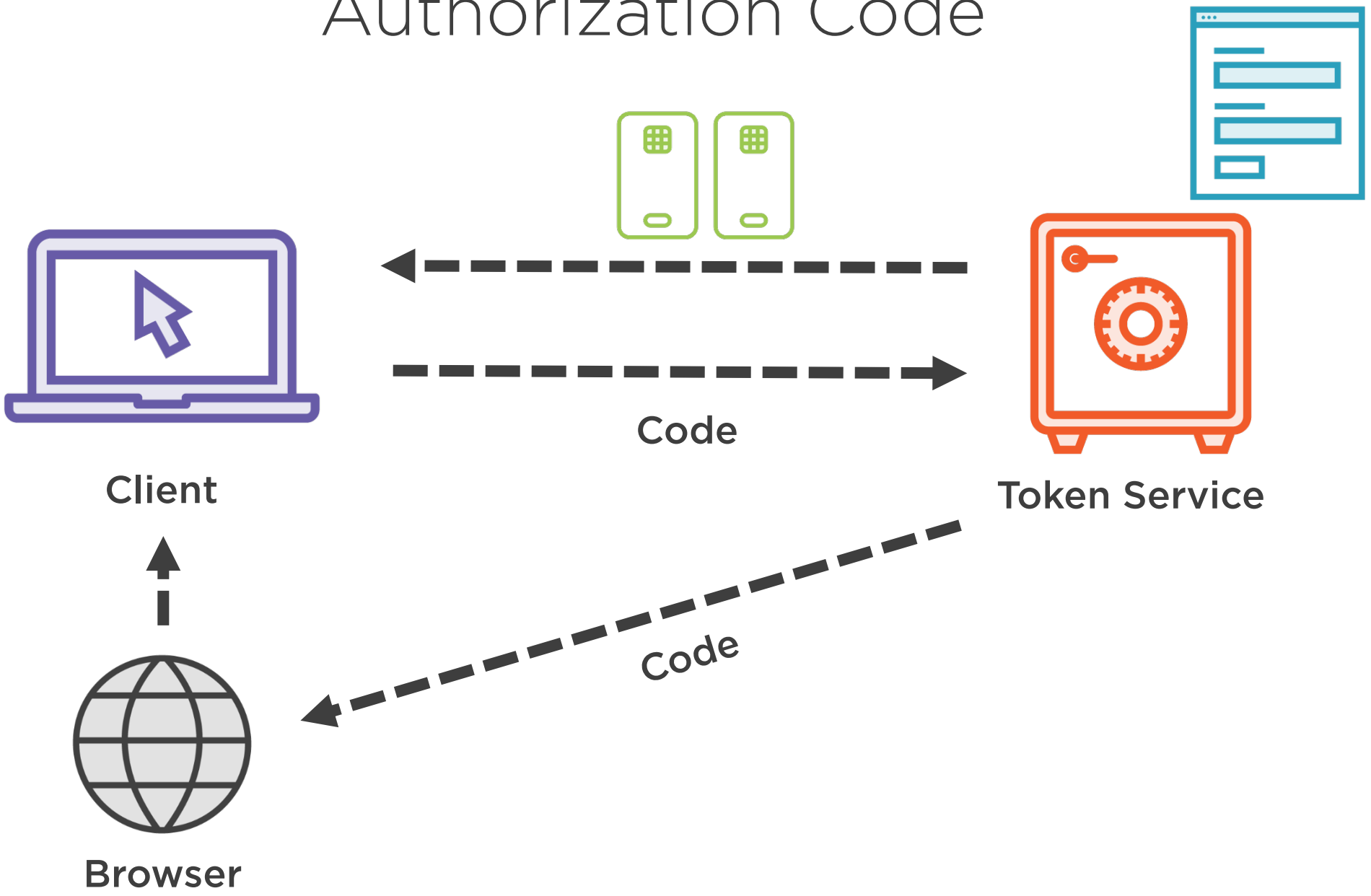
Resource Owner Password



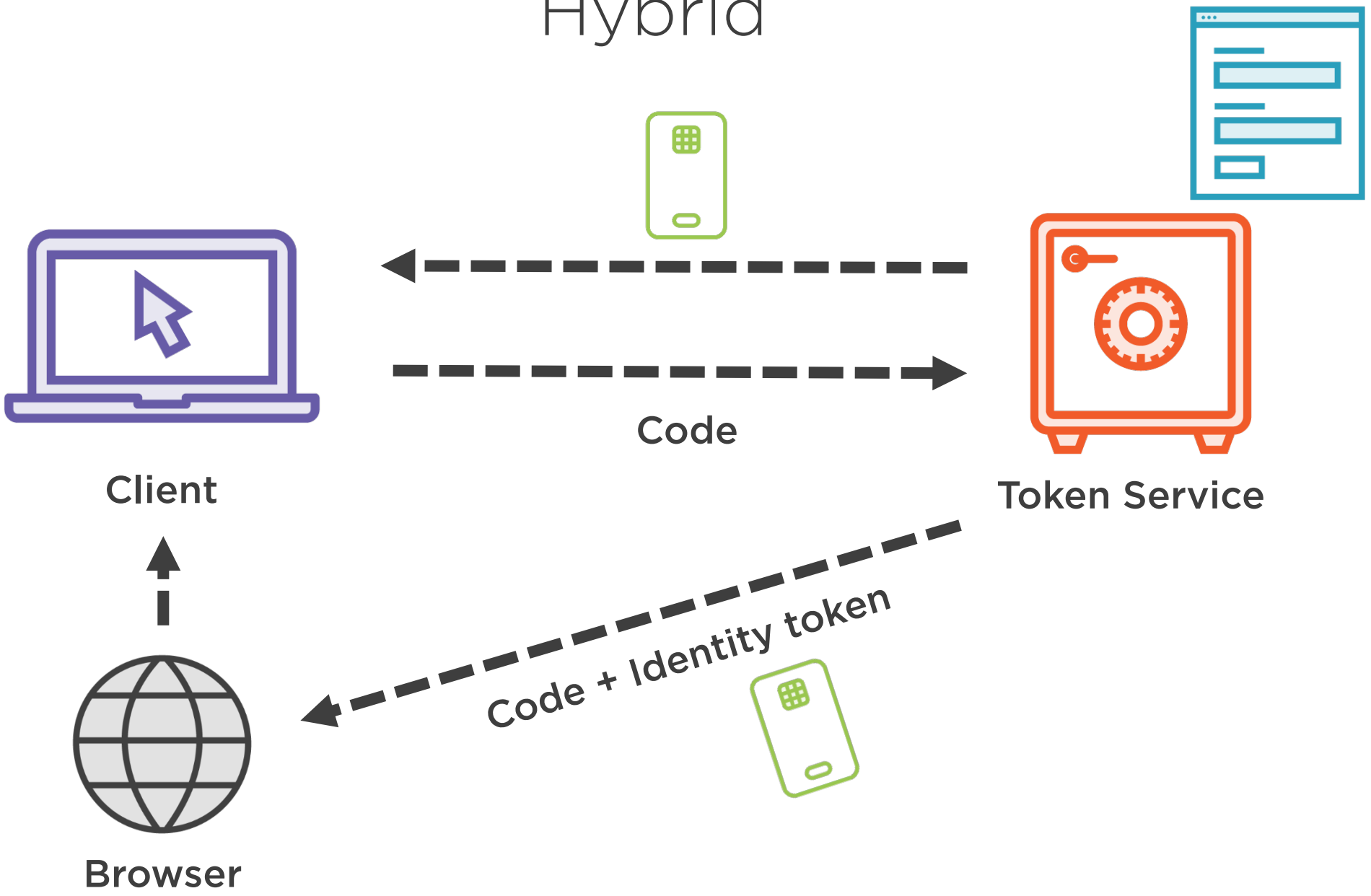
Implicit



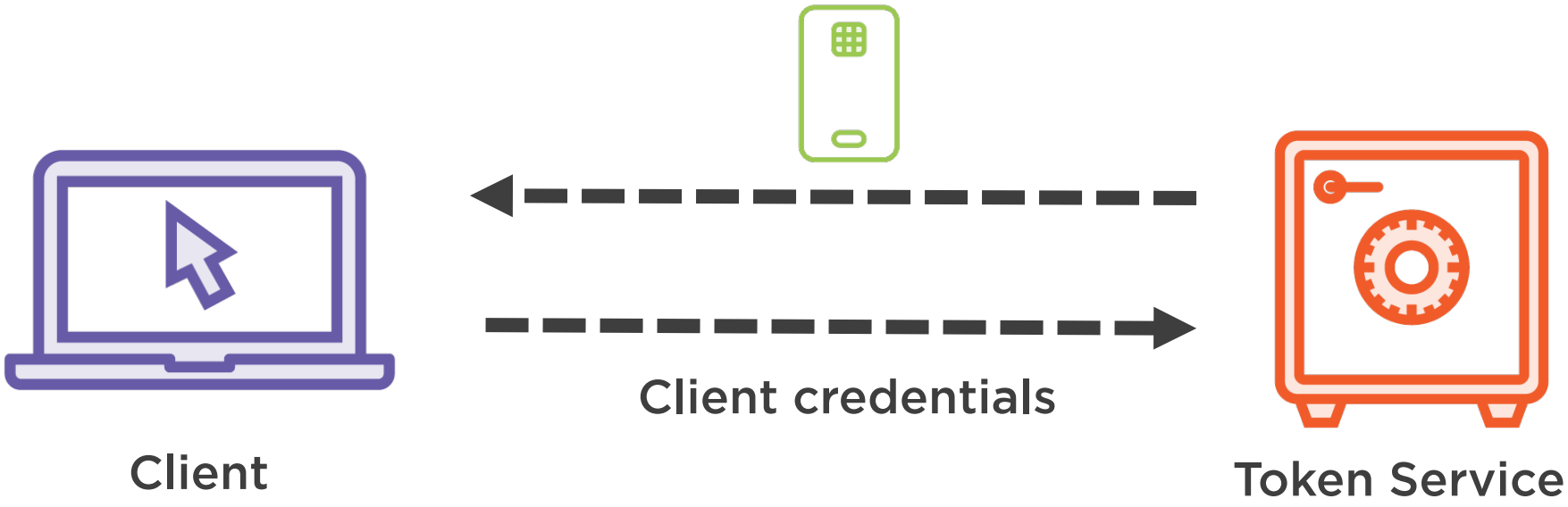
Authorization Code



Hybrid



Client Credentials



Adding a Database

In memory configuration only suitable for demo scenarios

Add a database using Entity Framework Core

IdentityServer.EntityFramework

Microsoft.EntityFrameworkCore.SqlServer

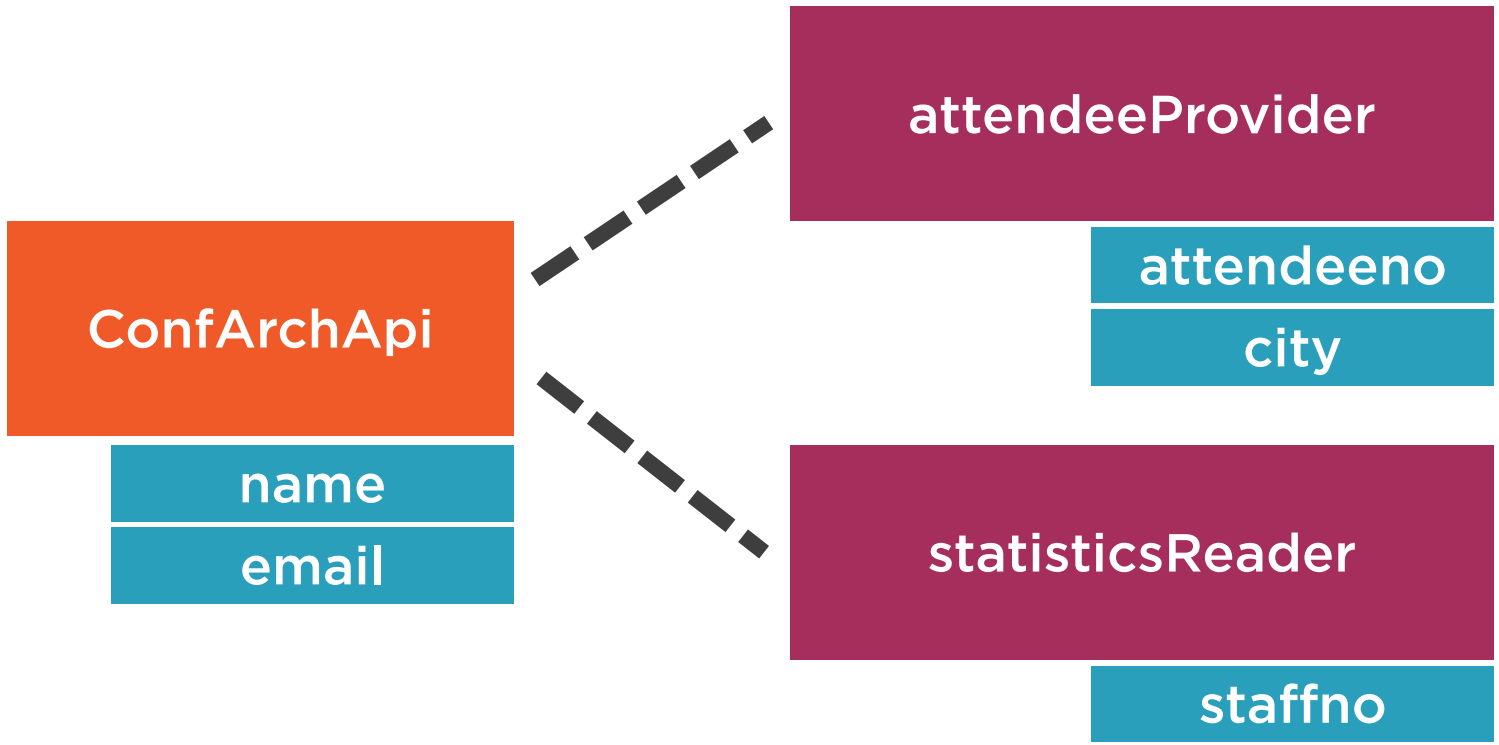
Microsoft.EntityFrameworkCore.Tools

Running the Migrations

```
dotnet ef migrations add InitialPersistedGrant
-c PersistedGrantDbContext
-o Migrations/IdentityServer/PersistedGrantDb

dotnet ef migrations add InitialConfiguration
-c ConfigurationDbContext
-o Migrations/IdentityServer/ConfigurationDb
```

An API Resource with Multiple Scopes



Adding a User Store

Create your own

Use ASP.NET Core Identity

Plugging in ASP.NET Core Identity

```
services.AddIdentityServer()
    .AddAspNetIdentity<ApplicationUser>();
```

Implementing IProfileService

```
public class ProfileService : IProfileService
{
    public Task GetProfileDataAsync(ProfileDataRequestContext context)
    {
        string subject = context.GetSubjectId();
        ...
    public Task IsActiveAsync(IsActiveContext context)
    {
        ...
```

Implementing IResourceOwnerPasswordValidator

```
public class ResourceOwnerPasswordValidator: IResourceOwnerPasswordValidator

{

    public Task<CustomGrantValidationResult> ValidateAsync(string userName,
        string password, ValidatedTokenRequest request)

    {

    ...
```

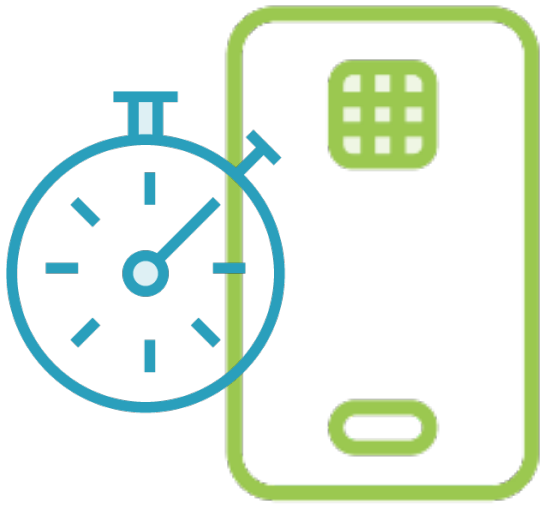
Registering the Classes

```
var builder = services.AddIdentityServer();

builder.Services.AddTransient<IResourceOwnerPasswordValidator,
   ResourceOwnerPasswordValidator>();

builder.Services.AddTransient<IProfileService, ProfileService>();
```

Refresh Tokens



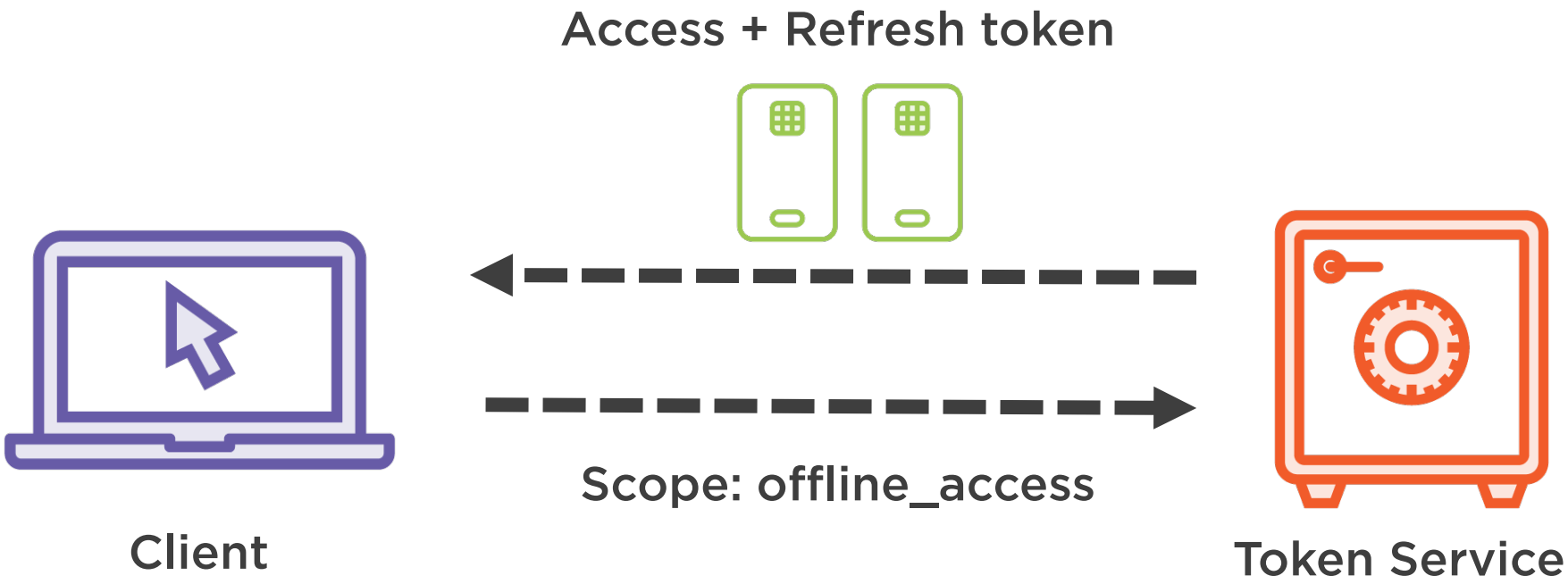
Refresh Tokens

A token to renew the access token

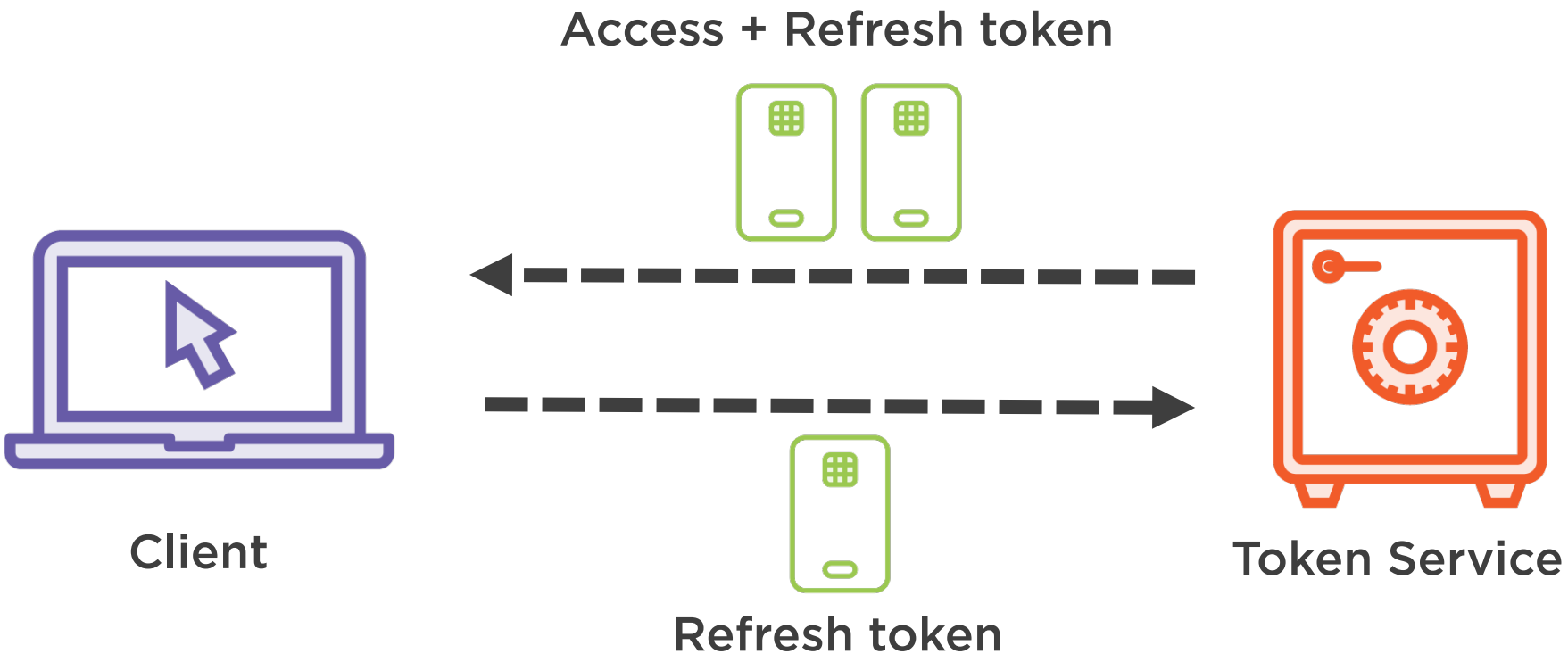
User doesn't have to re-authenticate

Longer expiration time than access token

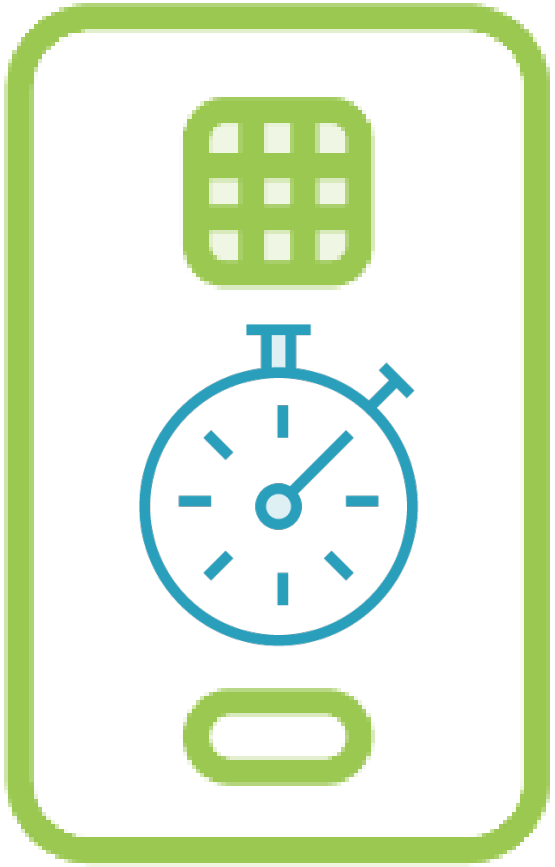
Refresh Tokens



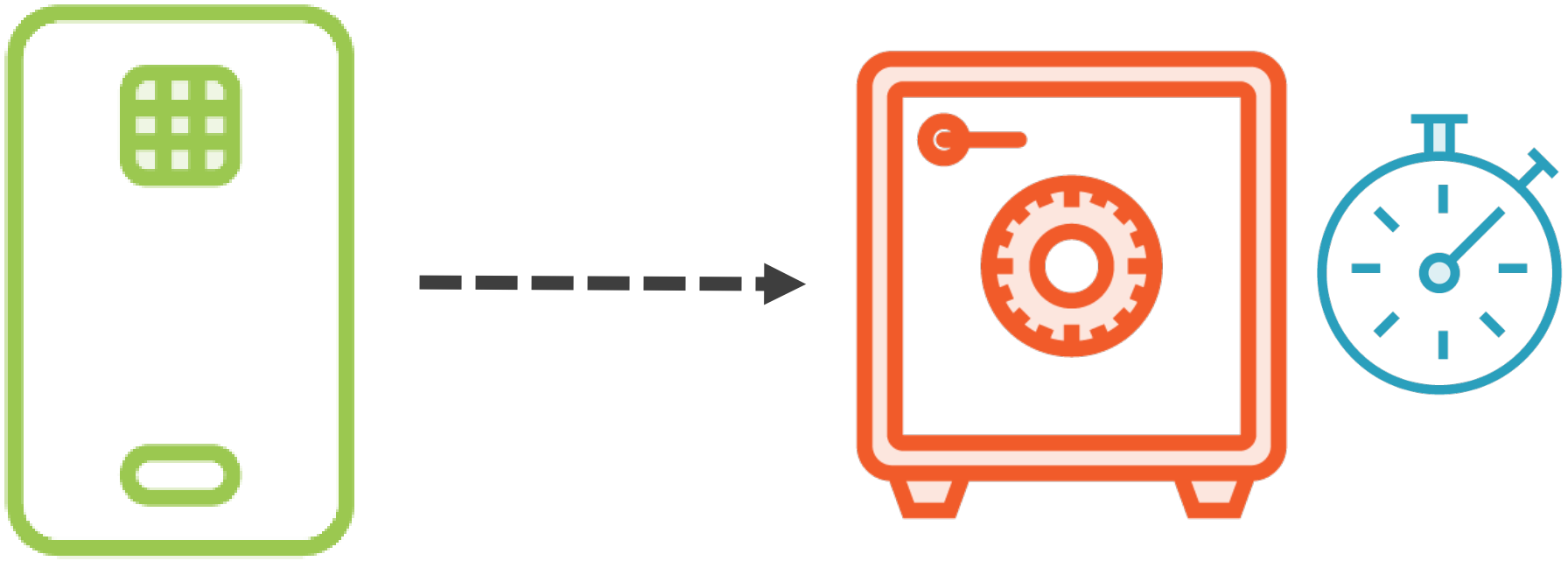
Refresh Tokens



Self-contained Access Tokens



Reference Tokens



Endpoints

- Authorize
- Token
- UserInfo
- Discovery
- End session
- Introspection
- Revocation

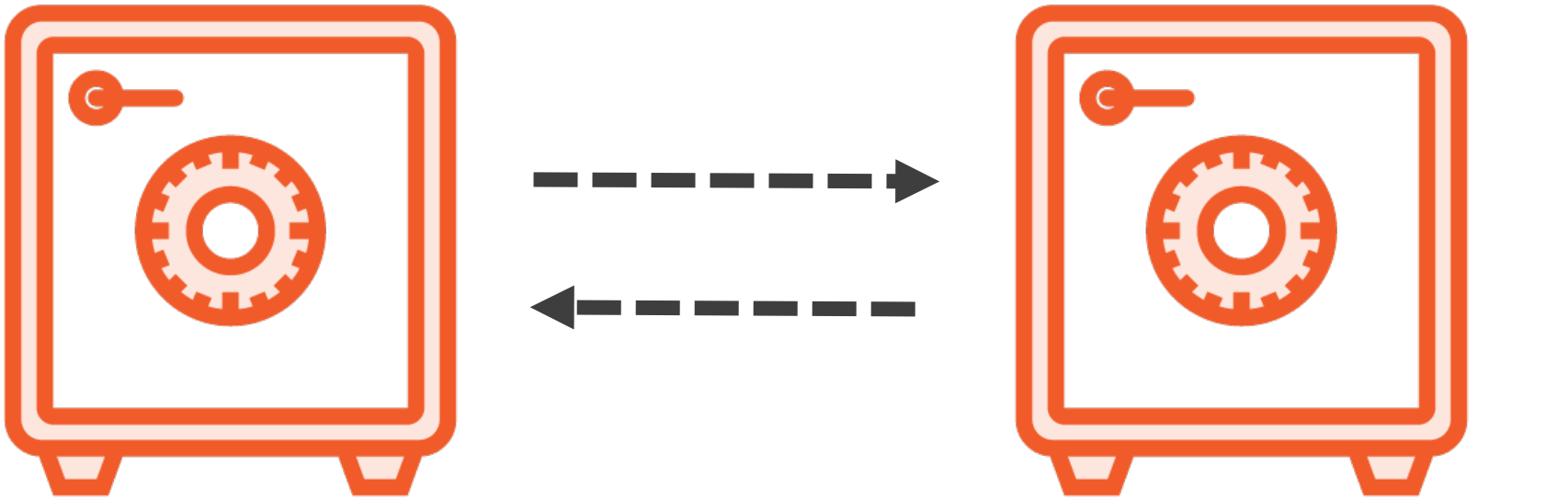
External Authentication Providers

Provide users with a possibility to login with an external account

User doesn’t have to remember the username and password for your app

Single signon

External Authentication Providers



Our tokenservice

Google's tokenservice

http://tinyurl.com/extprovs

Summary

Benefits of centralized token service

Users, clients, resources, scopes, claims

Tokens

Grants

Endpoints

External authentication providers