



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

A hand is shown from the right side, placing a single wooden block on top of a stack of three other wooden blocks. The blocks are light-colored wood and are arranged in a slightly staggered fashion. The background is a plain, light gray surface.

Rethinking Auth for SPAs and Micro Frontends: Easy and Secure With Gateways

Manfred Steyer, [ANGULARarchitects.io](https://angulararchitects.io)

Token-based Security

Authorization-Server



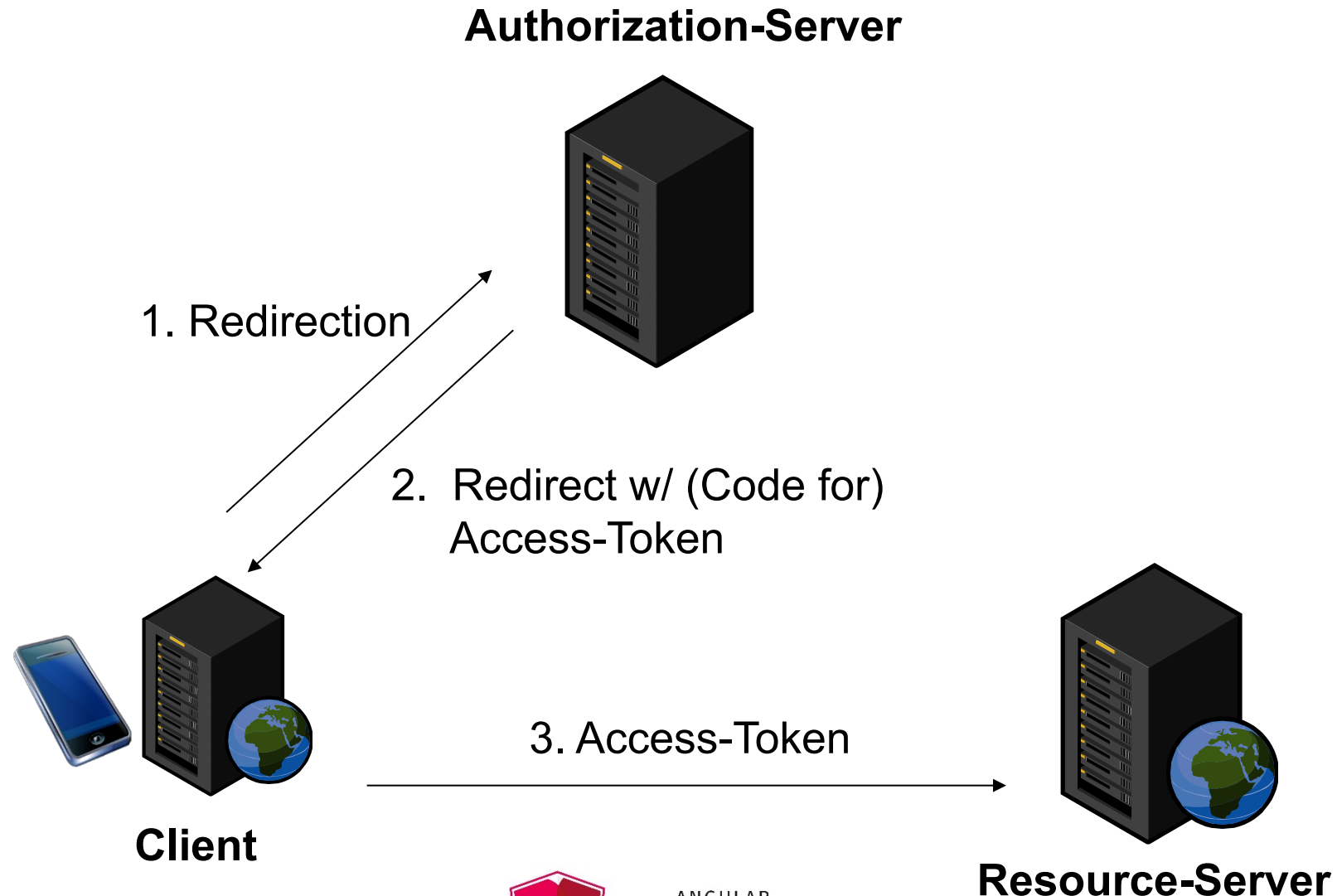
Client



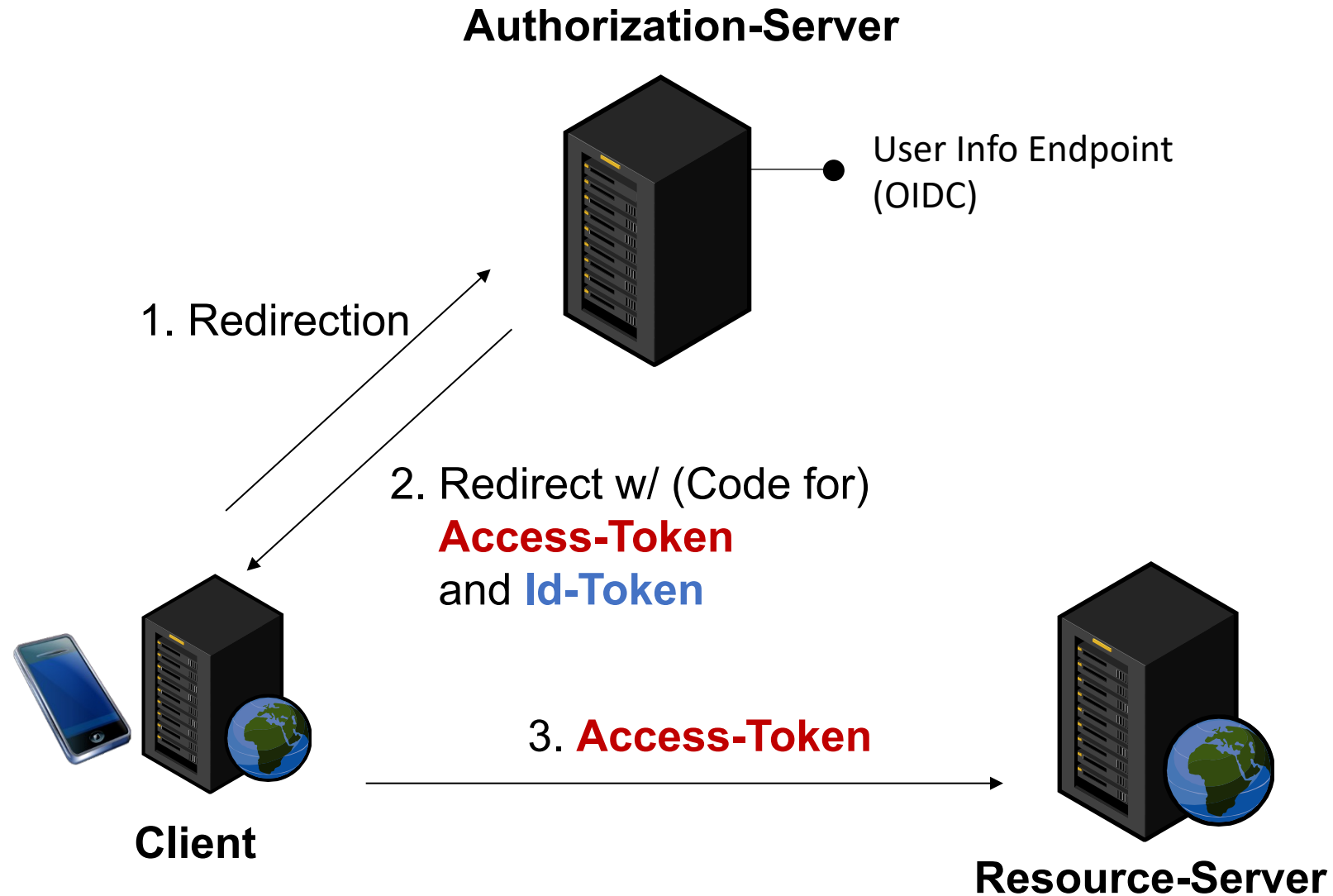
Resource-Server



OAuth 2



OpenId Connect



Where to **store** the tokens?
How to **refresh** tokens?



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

Contents

1)
"Modern"
OAuth 2

2)
Token Refresh

3) Auth
Gateways



#1: "Modern OAuth 2"



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

Current Best Practices Documents

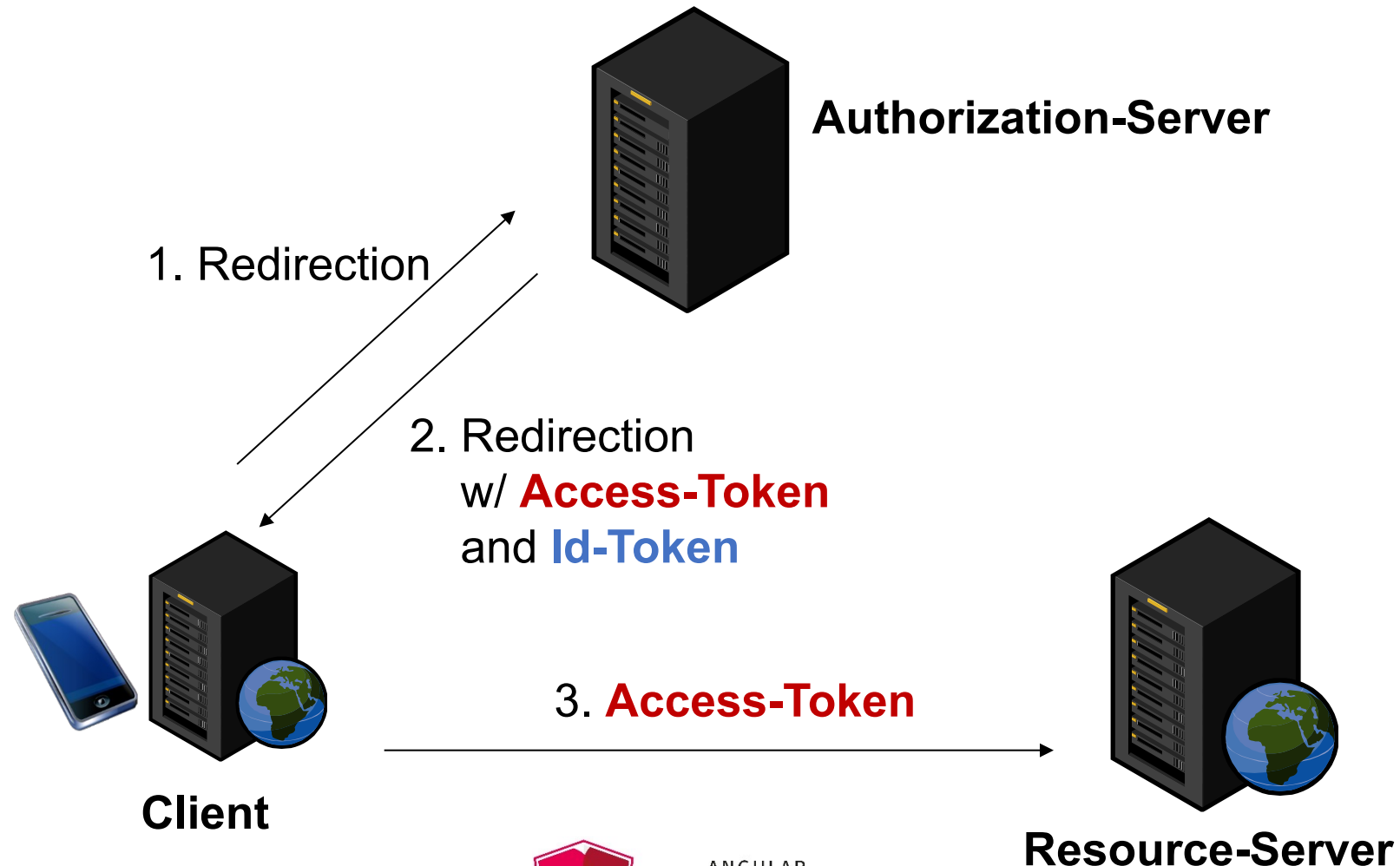
Advice Against Implicit Flow



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

Implicit Flow

(not recommended anymore)

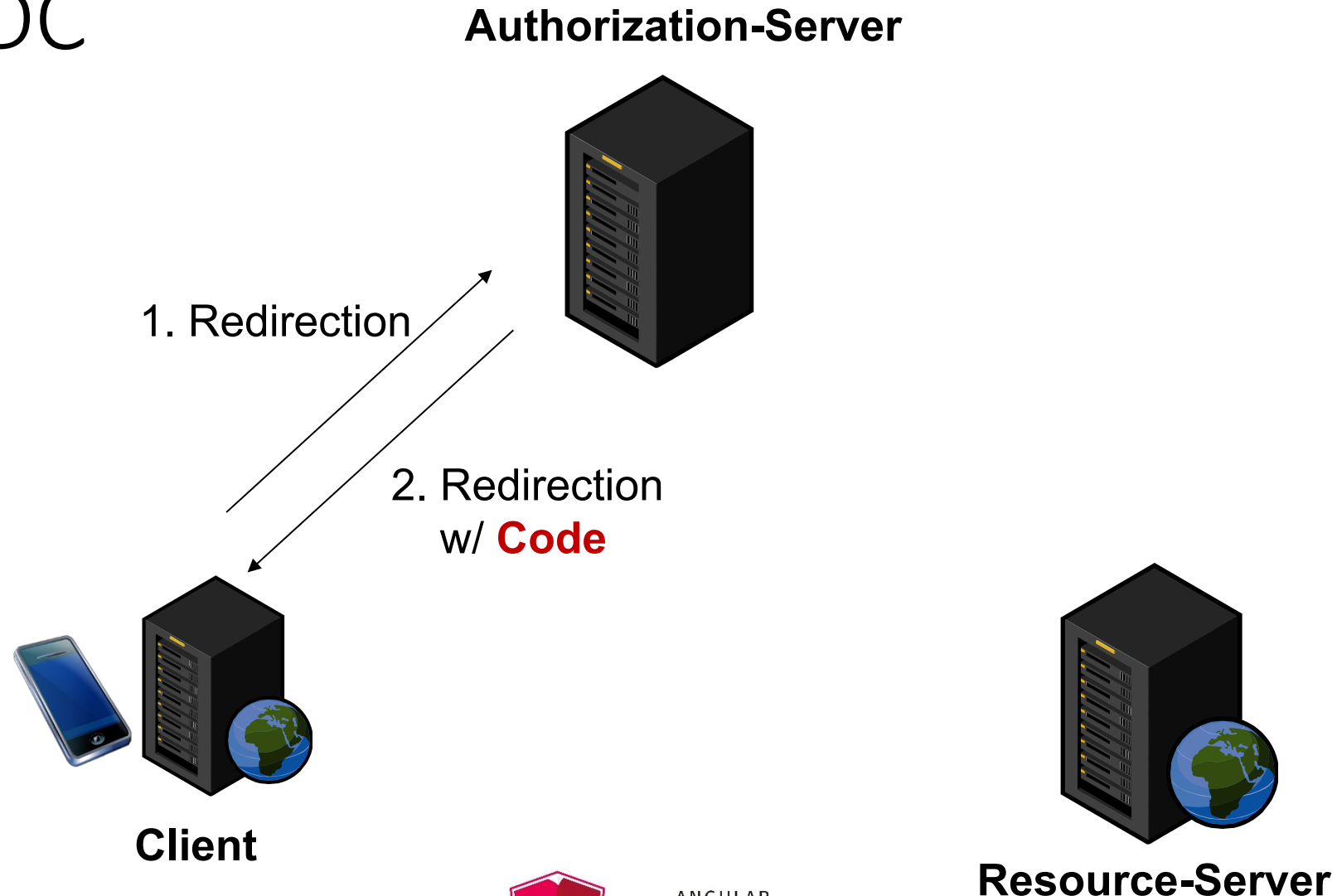


Proposed Solution

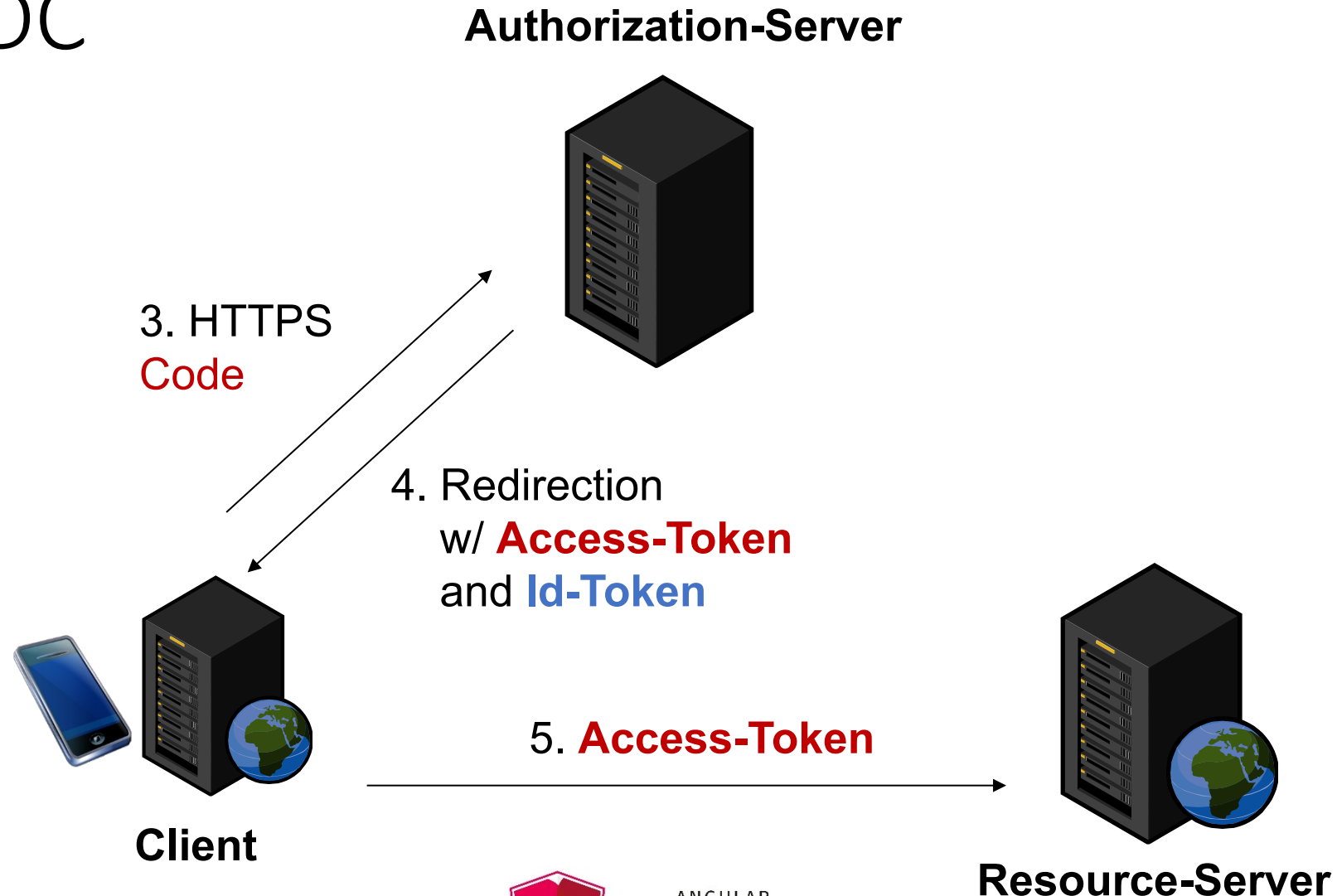


ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

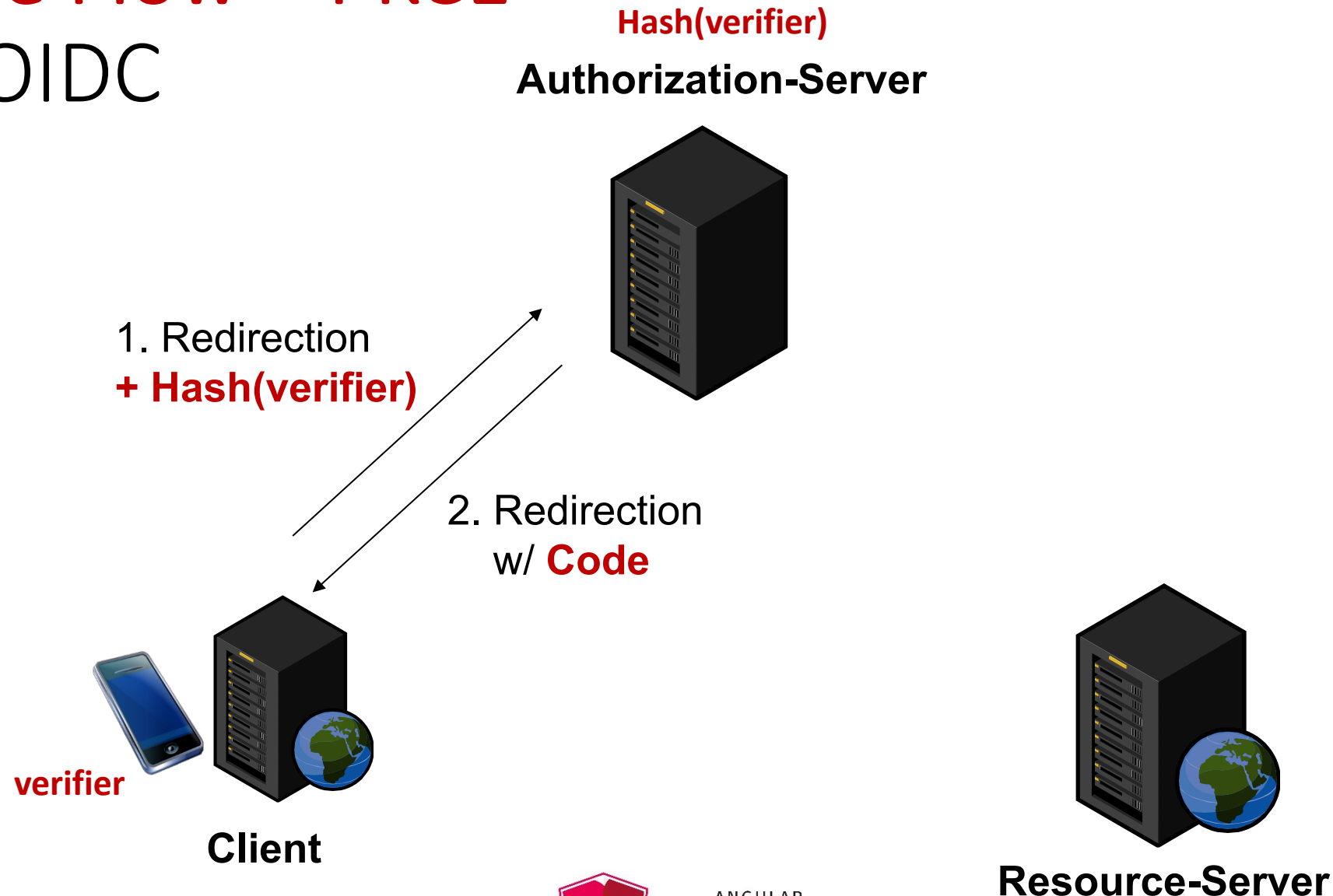
Code Flow w/ OIDC



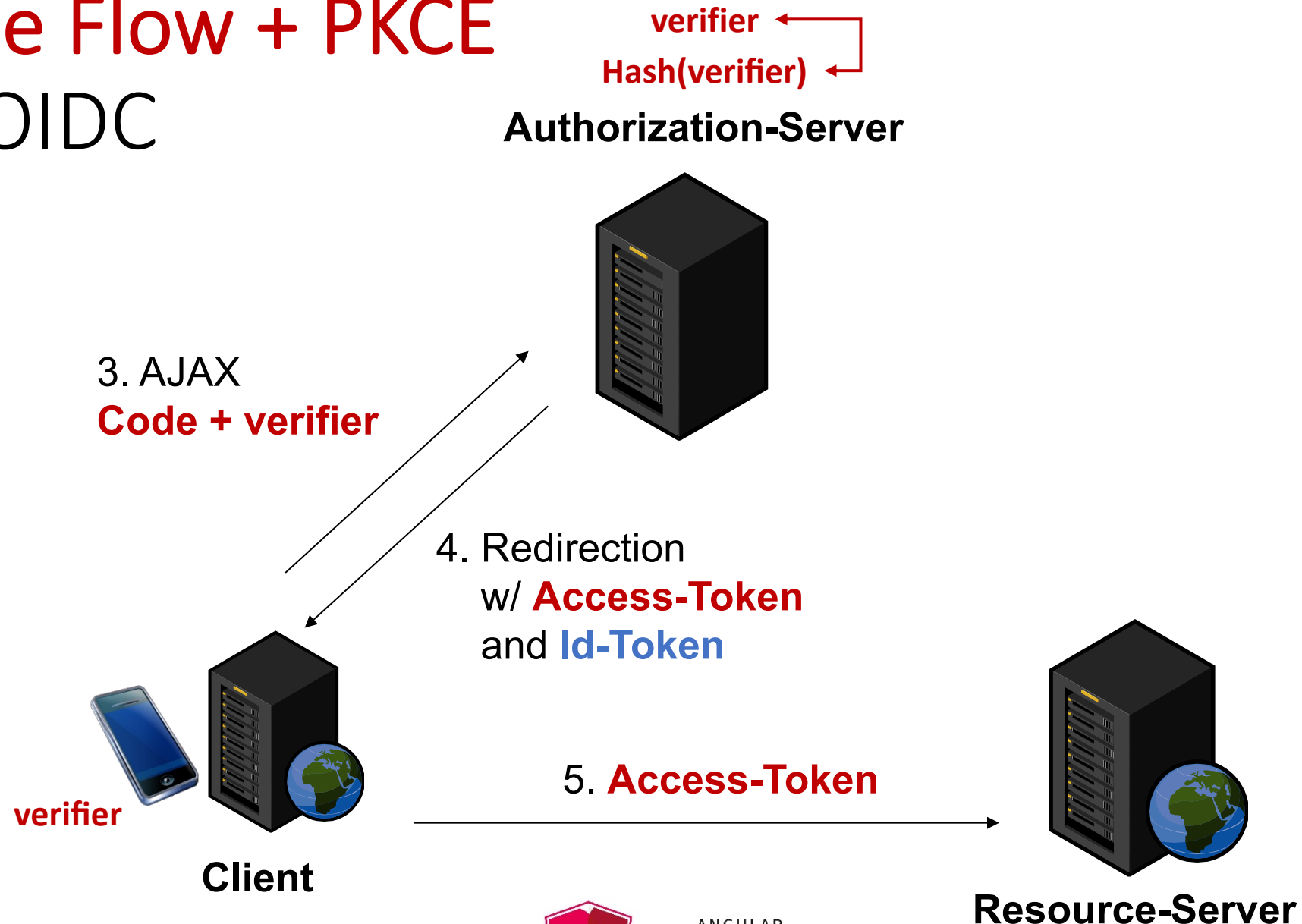
Code Flow w/ OIDC



Code Flow + PKCE w/ OIDC



Code Flow + PKCE w/ OIDC



Several suggestions for using OAuth 2 in a more secure way



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

Example: Using Code Flow + PKCE instead of Implicit Flow



Remaining Problem:
XSS -> Stealing Tokens



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

DEMO



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

LAB



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

#2: Token Refresh



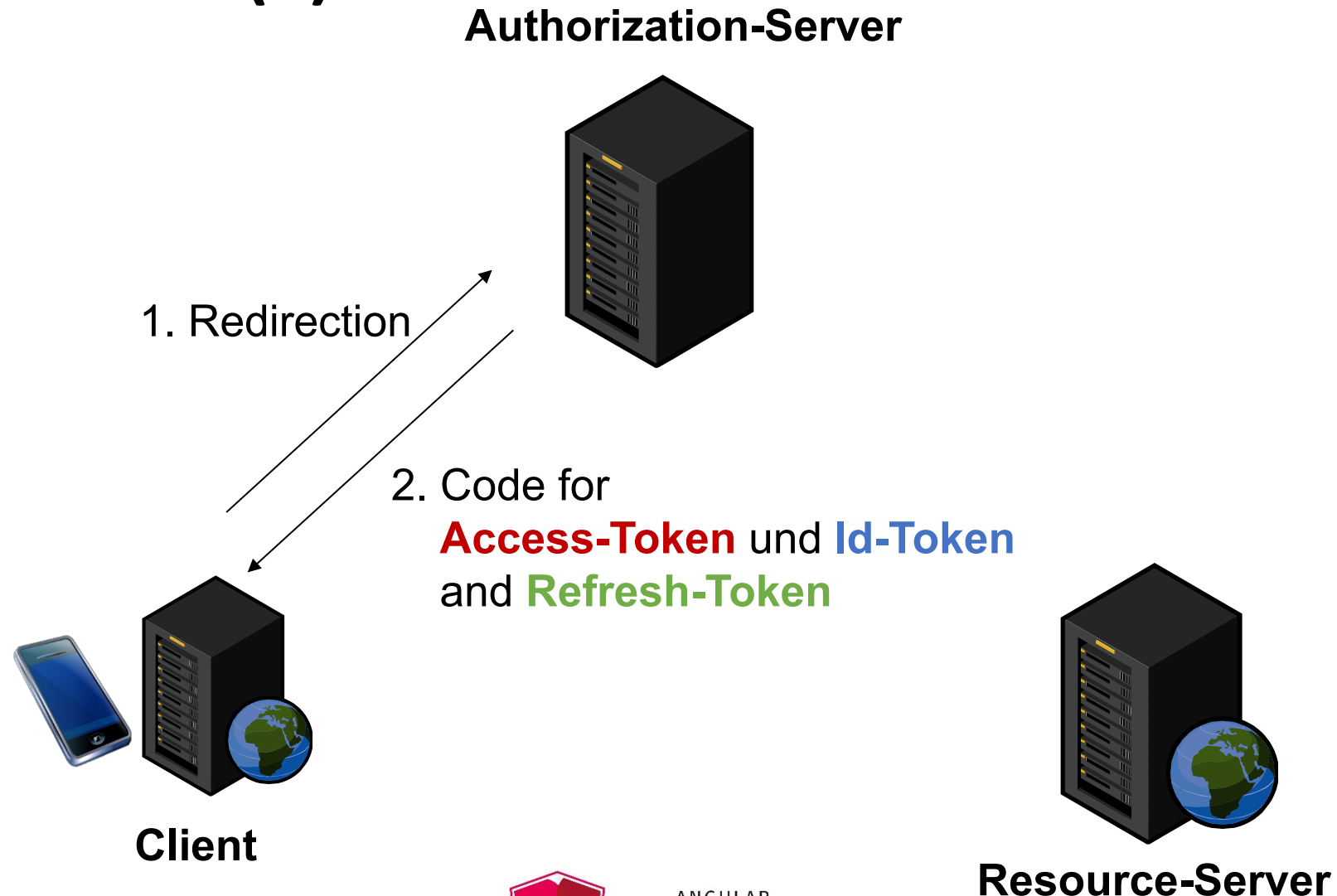
ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

Why Token Refresh?

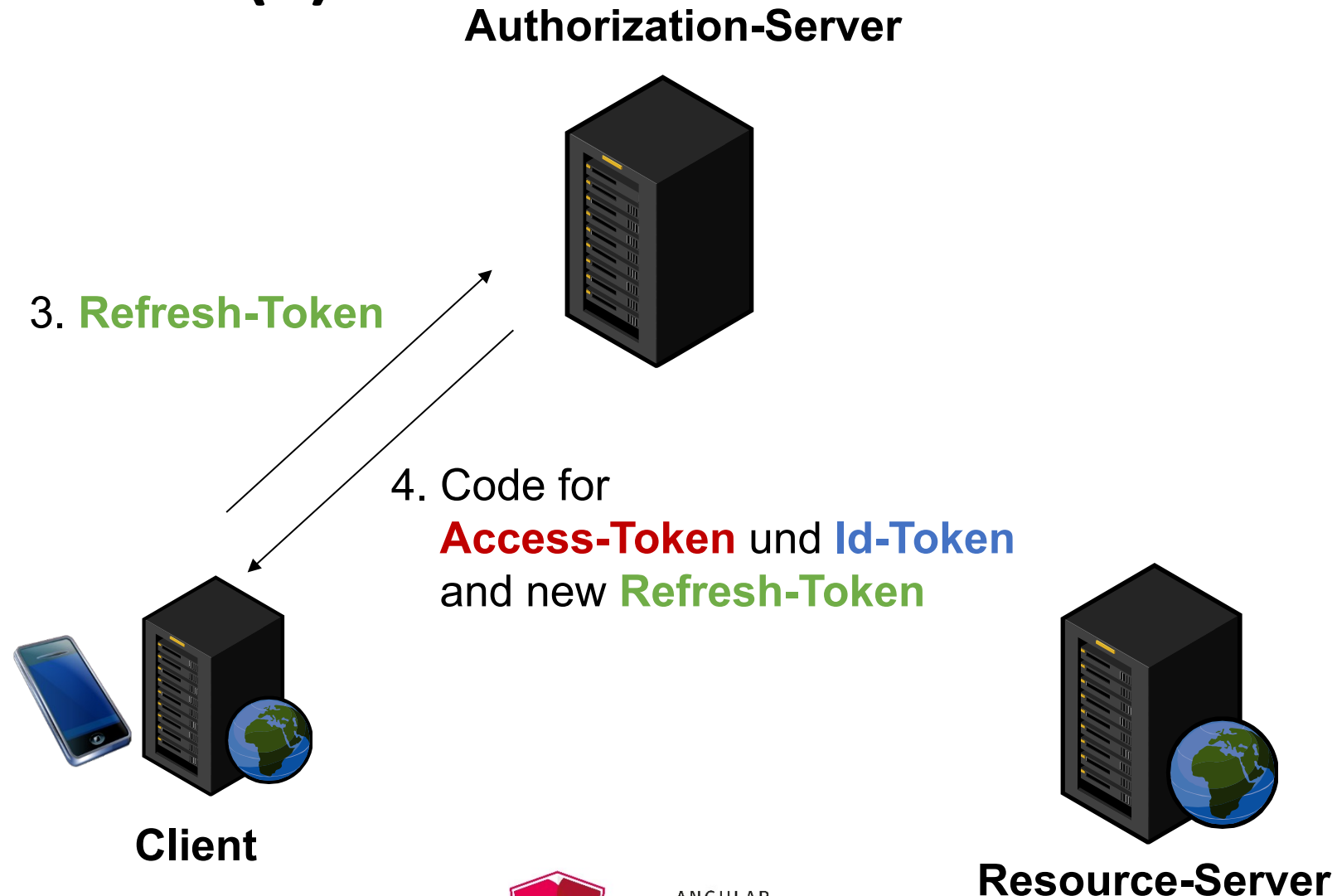
Short living Tokens
increase Security

Users don't want to
login over and over
again

Refresh Token (1)



Refresh Token (2)



Refresh Tokens in the Browser?

Forbidden by
Standards

Allowed by
Current Best
Practices*

* in specific situations ...



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

#3: Auth Gateways



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

JavaScript Application with a Backend

Server-side
OAuth

Store Tokens
on Server

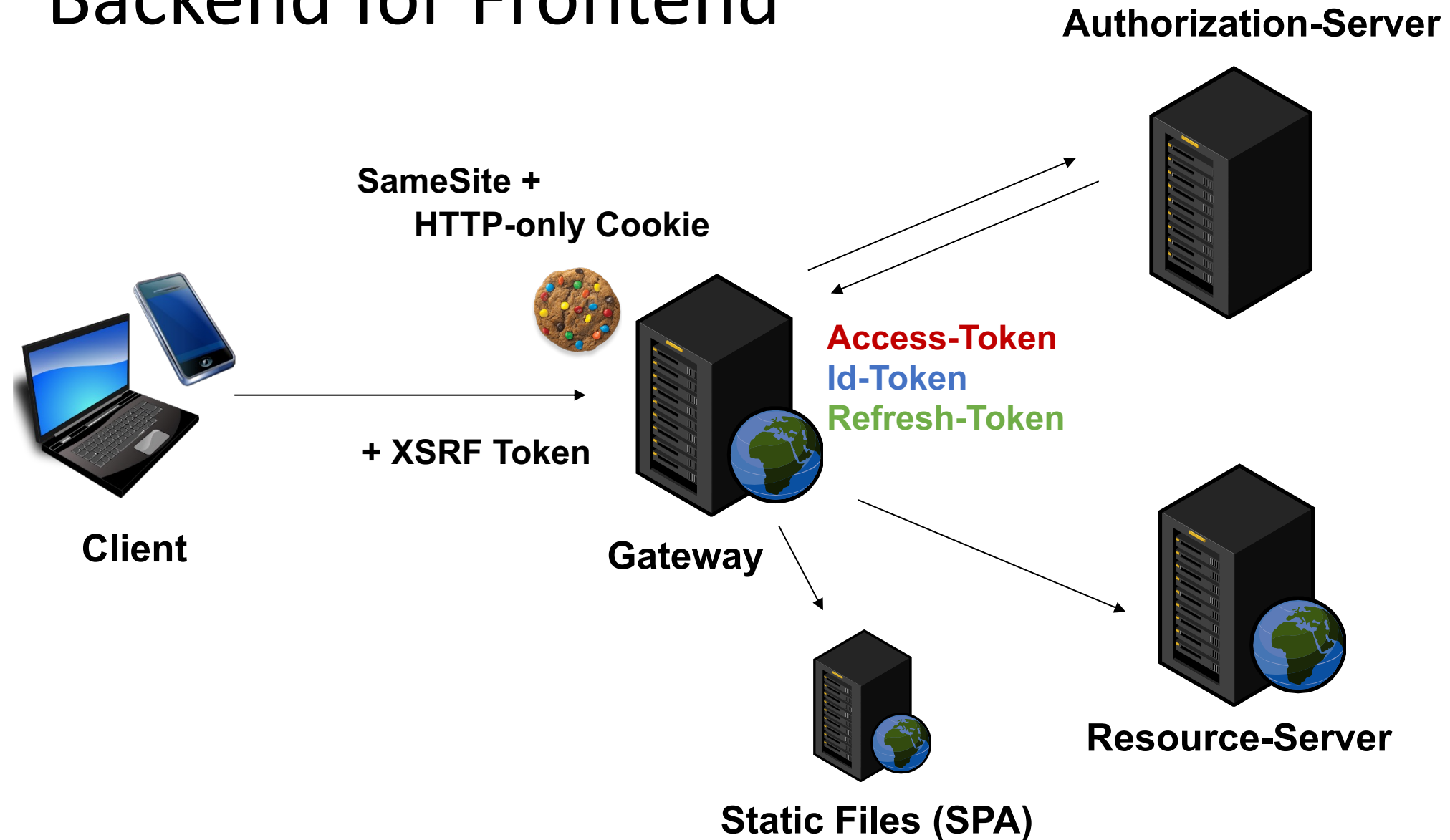
Tunnel API-
Calls Through
Backend

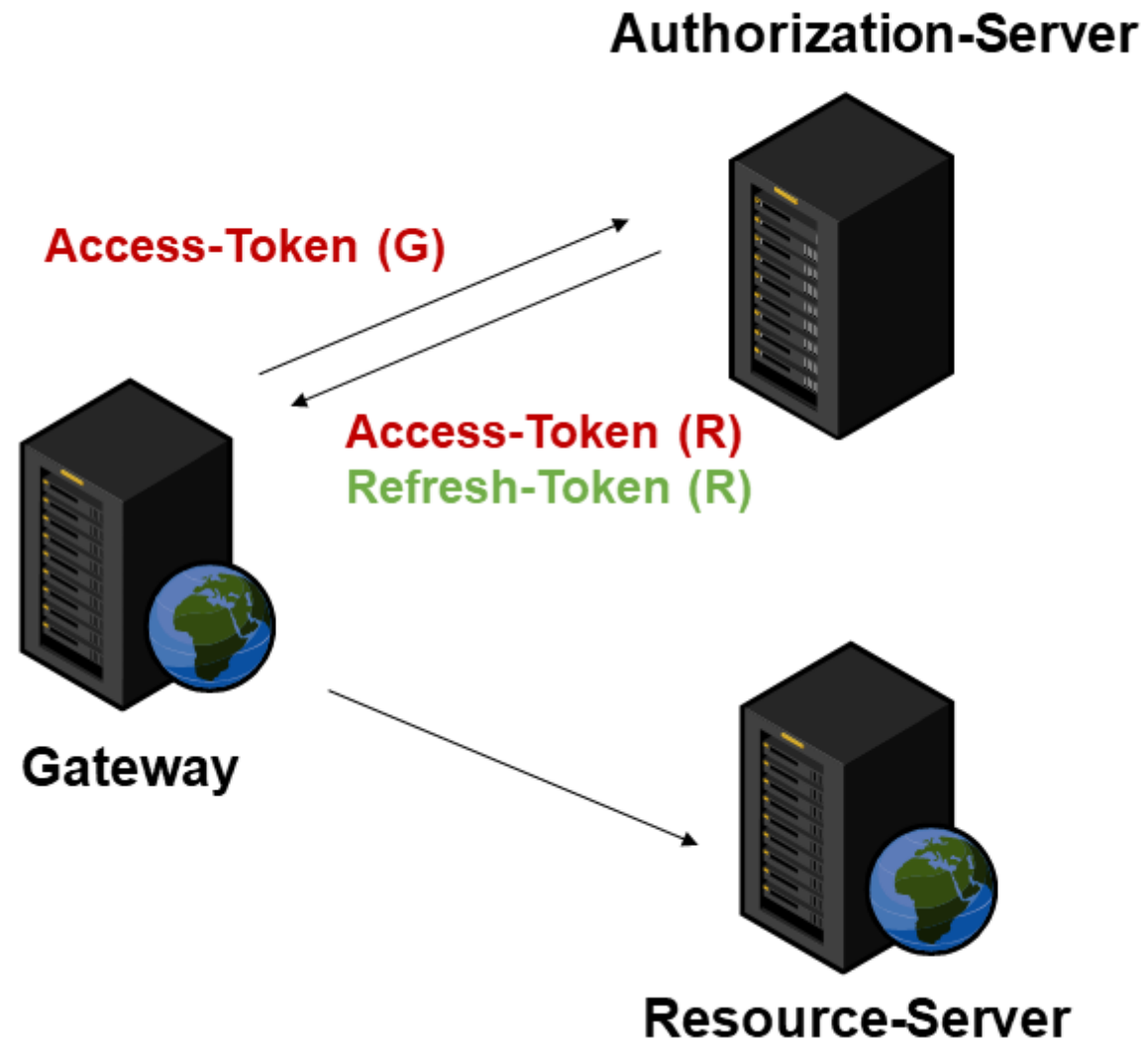
Client: Http-
only Cookie



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

"Backend for Frontend"





Token for Gateway: Key for Key Room



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

Possible Solutions

Kong API
Gateway

Traefik API
Gateway

Amazon API
Gateway

Azure API
Management

Identity
Server BFF

...



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

YARP Documentation

+

https://microsoft.github.io/reverse-proxy/index.html

🔍

🔗


☆


⚙️

🖨️

👤

⋮





About YARP

YARP: Yet Another Reverse Proxy

Welcome to the documentation for YARP! YARP is a library to help create reverse proxy servers that are **high-performance, production-ready, and highly customizable**. Please provide us your feedback by going to [the GitHub repository](#).



ANGULAR
ARCHITECTS
INSIDE KNOWLEDGE

YARP 101

```
// 1. Register Services
```

```
var builder = WebApplication.CreateBuilder(args);
```

```
builder.Services.AddReverseProxy()  
    .LoadFromConfig(builder.Configuration.GetSection("ReverseProxy"));
```

```
[...]
```

```
builder.Services  
    .AddAntiforgery([...])  
    .AddSession([...])  
    .AddAuthentication([...])  
    .AddCookie([...])  
    .AddOpenIdConnect([...]);
```



YARP 101

```
// 2. Add Middleware
```

```
app.UseSession();  
app.UseAuthentication();  
app.UseAuthorization();  
app.UseCookiePolicy();  
app.UseXsrfCookie();  
app.UseGatewayEndpoints();
```

```
app.MapReverseProxy([...]);
```

```
// 3. Start Sever
```

```
app.Run("http://+:8080");
```



manfredsteyer/yarp-auth-proxy x +

← → ↻ 🔒 https://github.com/manfredsteyer/yarp-auth-proxy 🔍 ↗ ☆ ⚙️ □ 👤 ⋮

☰ readme.md ✎

🔥 Features

- ☒ Easily implementing Authentication, Authorization, and SSO for SPAs (e. g. Angular) by making this gateway taking care of the heavy lifting on the serve side
- ☒ Tokens (id_token, access_token, refresh_token) are only stored on server-side in order to increase security
- ☒ Uses OAuth 2 and OpenId Connect (OIDC)
- ☒ Successfully tested with Keycloak, Azure Active Directory, Auth0, and Identity Server
- ☒ Supports Token Exchange (RFC 8693) and as an alternative Azure AD's OBO-Flow (On-Behalf-of flow)



Demos & Samples

- SPA:
<https://purple-flower-021fa1b03.azurestaticapps.net/home>
- SPA behind Security Gateway:
<https://demo-auth-gateway.azurewebsites.net/home>
- Source Code for Gateway:
<https://github.com/manfredsteyer/yarp-auth-proxy>
- Source Code for Auth in SPA:
<https://github.com/manfredsteyer/auth-gateway-client/>



Conclusion

Browser: No
Safe Place for
Tokens

Gateway:
Generic
Implementation

Token Refresh

Easier + More
Secure

