Roles

Authorization-Server

Client

Resource-Server

SOFTWAREarchitekt.at

Flow

Authorization-Server

One central user account

Only Auth-Svr. sees the Password

Auth. decoupled from Client

Tokens provide flexibility

No Cookies: No XSRF

1. Redirection

2. Redirection
w/ Access-Token

3. Access-Token

Client

Resource-Server

SOFTWARE*architekt.at*
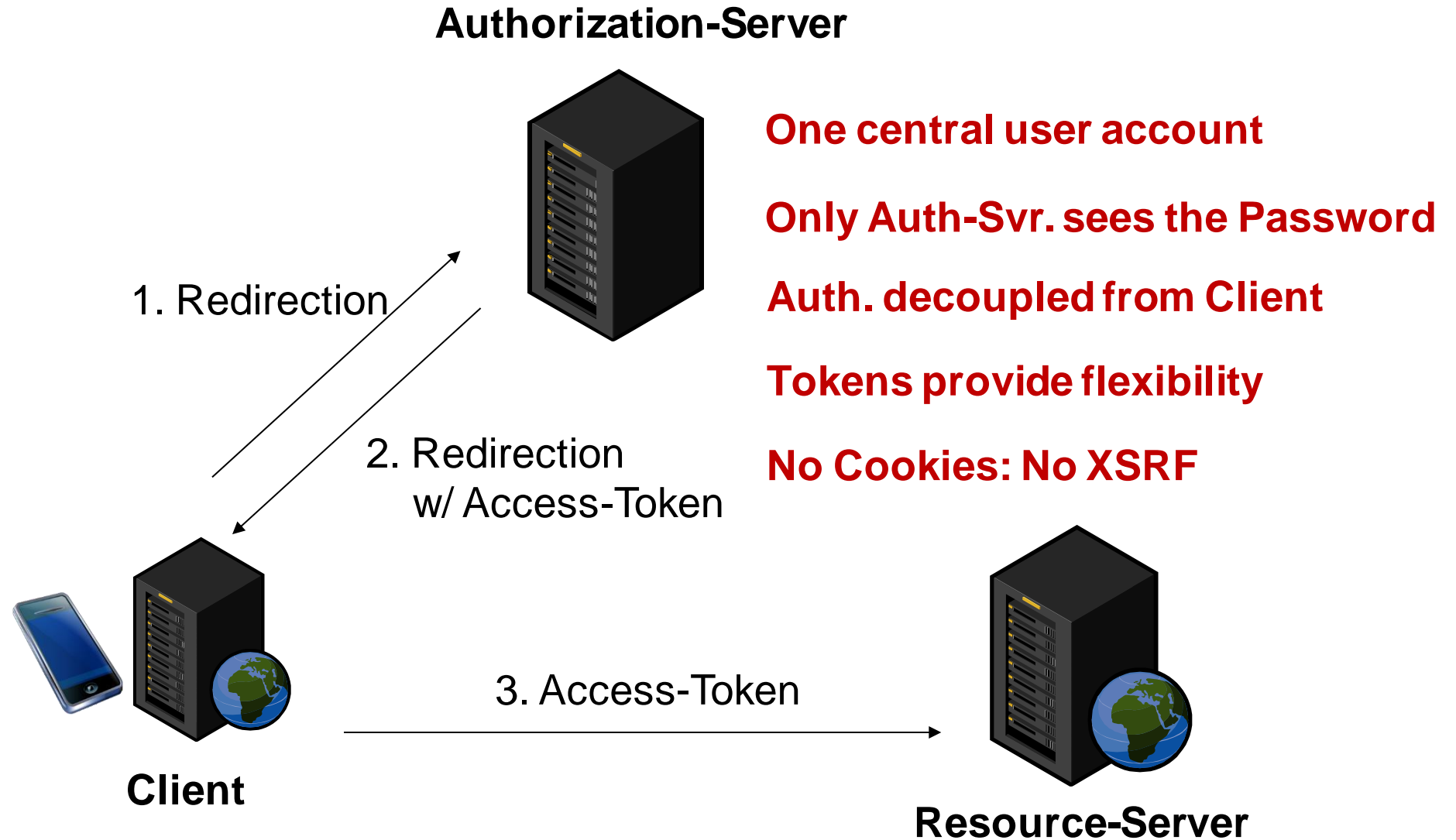
Lots of Auth Server out there …

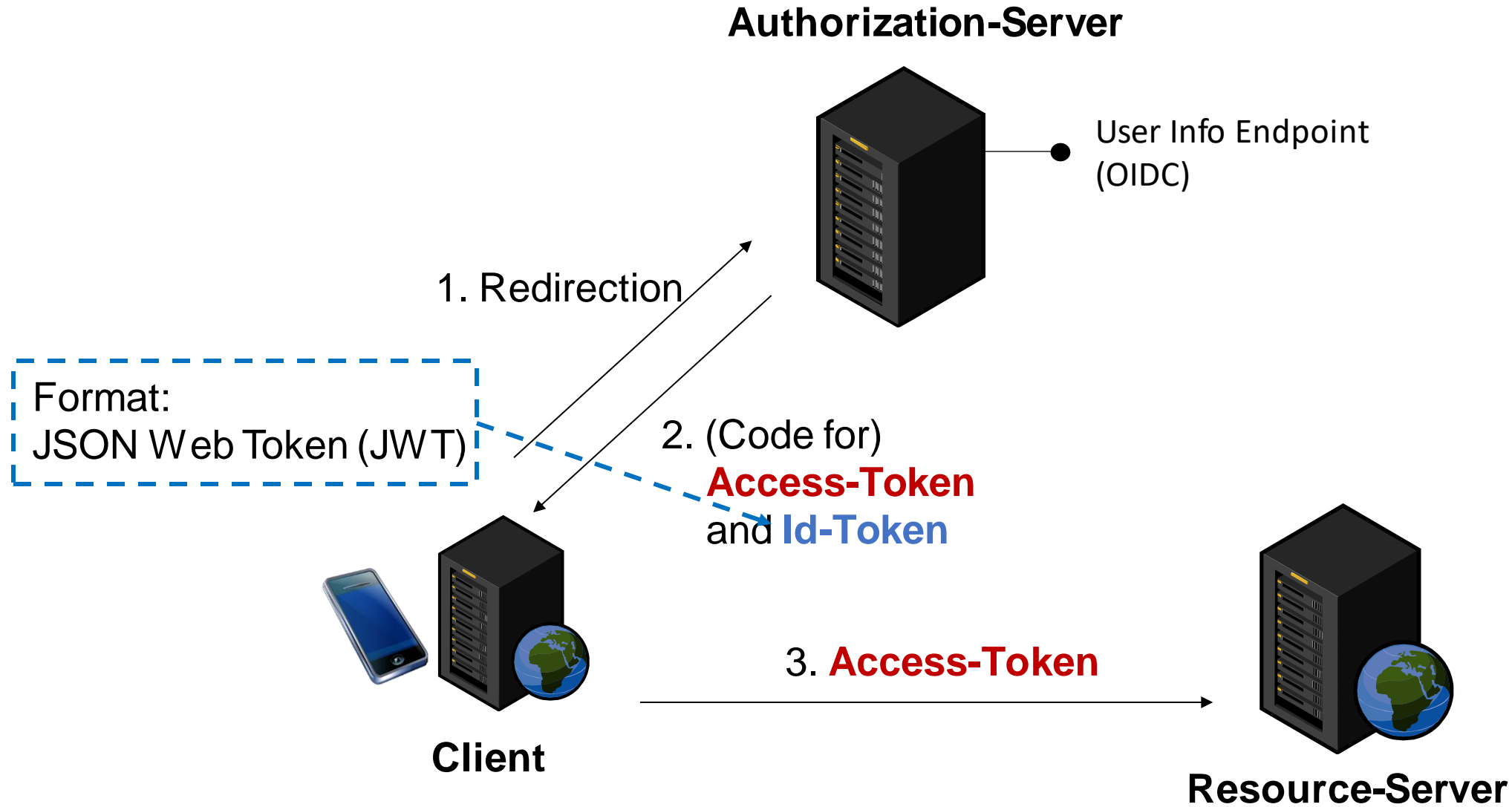|			
Active Directory Federation Services	Identity Server (.NET)	Redhat Keycloak (Java)	Okta
Auth0	Firebase	Azure Active Directory	…

SOFTWARE*architekt*.at

OAuth 2 and OpenId Connect

OAuth2

Authorization-Server

1. Redirection

2. (Code for)
   Access-Token

Client

3. Access-Token

Resource-Server

SOFTWARE*architekt.at*

OpenId Connect

Authorization-Server

User Info Endpoint
(OIDC)

1. Redirection

Format:
JSON Web Token (JWT)

2. (Code for)
Access-Token
and **Id-Token**

3. **Access-Token**

Client

Resource-Server
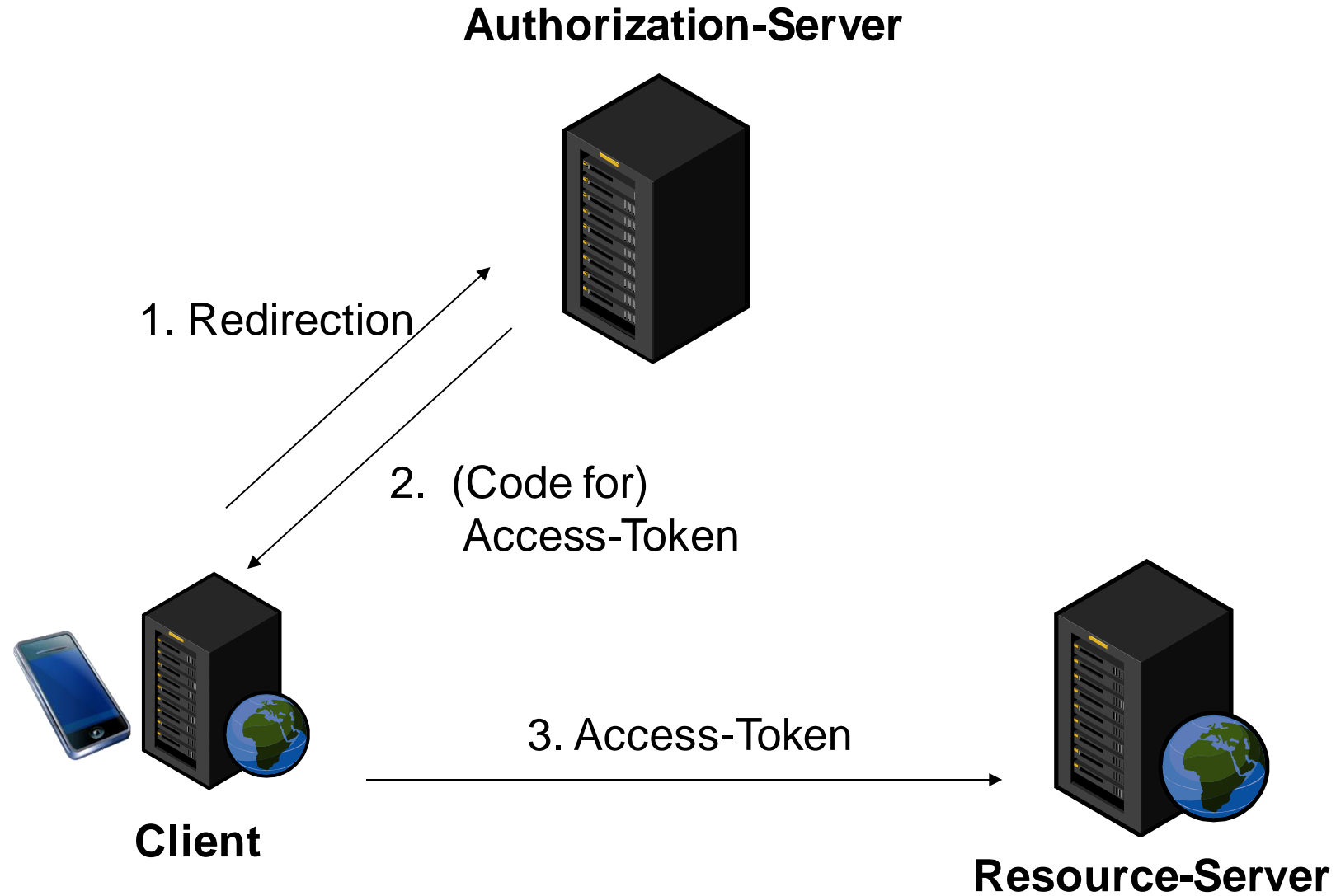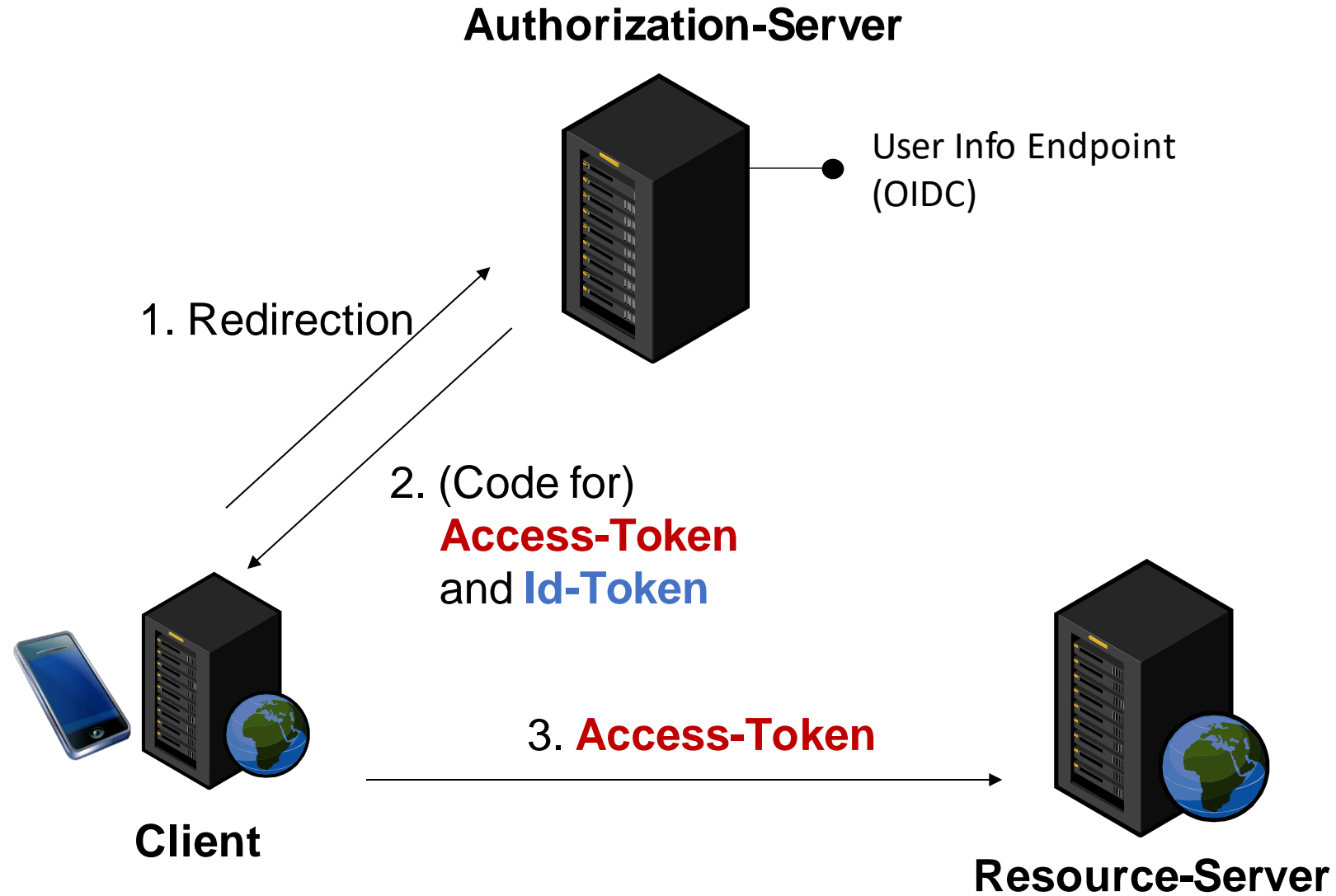
OpenId Connect

Flows for SPA

- Implicit Flow

  - originally for SPA,

  - Deprecated with OAuth 2.1

  - Tokens in URL

- Code Flow + PKCE

  - now recommented!

angular-oauth2-oidc - npm   ✕   +

← → C   🔒 https://www.npmjs.com/package/angular-oauth2-oidc   ↗ ★   ⊞ 👤 ⋮

angular-oauth2-oidc [TS]

13.0.1 • Public • Published a month ago

| 📄 Readme | 🗜 Explore [BETA] | 📦 2 Dependencies | 🎲 346 Dependents | 🏷 85 Versions |

angular-oauth2-oidc

Support for OAuth 2 and OpenId Connect (OIDC) in Angular. Already prepared for the upcoming OAuth 2.1.

Install

```
> npm i angular-oauth2-oidc
```

Repository

◈ github.com/manfredsteyer/angular-oa...

Homepage

🔗 github.com/manfredsteyer/angular-oa...

⤓ Weekly Downloads

119.863

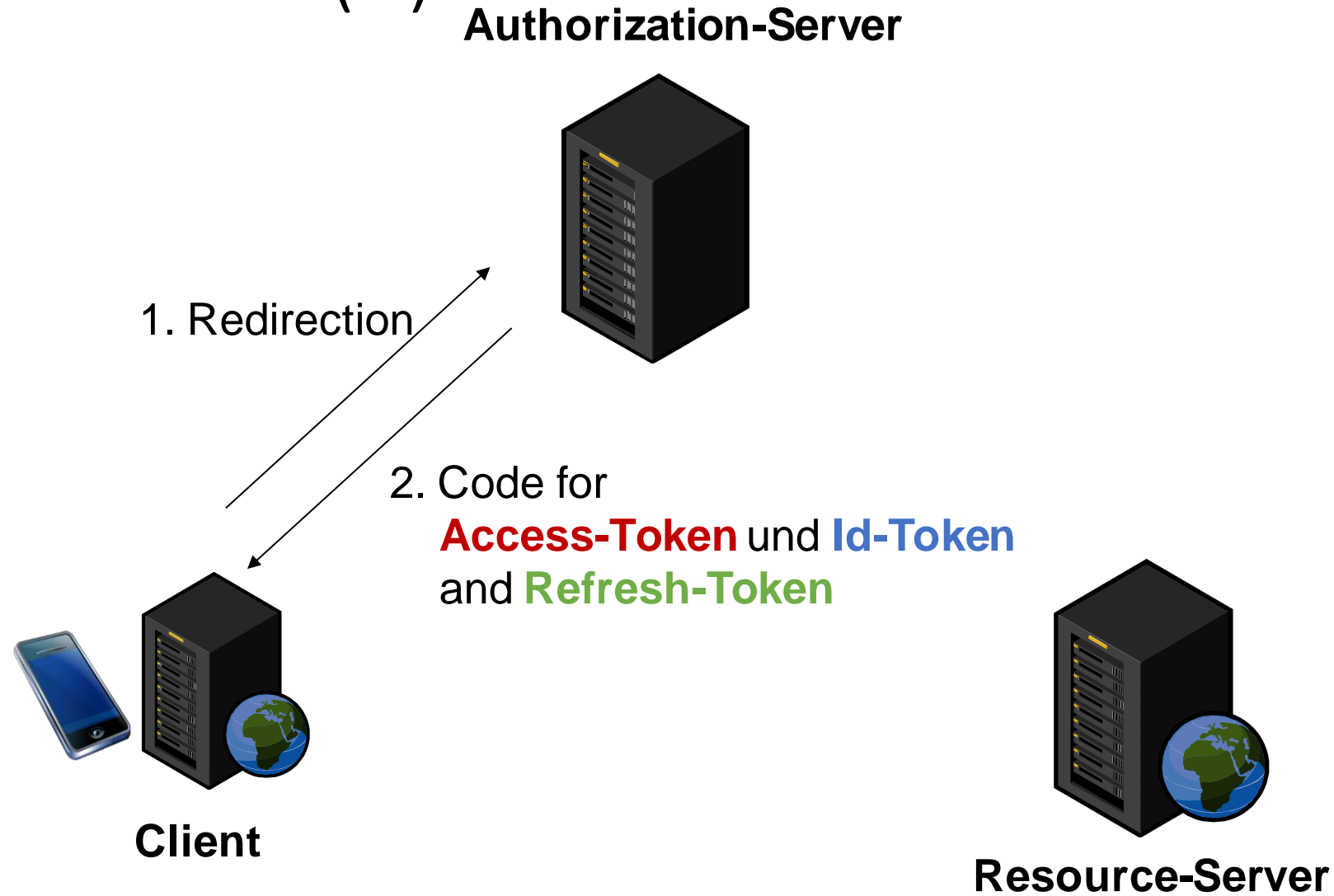| Version	License
13.0.1	MIT

Token Refresh

———

Why Token Refresh?

Short living Tokens increase Security

Users don't want to login over and over again

Refresh Token (1)

Authorization-Server

1. Redirection

2. Code for
Access-Token und **Id-Token**
and **Refresh-Token**

Client

Resource-Server

SOFTWARE*architekt.at*

Refresh Token (2)

Authorization-Server

3. **Refresh-Token**

4. Code for
Access-Token und **Id-Token**
and new **Refresh-Token**

Client

Resource-Server

SOFTWARE*architekt.at*
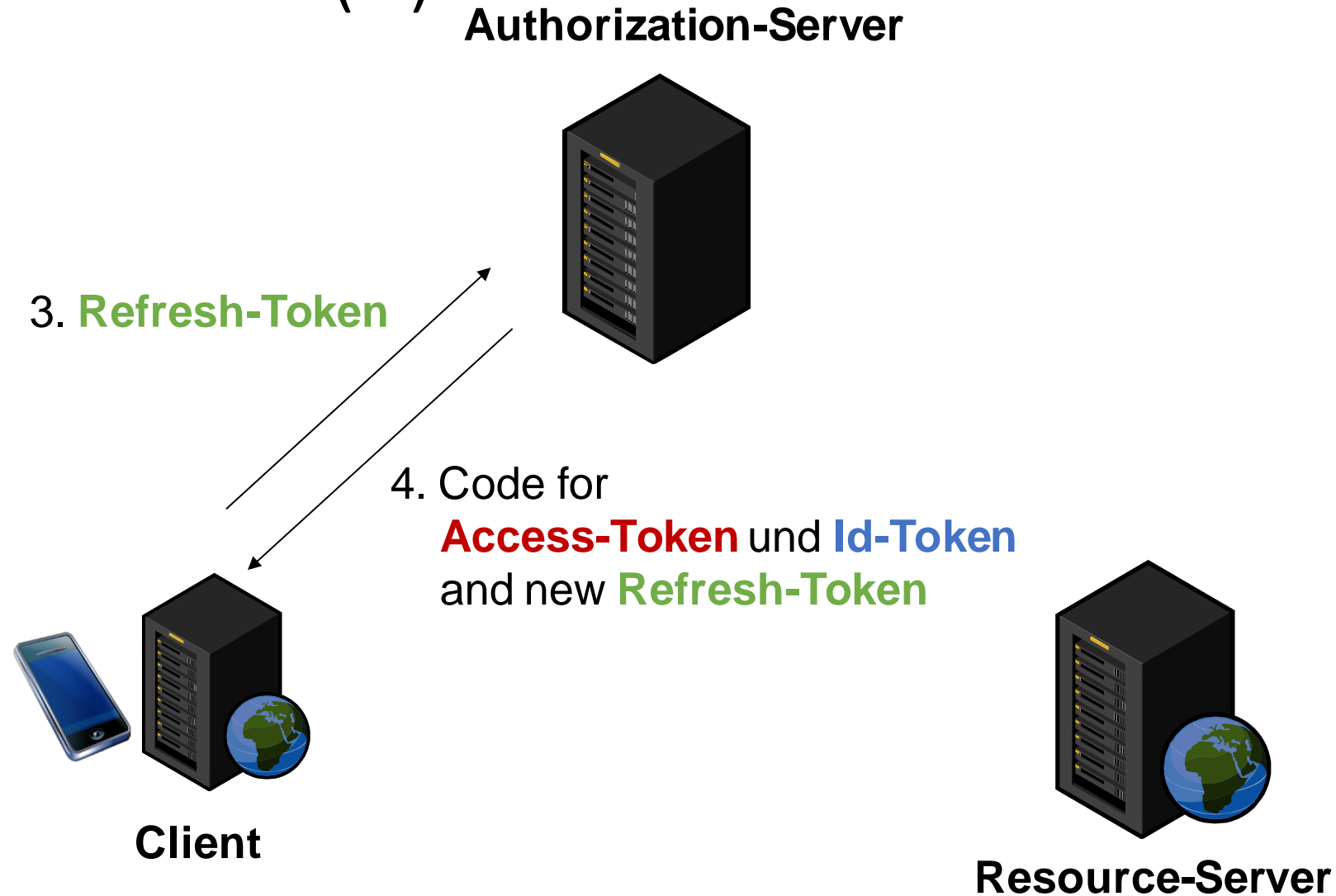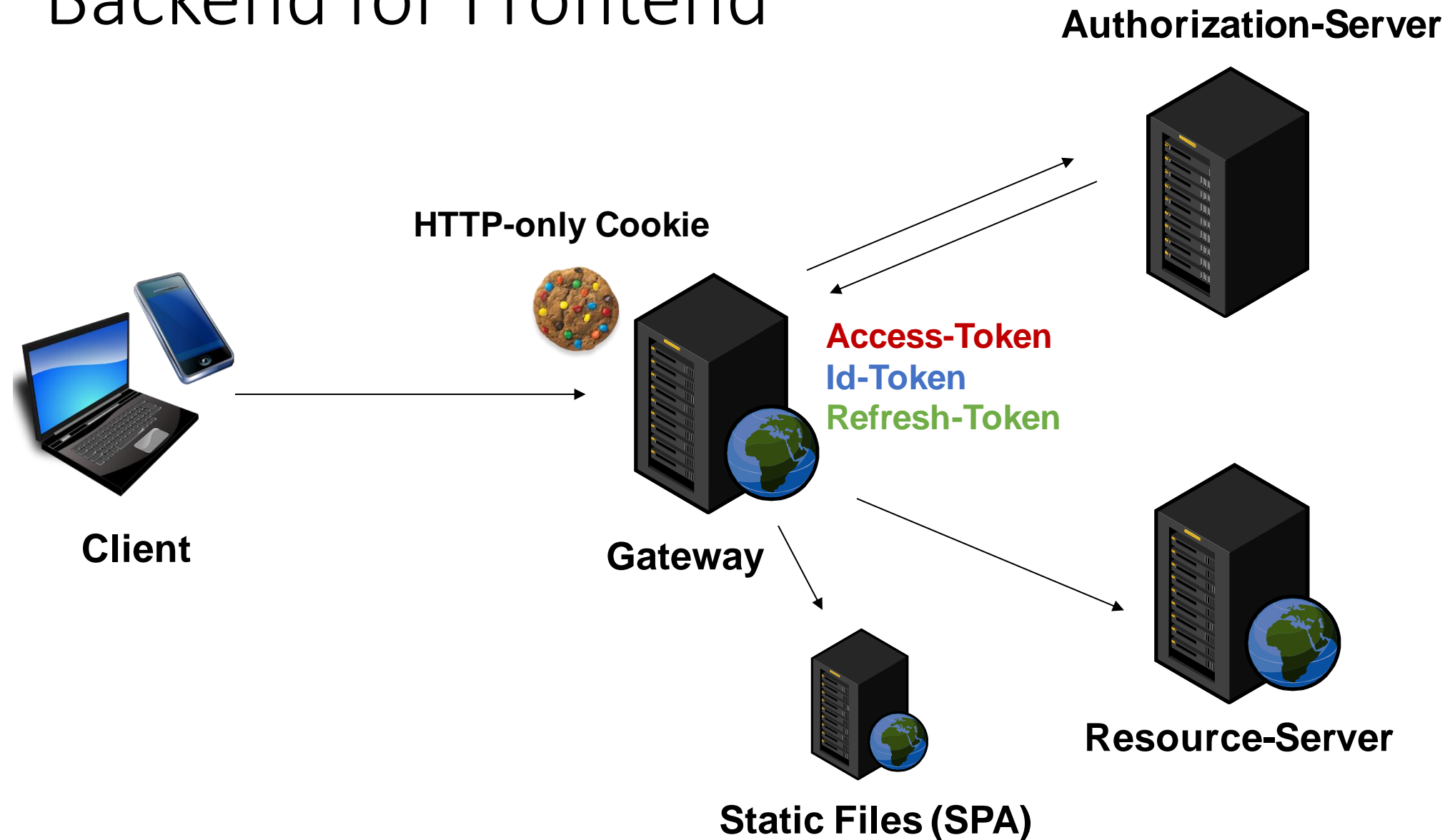
Refresh-Token and Browsers

- [OAuth 2.0 Security Best Current Practice](#) allows it under specific circumstances

- Security Audit (XSS!)

- Refresh Token needs to be one-time token

- After Refresh: Client gets new refresh token

- If used by several users: log out both

SOFTWARE*architekt.at*

"Backend for Frontend"

Authorization-Server

HTTP-only Cookie

Client

Gateway

Access-Token
Id-Token
Refresh-Token

Static Files (SPA)

Resource-Server

Possible Solutions

Kong API Gateway

Traefik API Gateway

Amazon API Gateway

Azure API Management

...

SOFTWARE*architekt.at*

Demo

- 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/

SOFTWARE*architekt.at*

Conclusion

Token: Flexibility, Cross Origin …	OAuth 2: Access to Service	OpenId Connect: SSO at Client
Implicit Flow	Code Flow + PKCE	

SOFTWARE*architekt.at*