Securing Java apps with OAuth2, OIDC and Spring Security

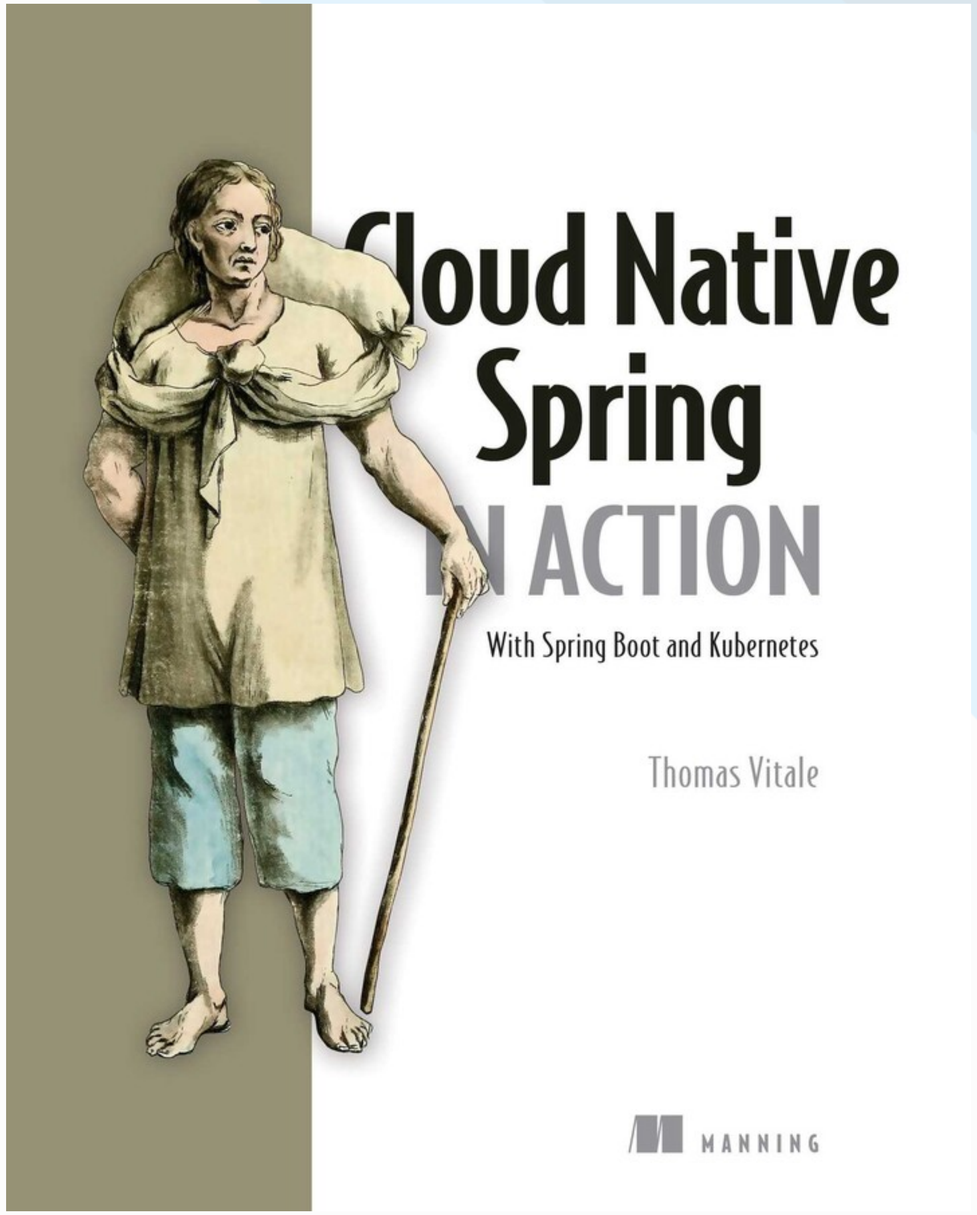
Thomas Vitale
Star of Java
Oct 13th, 2022

@vitalethomas

Thomas Vitale

Systematic

- **Software Architect** at Systematic, Denmark.
- Author of “**Cloud Native Spring in Action**” (Manning).
- **OSS contributor** (Java, Spring, Cloud Native Technologies)



thomasvitale.com

@vitalethomas

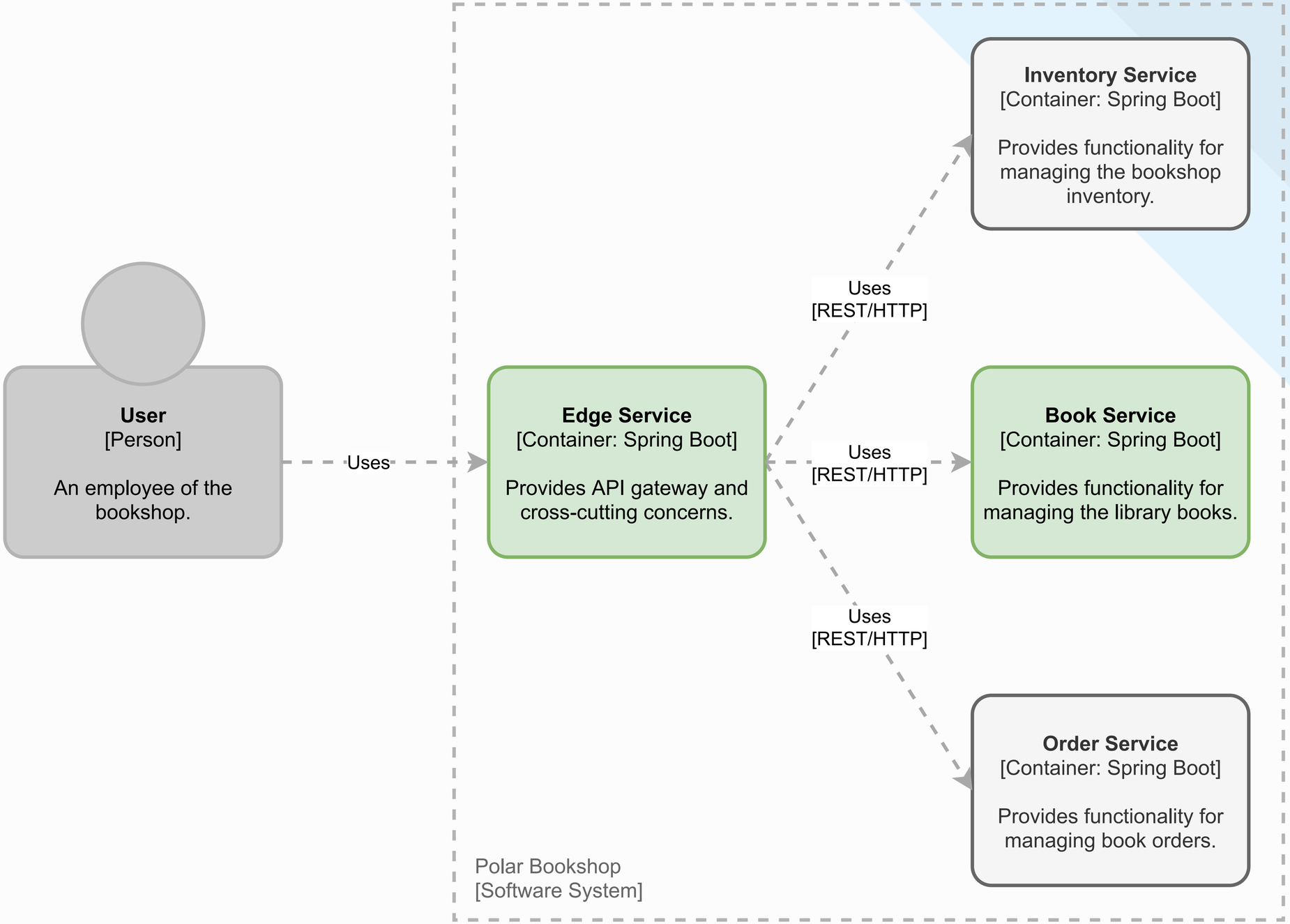
Security

Access Control

Access Control

Three Steps

Identification	Authentication	Authorization
▸ A user claims an identity ▸ e.g. username	▸ Verifying the claimed identity ▸ e.g. password, token	▸ Verifying what the user is allowed to do ▸ e.g. roles, permissions

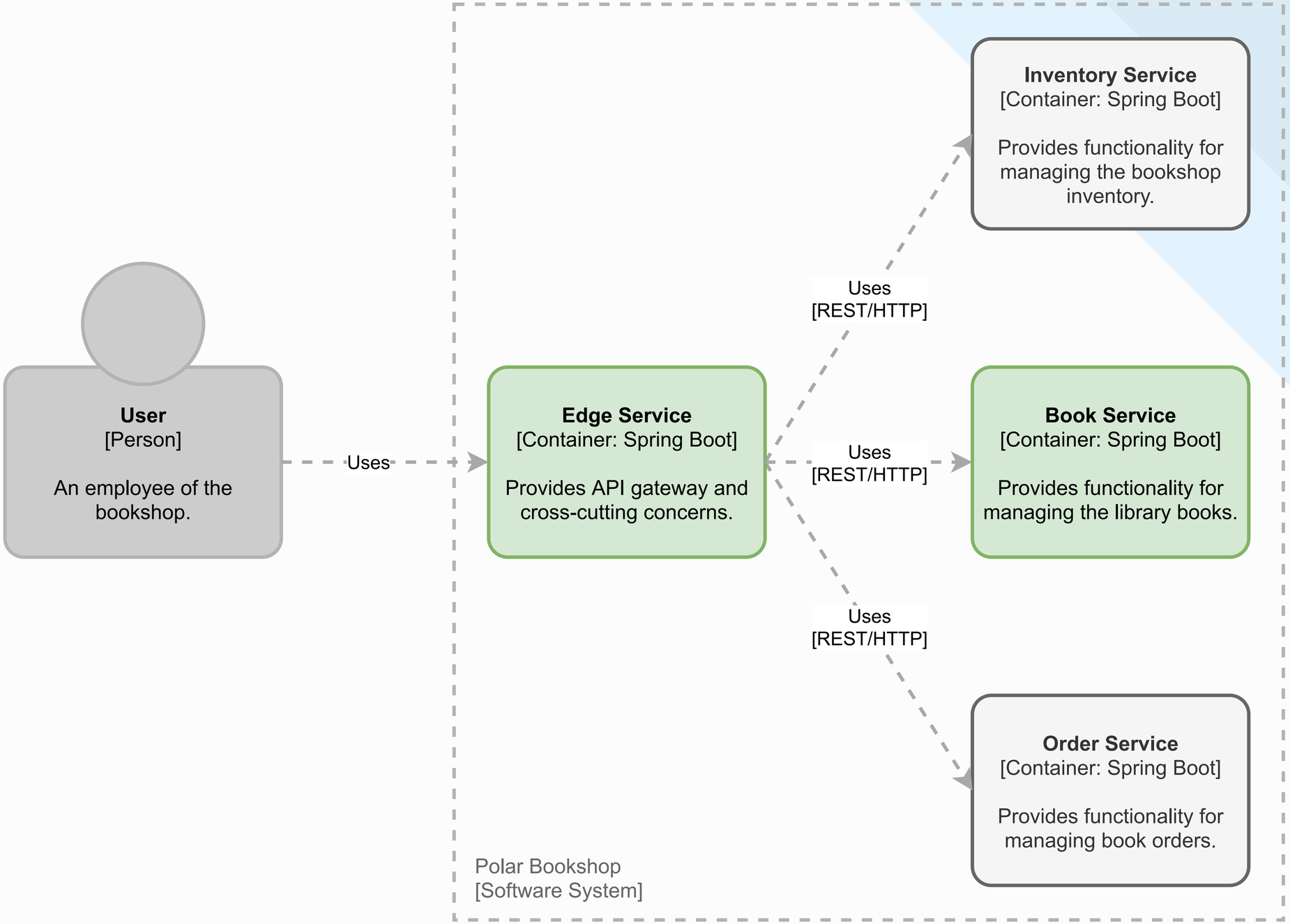

Inventory Service
[Container: Spring Boot]
Provides functionality for managing the bookshop inventory.
Uses
[REST/HTTP]
User
[Person]
An employee of the bookshop.
Uses
Edge Service
[Container: Spring Boot]
Provides API gateway and cross-cutting concerns.
Uses
[REST/HTTP]
Book Service
[Container: Spring Boot]
Provides functionality for managing the library books.
Uses
[REST/HTTP]
Order Service
[Container: Spring Boot]
Provides functionality for managing book orders.
Polar Bookshop
[Software System]

Spring Security

De-facto standard for securing Spring applications

Authentication	Authorization	Protection against common attacks
▸ Username/password ▸ OIDC/OAuth2 ▸ SAML 2	▸ Endpoint ▸ Method ▸ Object	▸ Session fixation ▸ CSRF ▸ Content injection

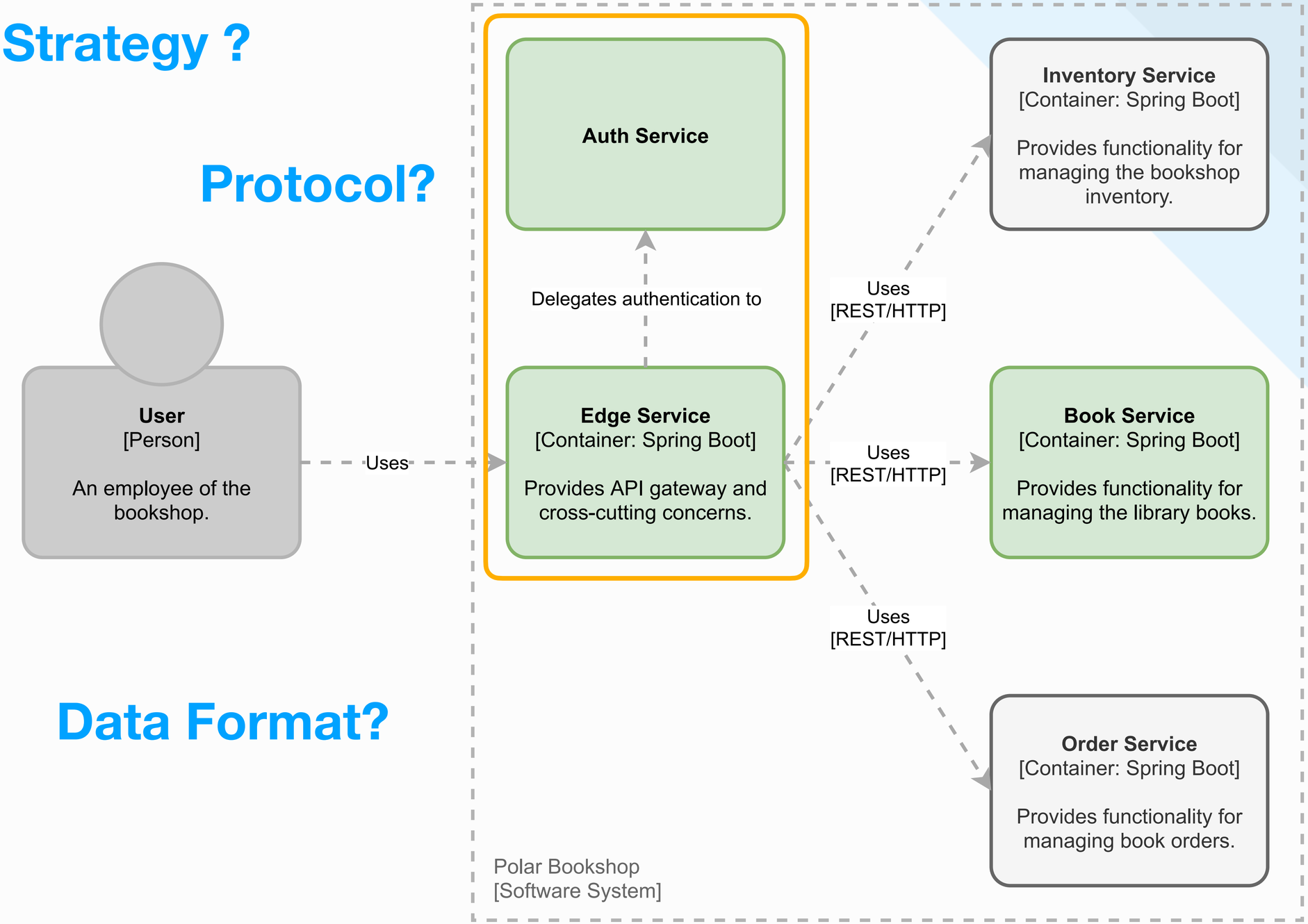
Authentication


Inventory Service
[Container: Spring Boot]
Provides functionality for managing the bookshop inventory.
Uses
[REST/HTTP]
User
[Person]
An employee of the bookshop.
Uses
Edge Service
[Container: Spring Boot]
Provides API gateway and cross-cutting concerns.
Uses
[REST/HTTP]
Book Service
[Container: Spring Boot]
Provides functionality for managing the library books.
Uses
[REST/HTTP]
Order Service
[Container: Spring Boot]
Provides functionality for managing book orders.
Polar Bookshop
[Software System]

Strategy ?

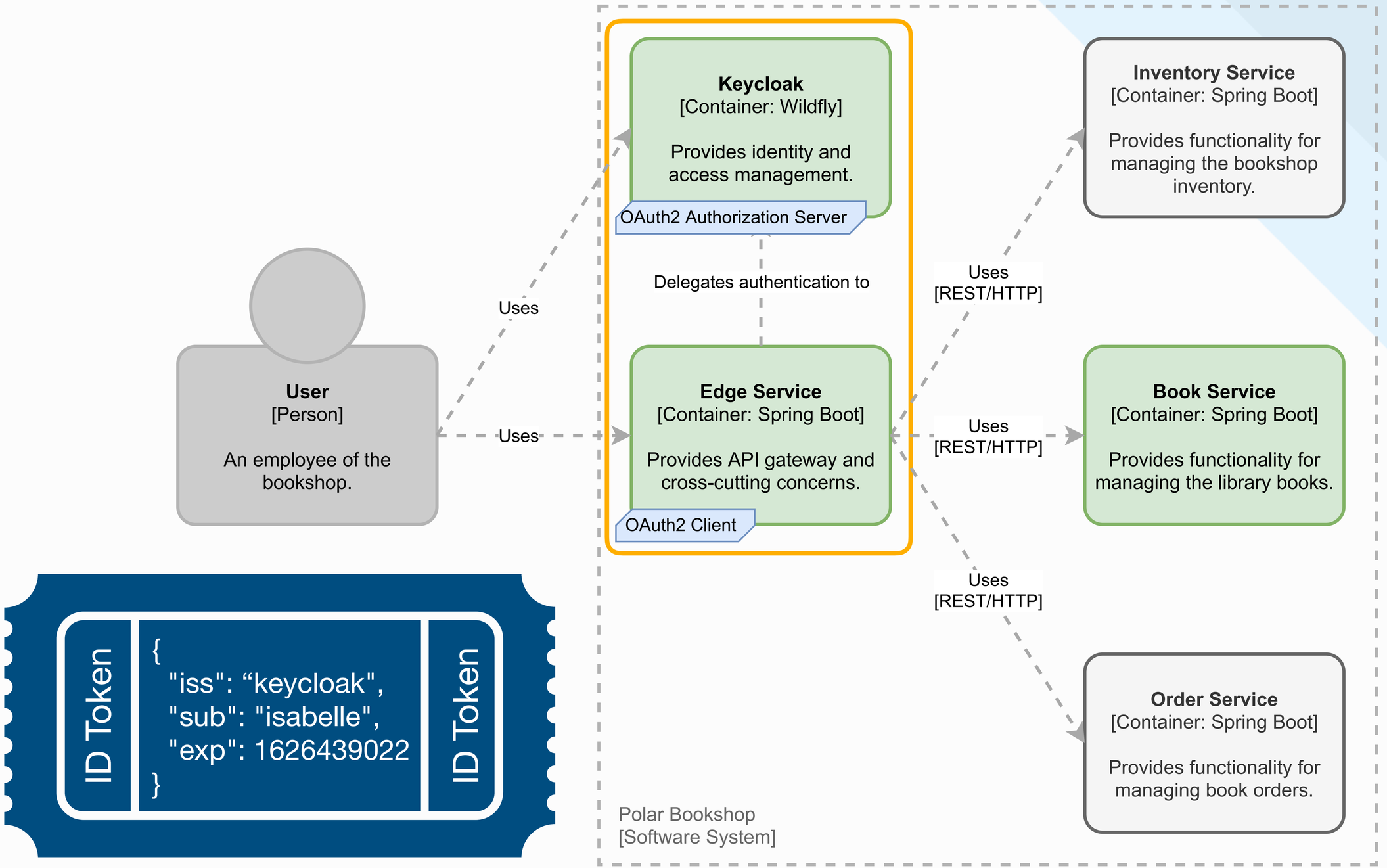
Protocol?

Data Format?



OpenID Connect

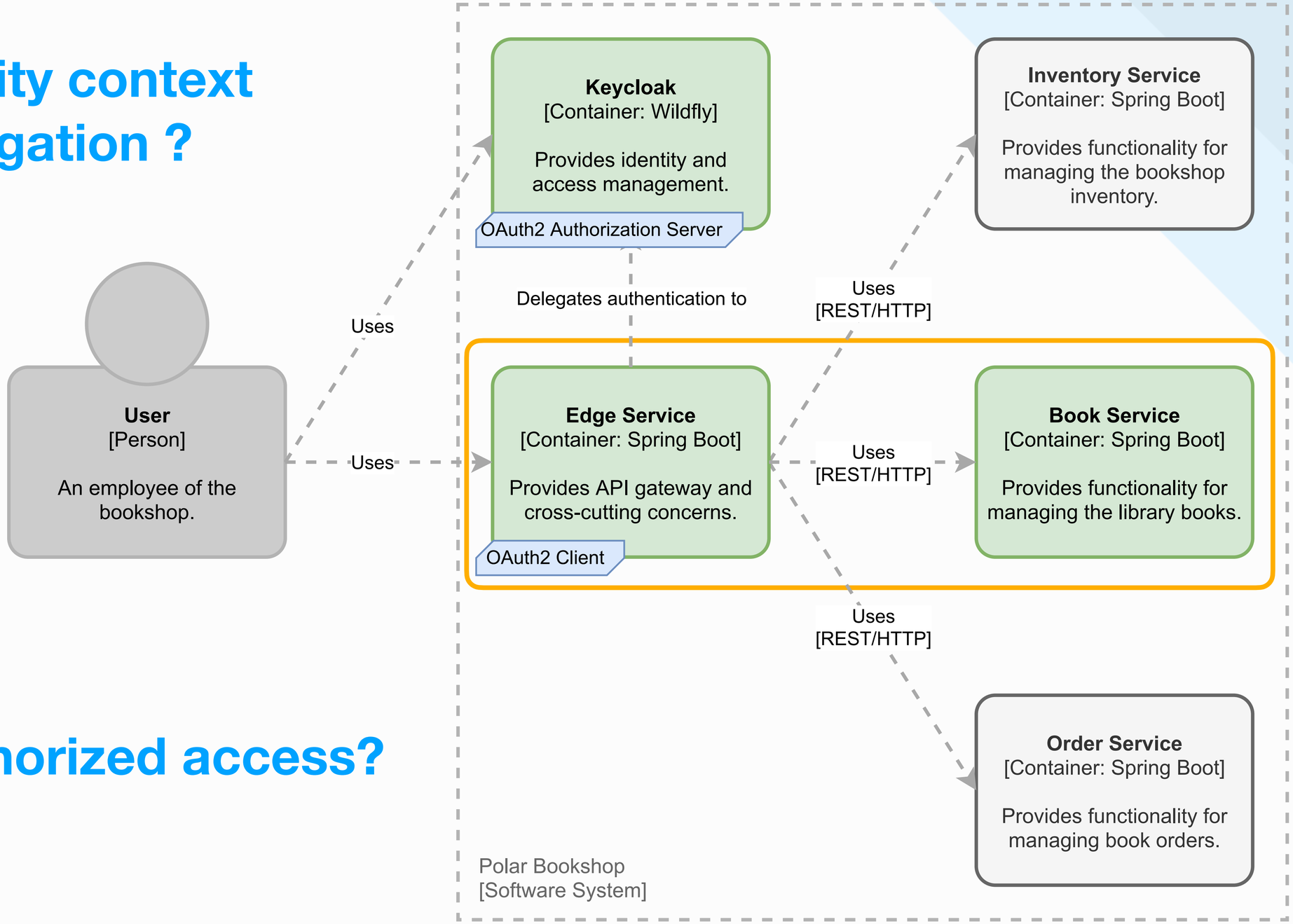
A protocol built on top of OAuth2 that enables an application (**Client**) to verify the identity of a user based on the authentication performed by a trusted party (**Authorization Server**).


Keycloak
[Container: Wildfly]
Provides identity and access management.
OAuth2 Authorization Server
Delegates authentication to
Edge Service
[Container: Spring Boot]
Provides API gateway and cross-cutting concerns.
OAuth2 Client
Inventory Service
[Container: Spring Boot]
Provides functionality for managing the bookshop inventory.
Book Service
[Container: Spring Boot]
Provides functionality for managing the library books.
Order Service
[Container: Spring Boot]
Provides functionality for managing book orders.
User
[Person]
An employee of the bookshop.
Uses
Uses
Uses [REST/HTTP]
Uses [REST/HTTP]
Uses [REST/HTTP]
Polar Bookshop
[Software System]

ID Token
{
"iss": “keycloak",
"sub": "isabelle",
"exp": 1626439022
}
ID Token

Delegated Access

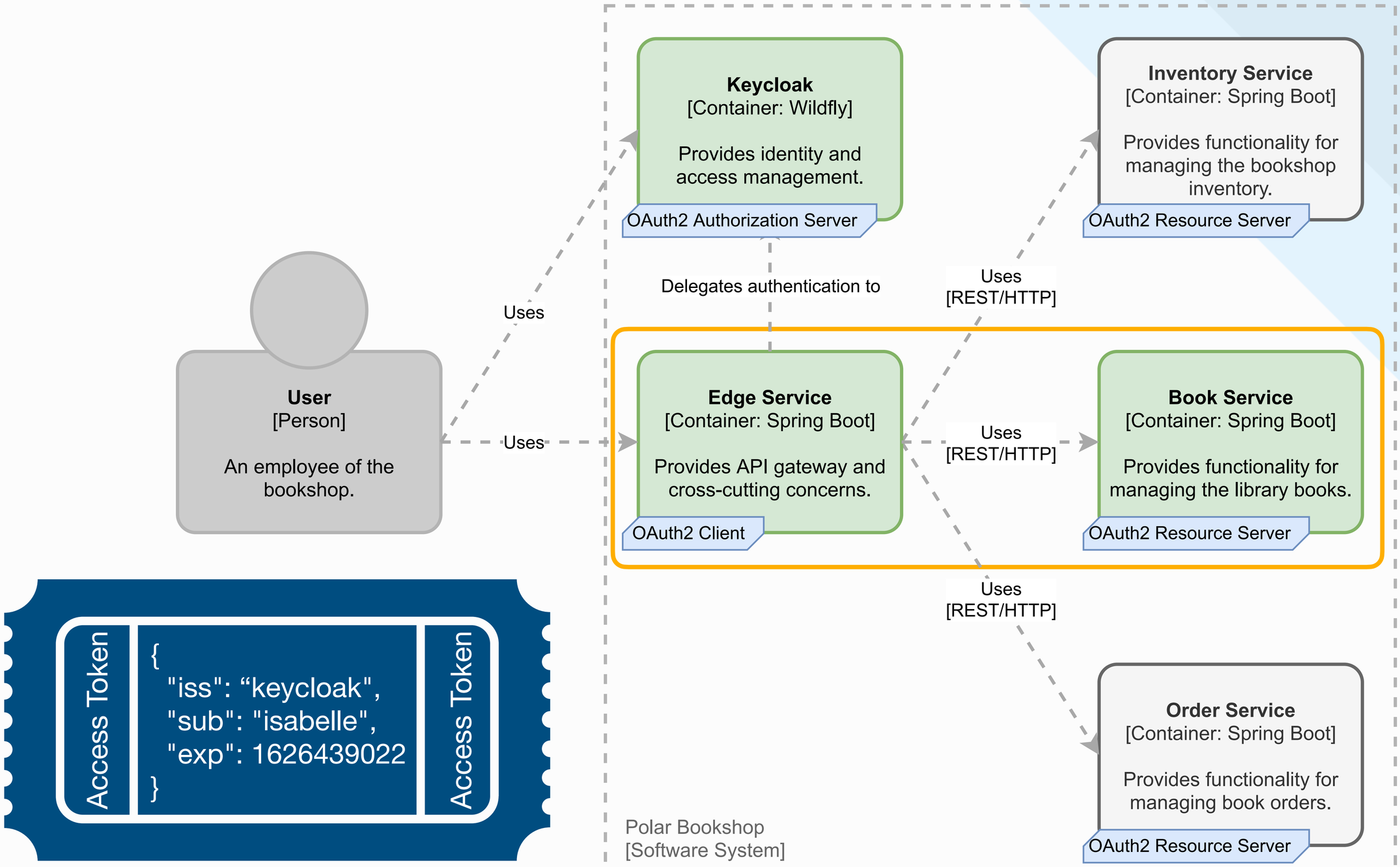
Security context propagation ?



Authorized access?

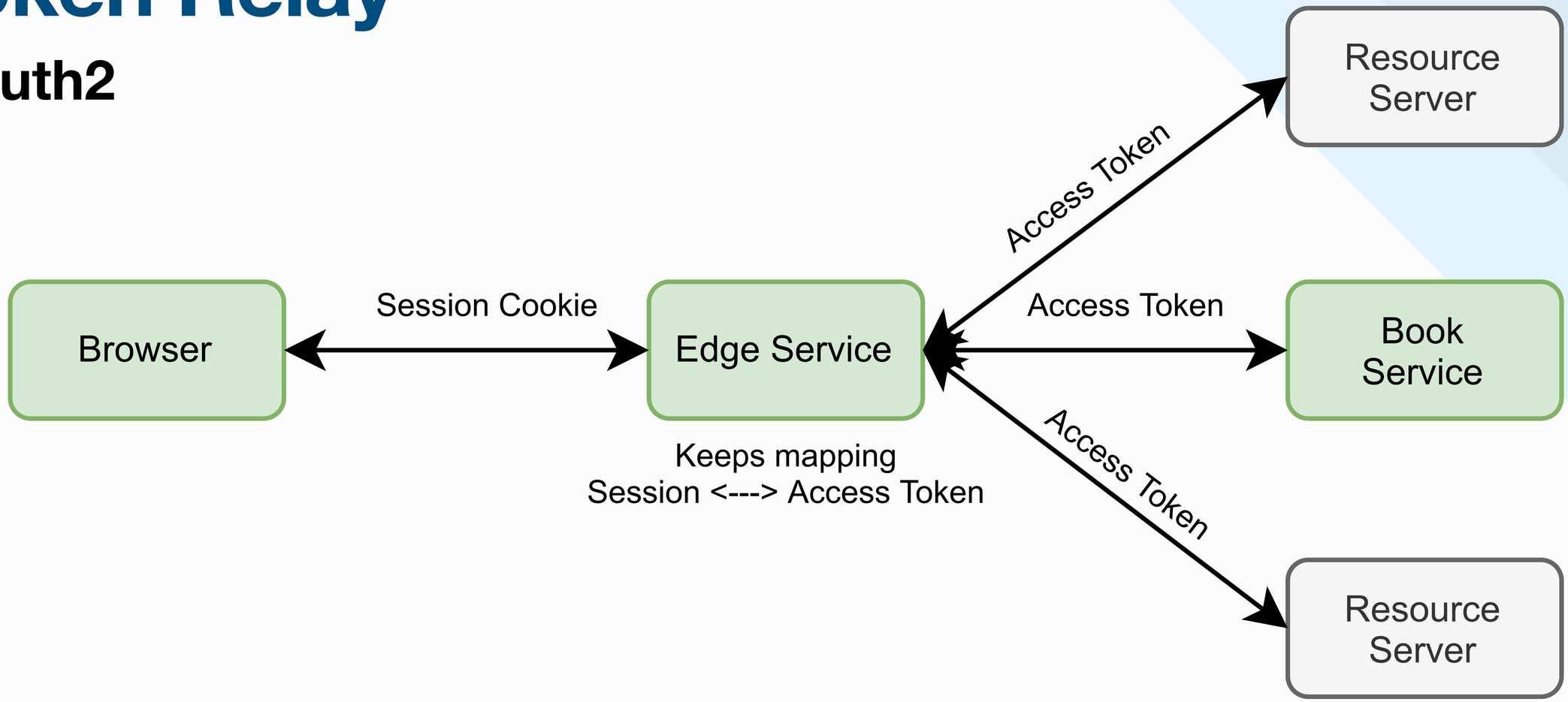
OAuth2

An authorization framework that enables an application (**Client**) to obtain limited access to a protected resource provided by another application (called **Resource Server**) on behalf of a user.


Keycloak
[Container: Wildfly]
Provides identity and access management.
OAuth2 Authorization Server
Inventory Service
[Container: Spring Boot]
Provides functionality for managing the bookshop inventory.
OAuth2 Resource Server
Delegates authentication to
Uses
[REST/HTTP]
User
[Person]
An employee of the bookshop.
Uses
Edge Service
[Container: Spring Boot]
Provides API gateway and cross-cutting concerns.
OAuth2 Client
Uses
[REST/HTTP]
Book Service
[Container: Spring Boot]
Provides functionality for managing the library books.
OAuth2 Resource Server
Uses
[REST/HTTP]
Order Service
[Container: Spring Boot]
Provides functionality for managing book orders.
OAuth2 Resource Server
Polar Bookshop
[Software System]
Access Token
{
"iss": “keycloak",
"sub": "isabelle",
"exp": 1626439022
}
Access Token

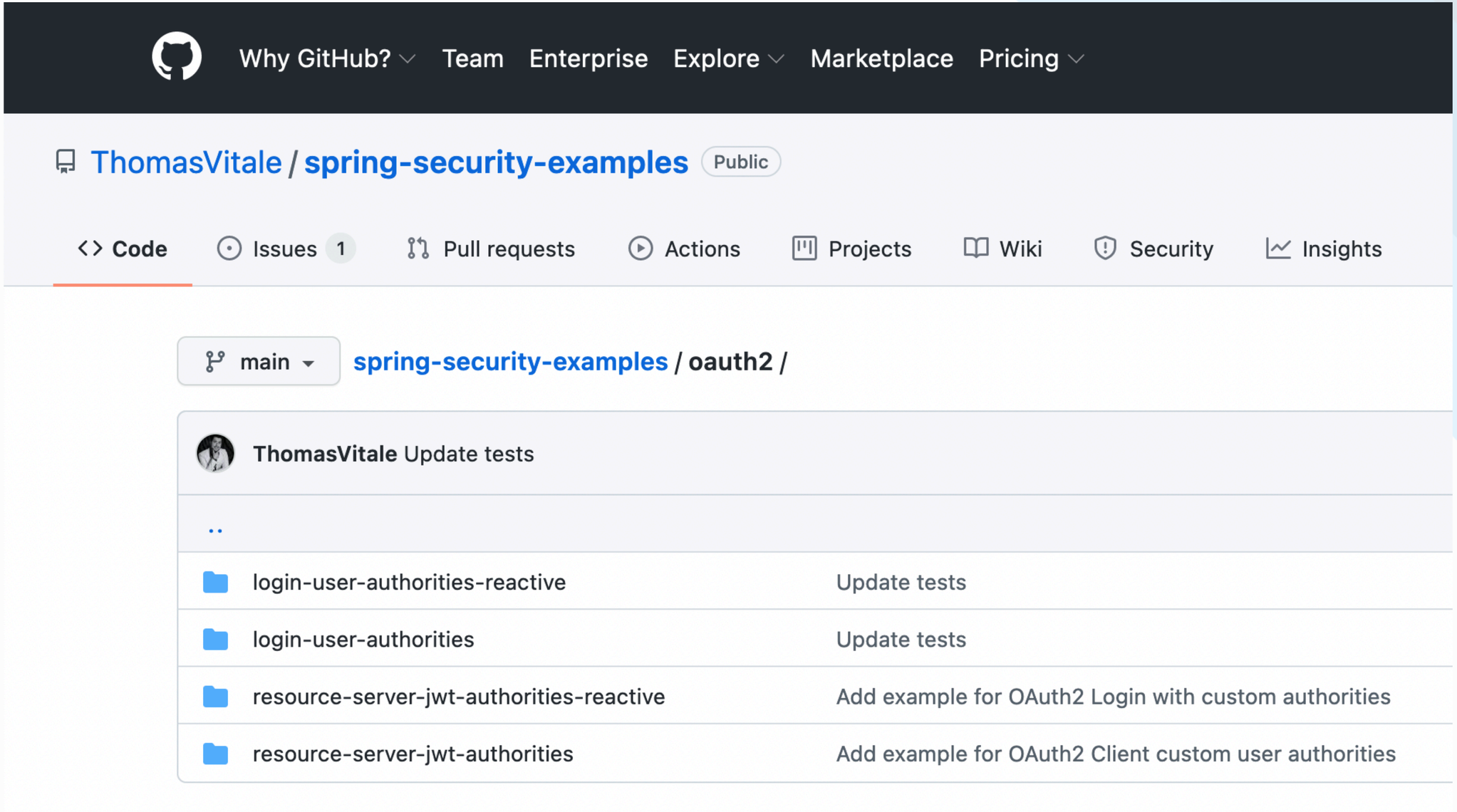
Token Relay

OAuth2



SPA

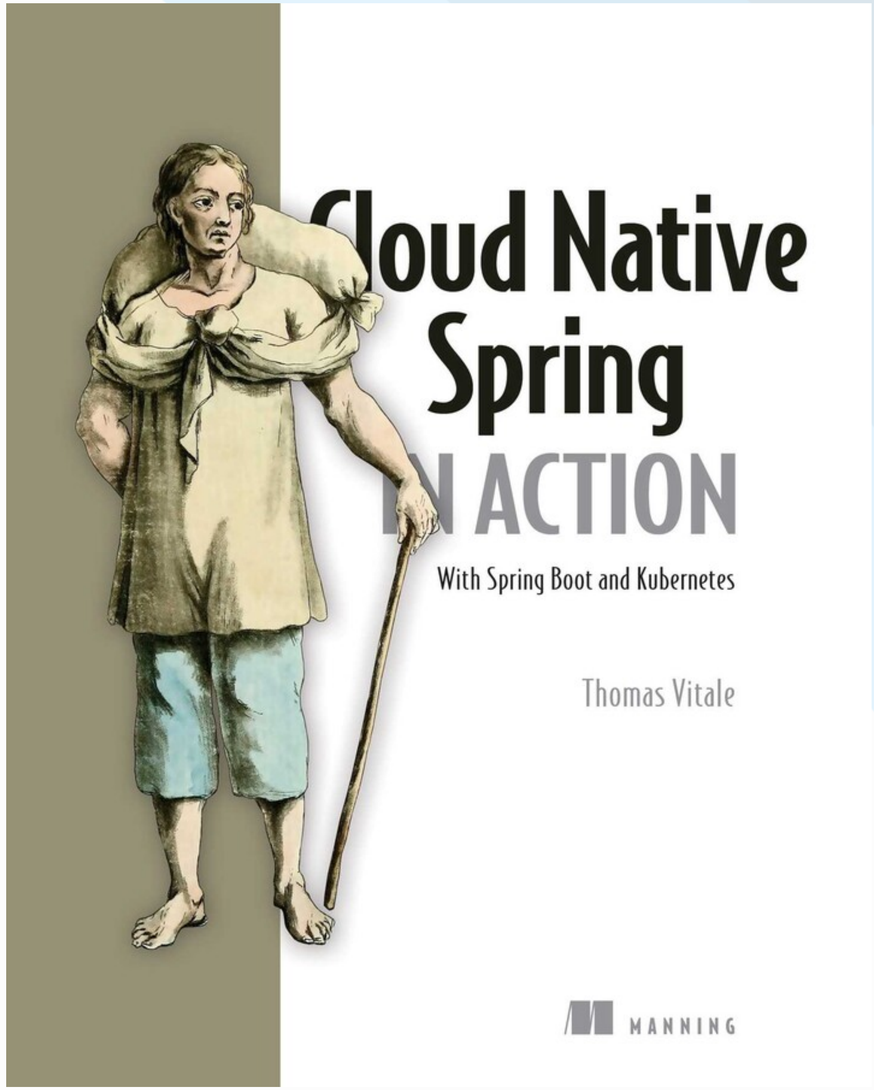
Authorization


Why GitHub?
Team
Enterprise
Explore
Marketplace
Pricing
ThomasVitale / spring-security-examples
Public
Code
Issues 1
Pull requests
Actions
Projects
Wiki
Security
Insights
main
spring-security-examples / oauth2 /
ThomasVitale Update tests
..
login-user-authorities-reactive
Update tests
login-user-authorities
Update tests
resource-server-jwt-authorities-reactive
Add example for OAuth2 Login with custom authorities
resource-server-jwt-authorities
Add example for OAuth2 Client custom user authorities

Discount codes

Manning

- **35% discount code**, valid for all products in all format
  - `ctwgotocph22`
  - manning.com



Securing Java apps with OAuth2, OIDC and Spring Security

https://github.com/ThomasVitale/securing-java-apps-oauth2-oidc-spring-security
https://github.com/ThomasVitale/spring-security-examples

Thomas Vitale
Star of Java
Oct 13th, 2022

@vitalethomas