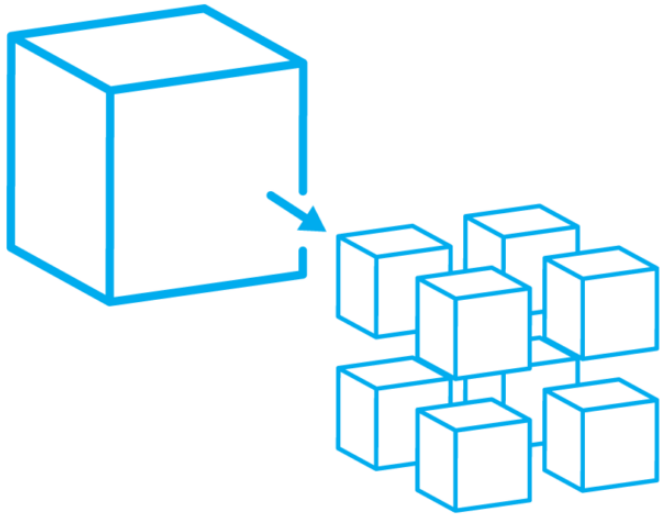


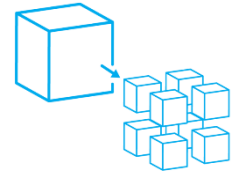
Microservicios – Arquitectura y Desarrollo

Por: Carlos Carreño

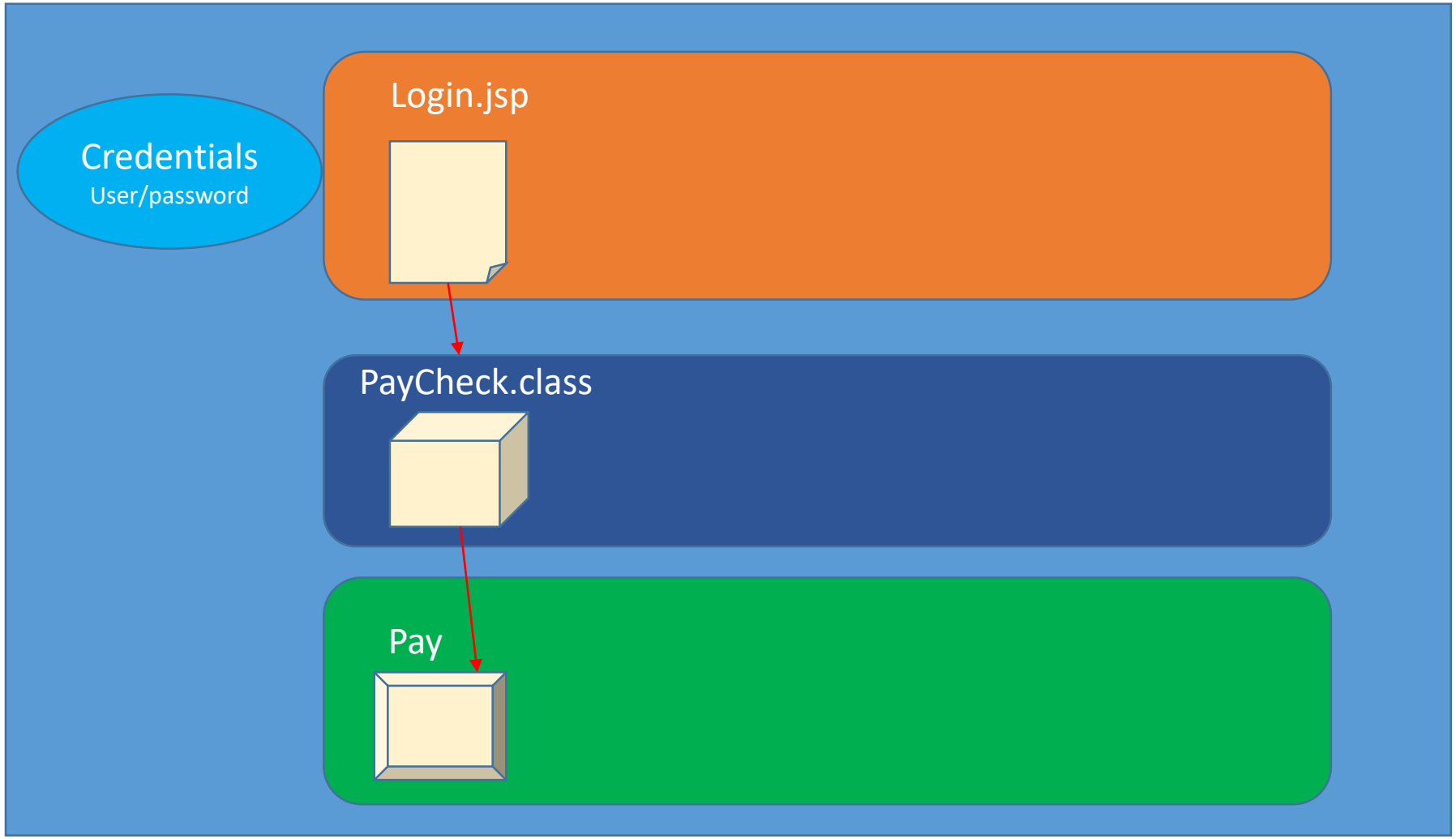
ccarrenovi@Gmail.com

Noviembre, 2020

Seguridad en los Monolitos



Finanzas.war

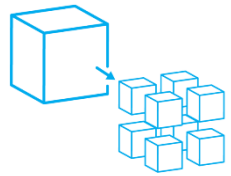


View

Business Logic

Data

Modulo 7 Implementando Seguridad en Microservicios con Oauth2 y JWT



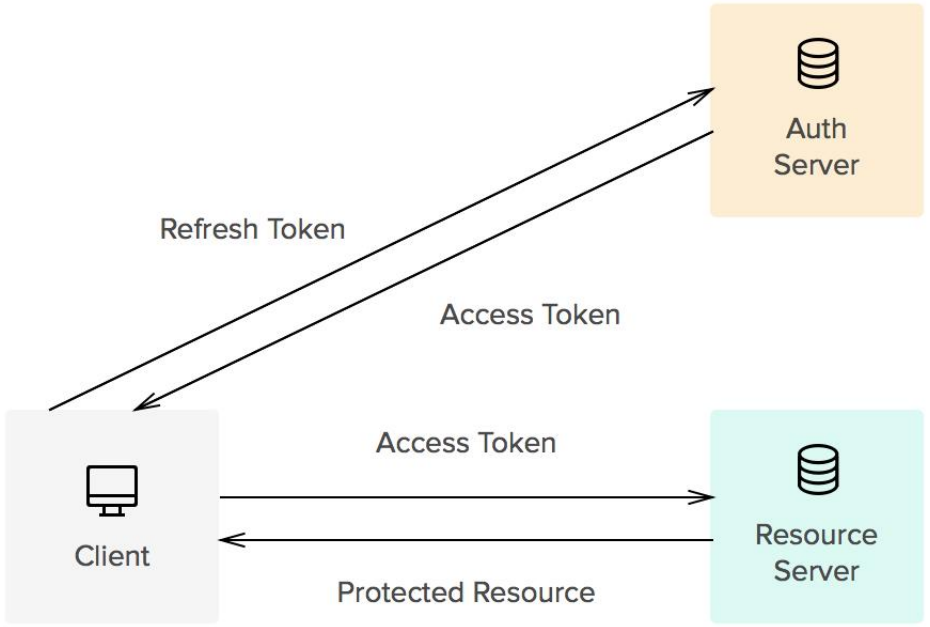
- Principios de Seguridad
- Access tokens
- Oauth2
- JWT
- Mejores prácticas de seguridad en Microservicios

Principios de Seguridad

- Principios de seguridad de los sistemas de información
  - ❑ **Integridad.** Es necesario asegurar que los datos no sufran cambios no autorizados
  - ❑ **Disponibilidad.** Se refiere a la continuidad operativa de la entidad.
  - ❑ **Confidencialidad.** Se refiere a la protección de datos frente a la difusión no autorizada

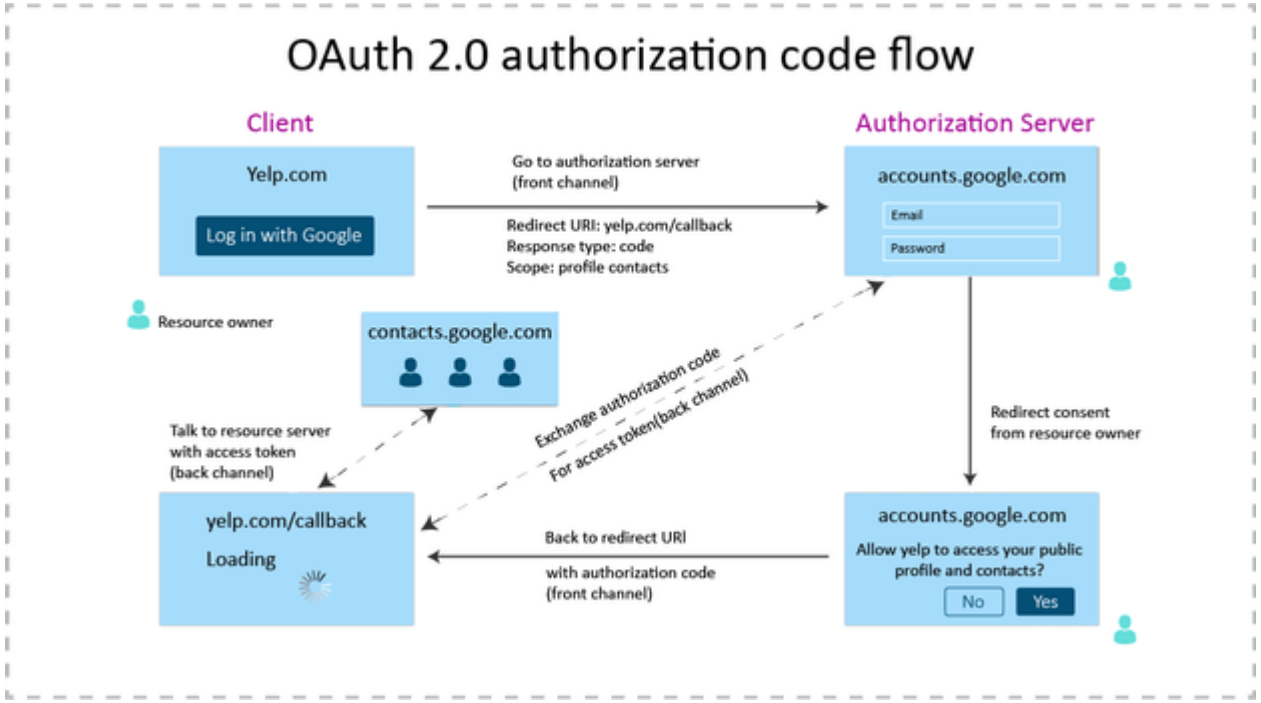
Access tokens

- un **token de acceso** contiene las credenciales de seguridad para una sesión de inicio de sesión e identifica al usuario , los grupos de usuarios, los privilegios del usuario y, en algunos casos, una aplicación en particular.



Oauth2

- La **especificación OAuth 2.0** define un **protocolo de delegación** que proporciona a los clientes "***acceso delegado seguro***" a los recursos del servidor ***en nombre del propietario del recurso*** (usuario).
- Oauth2, especifica un proceso para que los usuarios autoricen a terceros a ***acceder a los recursos de su servidor sin compartir sus credenciales***. Está destinado a funcionar con HTTP y permite que el servidor de autorización asigne ***tokens de acceso*** a clientes de terceros con la aprobación de un propietario de recurso especial. El canal posterior del cliente (servidor de aplicaciones) luego ***usa el token de acceso*** para acceder ***a los recursos protegidos*** alojados por el servidor de recursos.

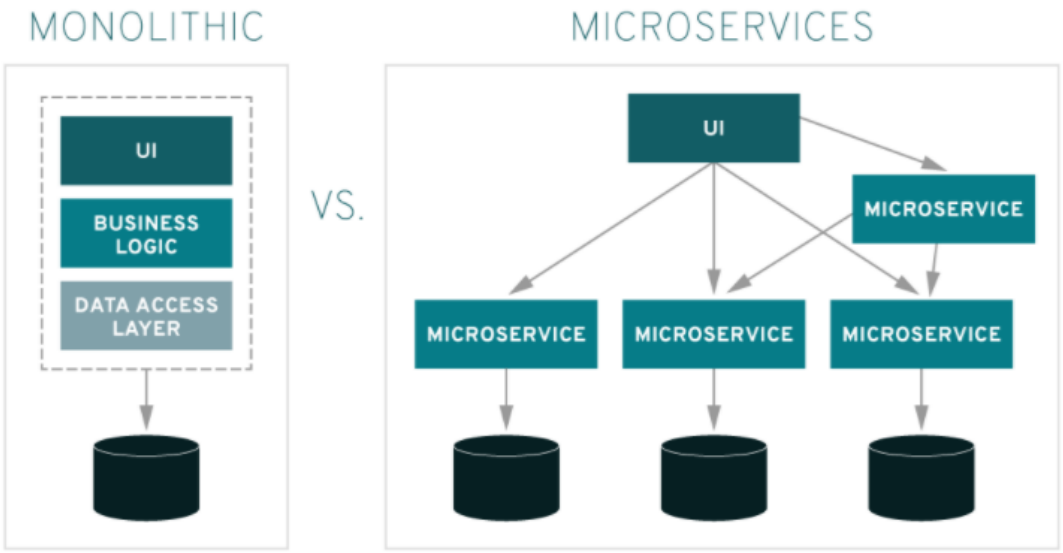


JWT

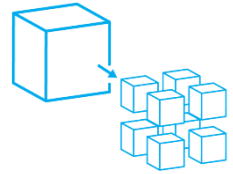
- **JSON Web Token (abreviado JWT)** es un estándar abierto basado en JSON propuesto por IETF (RFC 7519) para la creación de tokens de acceso que permiten la propagación de identidad y privilegios o claims en inglés.
- **Por ejemplo**, un servidor podría generar un token indicando que el usuario tiene privilegios de administrador y proporcionarlo a un cliente.

Mejores prácticas de seguridad en Microservicios

- Protección de aplicaciones, microservicios y usuarios
- Asegurar la gestión de identidades y accesos
- Protección de datos
- Mejorar la seguridad de las comunicaciones de servicio a servicio
- Monitoreo de microservicios y sistemas de seguridad



Laboratorio



- Lab 012 Microservicio de Gestión de Users
- Lab 013 Microservicios y OAuth Servidor de Autorizaciones
- Lab 014 Microservicios y Spring Security Obteniendo Tokens
- Lab 015 Microservicios – Información Adicional del Token (Opcional)
- Lab 016 Microservicios y Configuración Claims en Zuul

INTEGRACION DE ZUUL CON OAUTH

LAB 16