AUTENTICAÇÃO E AUTORIZAÇÃO

## *UTILIZAR MECANISMOS COMO CONSUMIDORES DE MENSAGERIA*



**Autenticação e Autorização** em sistemas de mensageria garantem que apenas usuários ou serviços autenticados (identificados) e autorizados (com permissão) possam acessar ou realizar ações em determinados recursos.

# **O que é?**

* 1. **Autenticação**: Processo de verificar a identidade de um usuário ou sistema (ex.: login).
  2. **Autorização**: Controle de permissões que define o que o usuário ou sistema autenticado pode fazer.

# **Como funciona?**

* 1. **OAuth (Open Authorization)**: É um protocolo que permite que aplicações de terceiros acessem os recursos de um usuário em outro serviço sem expor suas credenciais. Um exemplo comum é quando um app pede permissão para acessar suas fotos no Google sem pedir sua senha.
  2. **JWT (JSON Web Token)**: É um padrão para transmitir dados entre duas partes com segurança, geralmente para autenticação. O JWT é assinado digitalmente e pode ser validado por serviços de mensageria para garantir a autenticidade do remetente.

**Em mensageria**, esses mecanismos garantem que apenas clientes autenticados possam publicar, consumir ou administrar mensagens. Tokens (como JWT) podem ser usados para validar a identidade de quem está interagindo com o sistema de filas.

# **Programas que utilizam esses recursos:**

* 1. **Kafka**: Pode utilizar OAuth para autenticar produtores e consumidores de mensagens.
  2. **RabbitMQ**: Integração com JWT ou OAuth para autenticação e autorização de acesso.
  3. **Azure Service Bus** e **Amazon SQS**: Também utilizam mecanismos de OAuth e JWT para gerenciar o acesso às filas de mensagens.

Esses recursos são essenciais para a segurança e o controle de acesso em sistemas distribuídos e orientados a eventos.

Autor: Isabelle de S. Goffredo