Federação e autorização de mensagens em diferentes sistemas autónomos

No contexto da disciplina de Redes e Sistemas Autónomos a Ubiwhere foi desafiada a contribuir com um projeto de implementação. Nesse sentido, o desafio da Ubiwhere prende-se com a construção de um sistema de AAA[1] (Authentication, Authorization and Accounting) federado para o envio de mensagens de forma controlada pela rede. Ou seja, com este sistema as mensagens enviadas entre sistemas autónomos, dos sistemas autónomos ou para os sistemas autónomos terão de ser autorizadas através de um token JWT[2].

Na imagem seguinte, apresentamos um fluxo habitual de autorização, utilizando Keycloak[3]:

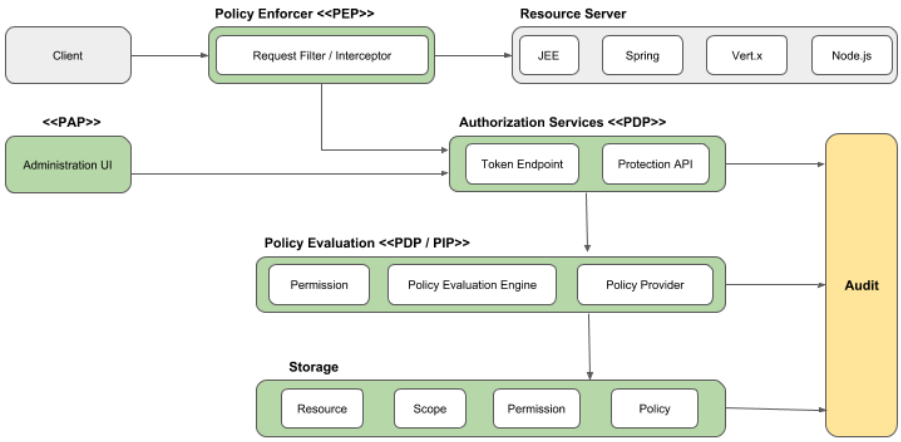

Figura 1 - Exemplo de fluxo de autorização com Keycloak

Para melhor compreensão do objetivo do presente trabalho, juntamos o fluxo de implementação desejado (baseado em Policy Enforcement Points):

[1] https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/
[2] https://jwt.io/
[3] https://www.keycloak.org/

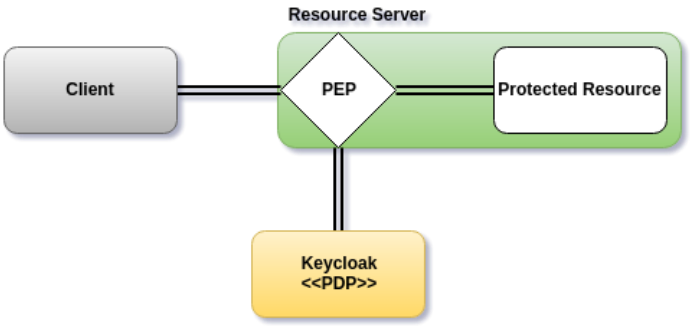

Figura 2 - Fluxo de Implementação de um PEP

Requisitos mínimos para a implementação da solução:

- Utilizar software Open Source (Keycloak, okta, etc);
- Basear a solução em oAuth 2.0 (não se esqueçam de explorar o OpenID Connect, pode dar jeito);
- Comunicar com 2 ou mais sistemas autónomos;
- Utilizar tokens JWT.

Definition of Ready:

A solução está pronta, quando uma mensagem enviada por um sistema autónomo possa ser consumida por outro (utilizando API, Message Bus, Websocket ou outros) de forma autorizada. Isto é, deve ser demonstrado enviando um grupo de mensagens entre diferentes atores da rede de forma autorizada (estas são lidas e recebidas) e outras, por exemplo, sem token, que não são recebidas.

Definition of Done:

A solução estará pronta quando todos os serviços funcionarem automaticamente (i.e. o serviço de autorização está a correr e não precisa de intervenção manual para validar as mensagens).

Exemplos de cenários:

- Domótica doméstica (Smart Home) ou industrial (Industry 4.0) onde a informação de sensorização é trocada entre dispositivos de forma “mais segura”
- Rede wireless em Campus. Informação de sensorização trocada entre postes. Os nós autenticam-se entre si para poderem trocar informação de forma autorizada.
- Este sistema autónomo deverá ser implementado sobre uma rede mesh Wifi, utilizando por exemplo o BATMAN.