Taller de Arquitectura Segura

Carlos Manuel Murillo Ibañez

Luis Daniel Benavides Navarro
Arquitecturas Empresariales

Escuela Colombiana de Ingeniería Julio Garavito
1 de Octubre del 2020
Bogotá D.C.

Índice

1. Resumen

En este artículo se expondrá la teoría y la forma en la que se implementó una arquitectura segura la cual consiste en realizar una aplicación LoginService que es la fachada y que tiene su propio certificado lo cual la hace unicamente accesible con HTTPS esta se comunica con la aplicación OtherService por medio de este protocolo y a su vez tiene su propio certificado.

2. Introducción

Este laboratorio tiene como objetivo principal desarrollar una arquitectura que sea capaz de garantizar la integridad, autorización, autenticación a nivel de usuarios, ademas de que también se garantiza la integridad, autorización, autenticación a nivel de servidores para esto se hace le uso de certificados digitales, de un login y del framework spark para manejar los permisos que se tienen. Para tener mayor claridad del tema en primera parte se realizará una explicación de la teoría que se necesitó para el desarrollo de esta arquitectura, en segunda parte se explicara como esta estructurada y como funciona esta arquitectura y para terminar en la tercera parte se presentaran las pruebas realizadas para confirmar el correcto funcionamiento de la arquitectura.

3. Teoria

- Certificado digital: Es un estándar de seguridad global que permite la transferencia de datos cifrados entre un navegador y un servidor web. [1]

4. Arquitectura

En esta sección se explicará el diseño que se tuvo en cuenta para el desarrollo de esta arquitectura, donde se implementaron dos proyectos un es LoginService y el OtherService

4.1. LoginService

Para la implementación de LoginService se utilizaron dos endpoints uno de ellos es el /login donde se realiza la autenticaccion del usuario y el otro es /information donde se inicia la conexión con OtherService.Para garantizar la integridad, autorización, autenticación a nivel de usuario se implementó un certificado digital que asegura que se harán consultas de manera confiable y segura a través del navegador a su vez tiene un trust store donde se almacena el certificado de OtherService para tenerlo como una fuente confiable y realizar una comunicación segura.

4.2. OtherService

Para la implementación de OtherService se utilizó un solo endpoint el cual es /information el cual se encarga de retornar un mensaje de prueba. Para garantizar la integridad, autorización, autenticación a nivel de servidores se realizó la implementación de un certificado digital y de un trust store en donde se almacena este certificado y así poder dárselo a LoginService y así poder realizar una comunicación de maner segura y confiable.

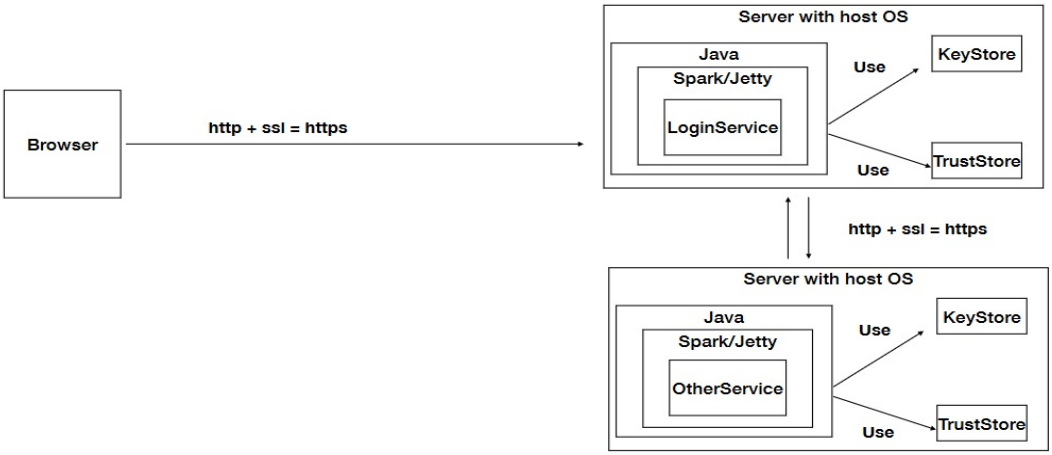

Figura 1: Diagrama.

5. Pruebas

Para asegurar la efectividad y el correcto funcionamiento de la arquitectura desarrollada se hicieron una serie de pruebas.

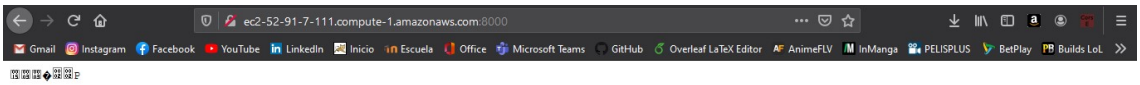

Figura 2: Ingreso a la aplicación LoginService por http.

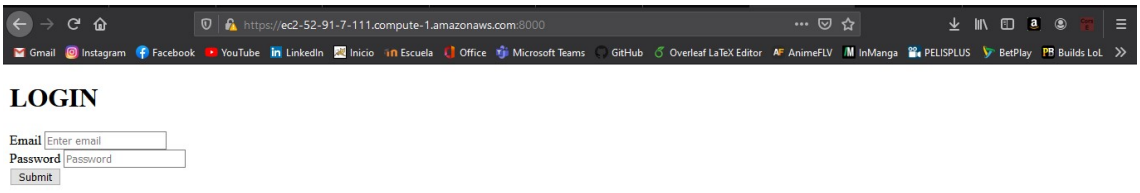

Figura 3: Ingreso a la aplicación LoginService por https.

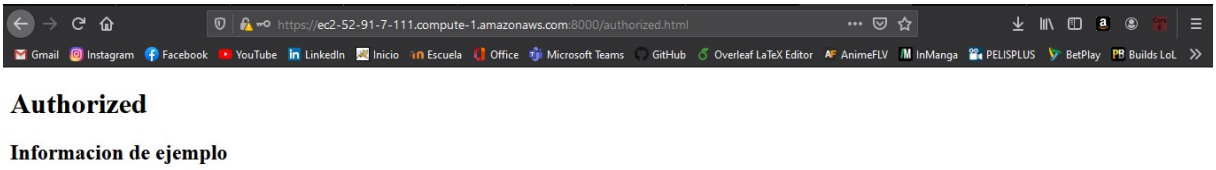

Figura 4: Información retornada por la comunicación segura con OtherService.

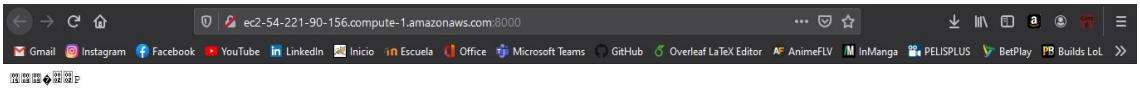

Figura 5: Ingreso a la aplicación OtherService por http.

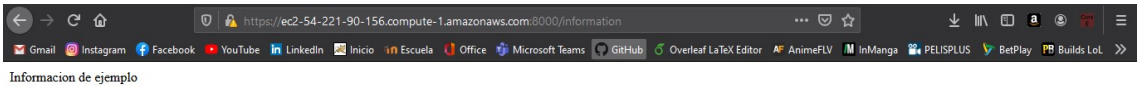

Figura 6: Ingreso a la aplicación OtherService por https.

6. Conclusiones

Gracias a este laboratorio se logró entender mejor la seguridad que necesita tener una arquitectura, ademas de lo importante que es y de como esto puede traer grandes beneficios, también se aprendió a implementar esta seguridad por medio de certificados digitales, logins, truts stores, etc.

Referencias

[1] Certificado. https://www.verisign.com/es_LA/website-presence/online/ssl-certificates/index.xhtml