Aplicación distribuida segura en todos sus frentes AREP 2019

Yohanna Andrea Toro Duran

Escuela Colombiana de ingenieria Julio Garavito

1 Introducción

En el momento de desarrollar una aplicación web es necesario pensar la parte de la seguridad y como garantizar la integridad, autenticación y autorización de cada uno de los usuarios.

Por ende se desarrollo una aplicación web que tiene como objetivo establecer una conexion segura ssl donde la aplicación debe tiene una clave de cifrado que le asigna una autoridad de certificación en la forma de un Certificado. Una vez que haya una única clave en el canal, se establecer una conexión segura utilizando el protocolo SSL..

conexion ssl entre cliente y servidor

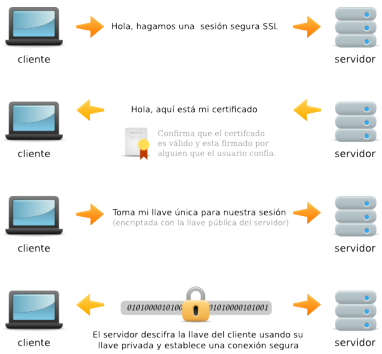


Figure 1. This is an example of a figure caption.

1. Un cliente intenta acceder a https:
2. El servidor responde proporcionando un certificado SSL
3. El cliente recibe el certificado SSL y lo verifica.
4. despues de la verificacion por parte del cliente se establece la comunicación SSL a través de una clave secreta compartida.

5.el servidor descifra la llave del cliente y establece una conexión segura.

2 Arquitectura

A continuación se muestra la arquitectura realizada para una aplicacion web usando como framework spark que consta de un login, registro y perfil de usuario las cuales hace peticiones post y get al servidor este retorna la fecha actual y se establce la el canal seguro entre la aplicacion y el servidor esta se encarga de generar un trustore y un keystore. Donde el trustore se encarga de almacenar los certificados de las entidades de confianza y el keystore se encarga de almacenar las claves del servidor

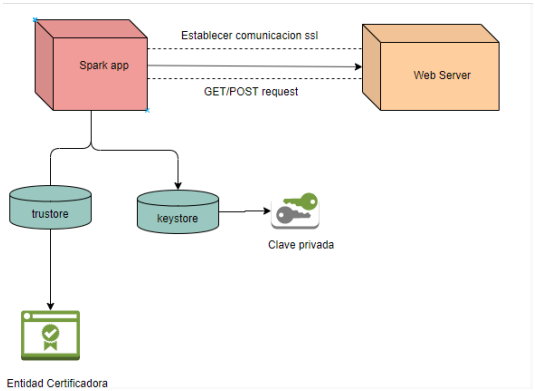


Figure 2.

3 Puebas

1. Establecimiento de ceritificados de confianza en el trustore y keystore

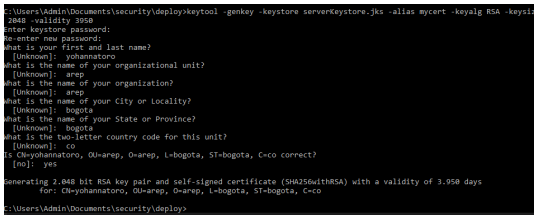


Figure 3.

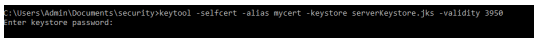


Figure 4.

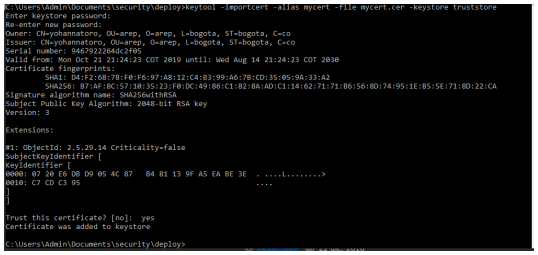
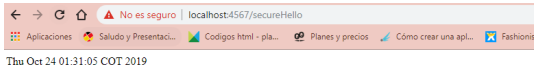


Figure 5.

2. El servidor responde la hora actual



3. desde el lado del cliente en el formulario verifica que la informacion proporcianada en el login esta alamcenada en la base de datos si es correcta permite la autenticacion de lo contrario rechaza el servicio

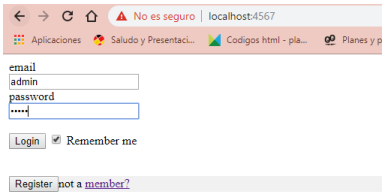


Figure 6.

Figure 7.

4 Conclusión

Las conexiones ssl son importantes debido a que le brinda al usuario seguridad e integridad de los datos que esta manejando dicha aplicación, esto permite que usuarios no autorizados ingresen y tambien a travez de los ceritifcados garantizan que el canal por el que se esta haciendo dicha transaccion es seguro.

References

https://ecolohosting.com/que-es-ssl/ https://www.it-swarm.net/es/java/trust-store-vs-key-store-creando-con-keytool/972567478/