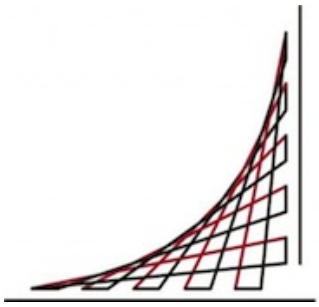

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

Ingeniería de Sistemas

Arquitecturas Empresariales
Laboratorio No.7
Aplicación distribuida segura en todos sus frentes

Diego Alejandro Puerto Gómez
diego.puerto@mail.escuelaing.edu.co

Bogotá
Octubre 2020

1 Introducción

La comunicación en el mundo digital ha traído grandes beneficios en cuanto al desarrollo de la humanidad, ha acercado a a quienes quieren realizar intercambio de información estando a unos cuantos metros o al otro lado del mundo. Se suele compartir información pública o de un alto grado de importancia, y es allí donde se convierte en una prioridad proteger dicha información, pues siendo expuesta podría implicar perjuicios económicos y de cualquier índole.

- **Integridad:** La información es modificable únicamente por los entes y momentos correctos
- **Autorización:** Todo servicio debe ser usado únicamente por los entes autorizados
- **Autenticación:** Es un mecanismo que busca garantizar que la persona o entidad sea ser quien dice ser.

Es necesario entender tres conceptos claves:

Se quiso desarrollar una arquitectura basada en tres principales frentes: un browser y dos servicios; el browser solicitará el acceso a un servicio específico, a través de la autenticación por campos de usuario y contraseña. Se generará una solicitud desde un servicio hacia otro también haciendo uso de una conexión https.

2 Diseño

El browser brinda acceso a un servicio por medio de una conexión https (*HTTP + SSL*) el cual será consumido por un cliente que interactúa con un formulario, allí validará un usuario y una contraseña para consumir correctamente el servicio.

Del mismo modo, los dos servicios ofrecidos, cada uno en una instancia *EC2* de *AWS*, poseen un *KeyStore* (Almacenamiento del certificado ofrecido) y un *TrustStore* (Almacenamiento de los certificados en los que se confía) para poder realizar el consumo exitoso del servicio. Los certificados fueron emitidos gracias una herramienta denominada *Keetool* la cual ofrece la posibilidad de generar pares de llaves y también el *KeyStore* importando el certificado emitido previamente gracias a comandos en *CMD* (figura 1).

El código es soportado por Java, que a su vez hace uso de *Spark/Jetty* que permite el manejo de dichos elementos. Desplegando los servicios en las instancias *EC2* se hace uso de *Maven*, y luego de permitir el acceso a la máquina por puestos específicos, se logra hacer el consumo exitoso del servicio tanto por parte del cliente a través del browser como por tarde de segundo servicio.

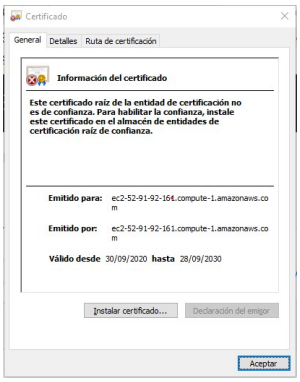

Figure 1: Certificado Generado para instancia *EC2*

3 Conclusiones

- Spark y Jetty nos brindan herramientas para tratar los certificados SSL dentro de código Java y así garantizar que las conecciónes son seguras
- Para garantizar seguridad en el desarrollo y posterior uso de software se deben garantizar tres principios fundamentales: Integridad, Autorización y Autenticación
- Los servicios y en general los servidores, poseen un KeyStore por medio del cual verifican la identidad de las páginas de internet que firman o usan certificados a las cuales solicitan recursos, restringiendo o permitiendo acceso a ellas

References

[1] Incibe-cert. Inicio / Blog / Protocolos AAA y control de acceso a red: Radius Protocolos AAA y control de acceso a red: Radius
`https://www.incibe-cert.es/blog/protocolos-aaa-radius`