ITESO, Universidad Jesuita de Guadalajara

Instituto Tecnológico y de Estudios Superiores de Occidente

Seguridad en Redes

Actividad 10: Firma de Documento WEB

Profesor:
Luis Julián Domínguez Pérez

Autor:
Kevin Antonio Moreno Melgoza
IS714714

Actividad 10 - Firma de Documento WEB

Kevin Antonio Moreno Melgoza
Instituto Tecnologico de Estudios Superiores de Occidente
Guadalajara,Jalisco. México
Email: is714714@iteso.mx

1. Introducción

Esta actividad consistió en desarrollar una página web en donde te pudieras registrar, iniciar sesión subir documentos, firmarlos con tu llave privada con la posibilidad de ver los archivos que se han subido al servidor y verificarlos. Todo desde la página web. Ya habiámos hecho firma de documentos en la clase pasada, pero esta vez el reto era implementarlo en una página web.

October 2, 2020

2. Funcionamiento

Primero tomé mis archivos de la actividad 2 que utilizaba node,consistía en una página web con certificado TLS. Una vez que comprobé que seguía en funcionamiento , procedí a desarollar la página. Primero hice todo frontend y luego el backend, con el que batallé mucho porque solo he llevado la primera materia de Programación Web, no se utilizar ningun framework y además no me acordaba de la parte del backend. PAra la parte de registros y inicio de sesión utilize MongoDb como base de datos. Después de mucho tiempo desarollando la página, porfin conecté el front y el backend. Una vez funcionando el login y register, le agregué la parte de subida de archivos utilizando file-upload de node, express,y globby para mostrar los archivos en el servidor. Después añadí la parte de la firma y verificacion de archivos con ayuda de el paquete de node ”crypto”, cada vez que se sube una archivo al servidor, automáticamente se firma con la llave privada. Una vez que subes el archivo al servidor, siempre se va a mostrar el archivo en una tabla, junto con un botón de verificación y un link para visualizar el código QR generado al firmar el documento.

Finalmente hice las pruebas subiendo archivos y verificandolos. Subí un archivo txt en blanco el cual después de firmarlo, le escribi un texto random. Despues de modificar el archivo lo verifique y si me daba verificación fallida.

3. Código

El código de mi proyecto se encuentra en el siguiente repositorio de Github https://github.com/kevinmorenom/Firma-Documentos-Web

4. Video

Este link redirecciona al video en donde se comprueba el funcionamiento de la actividad.
https://youtu.be/wKEUKGsZ5mk

5. Conclusión

Después de acabar esta actividad me doy cuenta que me tomó exageradamente mucho tiempo. La parte de firmar y verificar me costó trabajo pues habia muchas formas de hacerlo, sinembargo ninguna de ellas me funcionaba pues como no tengo mucho conocimiento de programación web tuve algunos problemas. Después de haber encontrado el paquete correcto fue mas fácil. En general siento que si mi conocimiento de programación web fuera mayor, la actividad me hubiera costado menos trabajo. Aún así estoy feliz con el resultado de mi actividad. Fue interesante implementarlo desde una página web y no desde la terminal.

Bibliografía

OpenSSL.Commands , *https://www.openssl.org/docs/man1.1.1/man1/* , 2020 Consultado 23/09/2020.
.
Firma Digital con OpenSSL , *https://youtu.be/GGirztvijMg* , 2016 Consultado 23/09/2020.

Notes Authentication P2020 , *https://iteso.instructure.com/courses/9418/modules/items/167848* , 2020 Consultado 23/09/2020.

Notes Authentication P2020 , *https://iteso.instructure.com/courses/9418/modules/items/167848* , 2020 Consultado 23/09/2020.

Kevin Méndez - Login y register con nodejs, express, JWT y mongoDB , *https://medium.com/@deskevinmendez/login-y-register-con-nodejs-express-jwt-y-mongodb-ff329ed25a3f*, 2020 Consultado 28/09/2020.

Nuwan Madhawa - Digital Signature for document signing , *https://github.com/itsnuwan/digital-signature-for-document-signing*, 2020 Consultado 01/10/2020.
.