Nombre del alumno: Yahir Aguilar Sicalhua.
Nombre del tema: Actividad 1.
Parcial: 1.
Nombre de la materia: Seguridad en la Información.
Nombre del profesor: Jorge Sebastián Domínguez Torres.
Nombre de la licenciatura: Ingeniería en Sistemas Computacionales.
Cuatrimestre: 9.

UNIDAD II CERTIFICADOS Y FIRMAS DIGITALES

PKI

Una PKI (Public Key Infrastructure, infraestructura de clave pública) es un conjunto de elementos de infraestructura necesarios para la gestión de forma segura de todos los componentes de una o varias Autoridades de Certificación.

HTTPS

Una conexión HTTP estándar en Internet puede ser fácilmente secuestrada por partes no autorizadas. El propósito de una conexión HTTPS es evitar esto: encriptar los datos para asegurar una transmisión de datos segura. La transmisión está encriptada y el servidor autenticado.

SSL

Lo que hacía el SSL (Secure Sockets Layer) y continúa haciendo TLS (Transport Layer Security) de forma más eficiente, es cifrar las comunicaciones mediante el uso de criptografía en diversos servicios online, como el correo electrónico o la web.

TSL

TLS 1.0 es una reimplementación mejorada de SSL 3.0, con suficientes diferencias para que ambos sean incompatibles entre ellos.

Las diferencias entre TLS y SSL es que la primera mejora al segundo corrigiendo vulnerabilidades de seguridad que se han ido encontrando en SSL, y que en TLS se autentifica al cliente, mientras que en SSL no.

SSH

SSH (Secure SHell) es un programa que nos permite comunicarnos, mediante una línea de comandos, con un servidor remoto de forma segura.

Fuente de información:
https://plataformaeducativauds.com.mx/libro.php?idLibro=172107258016