Programación para las Comunicaciones – Práctica 3

Enunciado

Requisitos obligatorios

El objetivo de esta práctica es implementar un canal seguro en la aplicación calculadora desarrollada en la práctica 2, utilizando los protocolos SSL y/o TLS. Se mantendrán sendos hilos en escucha para atender las peticiones no seguras y las peticiones seguras, en dos puertos distintos, intentando reutilizar la mayor cantidad de código posible. Se requerirá tanto autenticación de cliente como de servidor. Para ello se generará un certificado de servidor y un certificado de usuario (para el cliente).

Operativa de la aplicación

La operativa de la aplicación será la misma que la descrita en la práctica 2, y no debe de haber diferencia entre el funcionamiento seguro y no seguro.

Requisitos opcionales

Se podrán proponer por parte de cada uno de los alumnos, mejoras y extensiones adicionales al enunciado de la práctica. Se valorará el uso de certificados firmados por una CA, en lugar del uso de certificados autofirmados.

Herramientas

Para el desarrollo de la práctica se utilizarán las siguientes herramientas:

- Eclipse IDE for Java Developers. http://www.eclipse.org/

Entrega

La entrega de esta práctica se realizará medaiante la tarea correspondiente dentro de la herramienta '*Tareas*' del Aula Virtual, adjuntando un fichero comprimido (.zip) que incluirá los siguientes elementos.

- **Memoria técnica** de la práctica desarrollada en formato PDF, con una extensión máxima de DOS páginas. Se incluirá en un directorio */doc*. Deberá incluir: nombre y apellidos del alumno, descripción de la solución (diseño e implementación).
- **Archivos** relativos al trabajo desarrollado (código fuente y ficheros de configuración/ejemplos). Se incluirá en un directorio */src*.
- **Base de datos** con la información relacionada con los certificados (archivos X.509, claves privadas, CA, etc). Se incluirá en un directorio */cert*