REDES DE COMUNICACIONES II

Práctica 2 - Seguridad y criptografía

Volver a: Prácticas

1 Introducción

El objetivo de este segundo trabajo del curso es llevar a la práctica todos los conocimientos sobre seguridad y criptografía estudiados en teoría. Para ello se ha desarrollado un servicio de almacenamiento seguro de ficheros, llamado **SecureBox**, accesible mediante una API REST.

Este servicio permite recibir y enviar ficheros cifrados y firmados, para lo que se deberá diseñar e implementar un cliente (en Python o C, a elección del estudiante) que consuma este servicio y permita una serie de acciones desde la línea de comandos.

En líneas generales, el servicio SecureBox aporta dos grandes funcionalidades:

- **Repositorio de identidades**, al estilo de un servidor de claves PGP. En este almacén los usuarios pueden registrar sus identidades (clave pública y datos de identificación), de forma que otros usuarios puedan buscarles, recuperar su clave pública y enviarles archivos.
- **Almacén de archivos**. Los archivos anteriores no se envían directamente al usuario destinatario, sino que son almacenados en el servidor, para que éste pueda recogerlos posteriormente.

Por tanto, en esta práctica se deberá desarrollar un cliente de línea de comandos que consuma el servicio de SecureBox y que, a grandes rasgos, permita:

- Gestionar la identidad (crear, exportar, buscar y borrar) de un usuario, realizando las llamadas adecuadas al API de SecureBox. Un usuario solo podrá disponer de una identidad en cada momento.
- Cifrar y firmar archivos de forma local. En el primer caso, se deberá especificar la identidad del destinatario.
- Enviar un archivo al servicio SecureBox, que deberá haber sido previamente cifrado y firmado.
- Recibir un archivo almacenado en SecureBox, comprobando tras su descarga su firma digital.

Volver a: Prácticas