Lab 3: Secure Sockets (SSL/TLS)

Deadline: Friday 2/10 17:00

This lab can be done by at most two persons

This lab is about to implement secure sockets in Java. To be approved on this lab, you must demonstrate your program to Pierangelo.

Problem description

Consider a situation where we have a server whose file system contains files with sensitive information. Clients (if authorized) can:

- download
- upload, and
- delete files

(say text files) by connecting to the server via a secure connection (SSL/TLS). The client tells the server only the file's name it needs (suppose for simplicity that all the files on the server are located in the same folder, so the client does not have to specify where it is located). Basically, you have to implement a kind of secure FTP.

The following security conditions must be guaranteed by your Java program:

1. data integrity must be guaranteed
2. every file exchanged must be encrypted
3. client and server communicate via strong cryptographic algorithms
4. client and server have distinct keystores and truststores
5. the client must authenticate the server
6. the server must authenticate the client