Linnéa Mellblom
linme882
Linnéa Nåbo   linna887

TNM031 Lab 4 Rapport

Group number 9 and ports 4001 and 4020

In this lab, connections to two different webpages are attempted.

In the first task no additional information about which sites to trust or not is given. The https connections give the following responses:

- liu.se
  response: 200 (OK).
- tal-front.itn.liu.se
  error message: "java.security.cer.CertPathValidatorException: Trust ancor for certification path not found. "

Normally an https connection only allows well known CAs.
In this case, only the liu.se site has a well known certificate, while the tal-front page has a self-signed certificate, which is not trusted by a normal https connection.

In the second task, one more certificate is trusted, the tal-front with port 443. A keystore is created that includes the trusted CAs. Thereafter, a trustmanager is created, which trusts the CAs of the keystore. After establishing an SSL connection and trying to connect to the tal-front page through two different ports the following responses are sent:

- Port 4001
  response: 200 (OK).
- Port 4020
  error message: "java.security.cer.CertPathValidatorException: Trust ancor for certification path not found. "

The reason for this is that the 4001 port probably has the same certificate as the trusted port 443, while the second port is self-signed and therefore not trusted.