VPN Project General Information

In this project, you will implement a server and a client that implement a VPN – Virtual Private Network. A VPN is a secure network that runs of top of the existing Internet infrastructure. You can think of a VPN as a network of secure links, or *tunnels*, established over a public infrastructure. By connecting themselves to the VPN, clients can communicate with each other in a secure way through the tunnels.

This project includes many pieces of what is covered in this course:

- Encryption keys
- Symmetric encryption
- Public-key encryption
- Certificates

Organisation and Requirements

The project is organised in two parts. The first part consists of a number of smaller preparatory assignments, "tasks", which gradually introduce the concepts and where you implement basic functionality that you need for your VPN. Each task has its own due date.

In the second part, you take what that you have implemented in the first part, and put it together into a VPN system. This VPN consists of a client and a server implementation. The due date for submitting your implementation of the VPN system is the main due date for the entire project assignment.

The project is intended to be implemented in Java using JCA (Java Cryptography Architecture). There are licensing restrictions for Java that you need to be aware of, and for this project, it is assumed that you follow the recommendations at KTH. See https://intra.kth.se/it/programvara-o-system/system/oracle-java-new-license-1.862964 for more information about using Java at KTH.

Requirements

The requirements for completing the project assignments are:

- Submit solutions to all preparatory assignments before their respective due dates
- Submit a VPN implementation, consisting of a client and server, before the project's due date

More details about the requirements can be found in the instructions for each component.