PROJECT OUTLINE FOR BACHELOR'S THESIS IN COMPUTER SCIENCE

Place: Oslo

Date: 11.12.2019

Project name: Chestnut, Educational PKI Web App

Group members:

Abozar Afzali (INFORMATIK) – S315578@oslomet.no

Konstantinos Pascal (INFORMATIK) - S315567@oslomet.no

Assignment giver and contact person:

Thomas Sødring, Associate professor

Faculty of Social Sciences

Department of Archivistics, Library and Information Science

Thomas.Sodring@oslomet.no

Office: +47 67 23 82 87

Pilestredet 48, 0167 Oslo

Office number: R407

Assignment giver introduction:

Thomas Sødring is a professor at the Faculty of Social Sciences, OsloMet. Over the time, he has developed tools, some of which he has used to teach students the core concepts of computer science such as PKI, SOAP and REST.

Project description:

Chestnut aims to be a simple educational tool that can be used to teach both students and others interested, the principles behind PKI (Public Key Infrastructure). Currently, Chestnut has a Java implementation written in JavaFX, but which is not entirely functional. The application can be found at https://gitlab.com/OsloMet-ABI/chestnut

Our job is to take Chestnut and make it into a web application. This will solve many of the current issues, such as software portability between different environments. The implementation will mainly be in React for the front-end side and UI, together with Bootstrap or any other fitting toolkit for the design

We will also be using several cryptographic libraries for JavaScript for the basic operations of key generation, signing, verification, encryption and decryption. We have yet to decide upon these libraries, but our supervisor has given us the freedom to choose them ourselves.

Here are some of the more important project specifications for Chestnut:

- Creation and loading of private/public keys
- Signing data with private key and verifying of data with public key
- Encrypting of data with public key and decrypting data with private key
- Support for several encryption algorithms, both symmetrical and asymmetrical
- Exchange of data and public keys between users