Java: OpenSSL goes Java

Motivation
Occasionally one needs to manually inspect/create/edit cryptographic information like keypairs, certificates, etc. Having a generic tool that supports many of such operations is very practical. Our Java Toolkits don’t provide such a comprehensive tool like e.g. OpenSSL does. This project implements such a tool with a graphical interface as well as a command line interface. The tool should be designed in a modular and extensible way.

Project description
• Goals
  • GUI/Commandline tools for standard crypto operations like
    – Key pair generation
    – Certificate issuing
    – Document Signing and Encrypting
• Tasks
  • Implementing basic functionality
  • Making functions accessible using a command line interface
  • Making functions accessible using a GUI

Literature
• IAIK JCA Documentation, jce.iaik.tugraz.at
• OpenSSL manpages

Deliverables
• Project files (.zip, cleaned)
• Documentation (inline)
• User guide (getting started)
• Presentation (10 .ppt slides)

Project schedule
• Start Immediately
• Month 1 Reading, designing function set and commands, prototyping GUI
• Month 2 Implementation
• Month 3 Final deliverables

Master Project
Studies: INF SEW TEL
Prerequisites
• Java programming (Eclipse, git)

Advisor / contact
Peter.Lipp@iaik.tugraz.at
Dieter.Bratko@iaik.tugraz.at