Pretty Good Privacy

Motivation
OpenPGP is a non-proprietary protocol for encrypting email using public key cryptography. It is based on PGP as originally developed by Phil Zimmermann. The OpenPGP protocol defines standard formats for encrypted messages, signatures, and certificates for exchanging public keys. IAIK's set of Java(TM)-based tools misses an implementation of PGP.

Suitable for a team of two.

Project description

- Goals
  - Develop a PGP implementation based on the IAIK toolkit suite.
- Tasks
  - Study RFC 4880 and related background material
  - Implement a class library covering the PGP elements (Key Ids, Keyrings,...)
  - Implement the different packets
  - Implement en-/decoding
  - Handle Algorithm Preferences
  - Test Interoperability with other implementations
  - Implement a user interface to demo the workings of the library

Deliverables

- Project files (.zip, cleaned)
- Documentation (inline)
- Readme (getting started)
- Presentation (10 .ppt slides)

Project schedule

- Start Immediately
- Month 1 Reading, IAIK tool evaluation
- Month 2 Development
- Month 3 Development, final deliverables

Bachelor Project
Studies: ☑ INF ☑ SEW ☑ TEL

Prerequisites

- Java programming
- Android
- Digital XML signatures

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