Java: Crypto Protocols

Motivation
The world is full of all sorts of protocols that applications may want to use for different purposes. They have been standardized by different standardization organizations or user groups. We want you to implement one of them using our own crypto toolkit. Examples are XMLDSig 2.0, XMLEncryption 1.1, Json Web Signatures, Widget-Signatures, KMIP, XKMS, CMP, SCEP, CRMF, AS2, Adaption of ODF, UCF, Word Format for ASIC containers...

Project description
- Goals
  - Implementation of one protocol
  - Prototype Application using the protocol implemented
- Tasks
  - Selection of protocol (in coordination with advisor)
  - Designing implementation based on standard
  - Implementation as a toolkit
  - Implementation of prototype application

Literature
- IAIK JCA Documentation, jce.iaik.tugraz.at
- Specification of protocols

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

Project schedule
- Start: Immediately (incl. selection)
  - Month 1: Reading, designing implementation
  - 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
Konrad.Lanz@iaik.tugraz.at