JWS: JSON Web Signatures

Motivation
JavaScript Object Notation (JSON) is a lightweight, text-based, language-independent data interchange format that gains more and more importance. There also is an internet draft on JSON Web Signatures. We want to investigate what it takes to create and validate such signatures and what their advantages and drawbacks are.

Project description
- Goals
  - Develop an implementation that handles JSON Web Signatures as currently defined
  - indraft-ietf-jose-json-web-signature-18
- Tasks
  - Study the relevant standards
  - Look for a suitable JSON implementation in Java
  - Design an implementation for JSON Web Signatures
  - Implement Signatures
  - Test JSON Web Signatures by creating an Android App for our time management system that uses signatures to commit time declaration to the system (if time allows)

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

Project schedule
- Start: Immediately
- Month 1: Reading, JSON investigations
- Month 2: Signature implementation
- Month 3: App development, final deliverables

Bachelor Project
Studies: INF SEW TEL

Prerequisites
- Java and Javascript programming
- Android

Advisor / contact
Harald.Bratto@iaik.tugraz.at
Christof.Rath@iaik.tugraz.at
Manuel.Schallar@iaik.tugraz.at
Simon.Roth@iaik.tugraz.at

http://www.iaik.tugraz.at/