# OPENSIGN PROJECT - DESIGN

This document gives an overview of the software design of OpenSign server and client.

## 1. Open SIGN Server

The language of choice for writing the server is Java 1.6. The server application depends on the open source libraries BouncyCastle, for handling cryptographic operations, as well as on Hibernate, which serves as persistence on top of a relational database.

The server architecture follows the REST principle [1]. This is convenient as the server requires a web-interface as well as a web-service interface. With this RESTful architecture both goals are met.

### RESOURCES

Following resources are accessible:

|  |  |
| --- | --- |
| / | Will show index.html |
| /login | Page for handling user login |
| /users/[user name] | User profile |
| /ca | Root of a X.509 hierarchy  GET: returns the root public key  POST: takes a CSR and returns the certificate in case the user is authorised |
| /ca/[approver name] | First level of hierarchy  GET: returns public key of approver  POST: takes a CSR and returns the certificate in case the user is authorised |
| /ca/[approver name]/[user name] | Second level of hierarchy  GET: returns public key of the user  POST: takes a CSR and returns the certificate in case the user is authorised |
| /admin | Administration area |
|  |  |

### Building

Project is build using the build tool Maven2 [2].

TO BE CONTINUED

[1] <http://en.wikipedia.org/wiki/Representational_State_Transfer>

[2] <http://maven.apache.org/>