

# Projeto Final de Curso

Paul Crocker

## Título

Autenticidade dos Dados do cartão Cidadão

## Objetivo

O objetivo deste projeto é criar um modulo para uma biblioteca de Software que efetua o processo de verificação de autenticidade dos dados do Cartão de Cidadão (CC).

A autenticidade dos dados do CC é feito usando um ficheiro SOD (Security Object Data) que é colocado no cartão durante a fase na sua personalização que contém assinaturas eletrónicas sobre os dados de identificação, fotografia, morada e chaves criptográficos

Este verificação deverá ser efetuado usando a linguagem Java e fará uso das bibliotecas BouncyCastle (Desktop) e SpongyCastle para a versão para a plataforma Android.

Este projeto envolverá também a documentação e descrição do processo de verificação de autenticidade e criação dum plataforma de Testes.

## Plano de Trabalho

- Review of Hashes, Signatures and TimeStamps.
- Digital Certificate Standards and Formats.
- The Java Cryptography Architecture
- Verifying Digital Certificates -CLR's and OCSP.
- The Portuguese E-Id Card
- Standard Middleware - SOD and PKCS15.
- Desktop Module
- Android Module
- Test Suite and Documentation
- Project Report.

## Requisitos Técnicos

Programação. Estruturas de Dados. Sistemas Operativos. Segurança Informática .

## References (WEB)

- 1 Manual técnico do Middleware Cartão de Cidadão
- 2 PKCS 15—A Cryptographic-Token Information Format Standard for SmartCards

## Contactos

Paul Crocker