# OpenCA Workshop 2005

## OpenCA as a backbone for a Liberty compliant Trusted Secure Network

Chris Covell
Diginus Ltd.

diginus

# Introduction

- NERSC (North East Regional Smartcard Consortium) based in Sunderland, UK has developed a Trusted Secure Network based on Liberty 1.1 standards.
- OpenCA acts as the backbone of the infrastructure supplying digital certificates creating a users identity.
- Digital identities, located on a smart card, allow users authenticated access to online and offline services and products.

diginus

# What are the business benefits ?

- Regional infrastructure
- Aimed at Local Government, education and Local Businesses (transport, leisure and business).
- Supported by many applications:
  - Eduction (Sunderland University)
  - Football clubs
  - Local Government employees
  - Benefits claimants

diginus

# Technology

- Identity infrastructure is provided by Sun Identity Server.
- Smard cards managed and issued by ActivCard AIMS Smard Card Management System.
- Digital certificates issued by an OpenCA PKI infrastructure managed by Diginus Ltd.
- Root certificates created and stored on a SafeNet Luna SA key in hardware device.
- Project management by Fujitsu UK.

diginus

# Implementation

- OpenCA 0.9.2.2 out of the box implementation.
- Shared CA and RA database (no import/export).
- Certificates created by OpenCA Batch Processor.
- Bespoke routines extract certificates and private keys and store them encrypted on a new database.
- An API between AIMS and the PKI allows Registration Agents to securely download certificates and key pairs and submit a revocation request.

diginus

# Implementation (cont)

- The encrypted keys and certs are decrypted and re-encrypted for the AIMS system during the download.
- Revocation requests are injected directly into the OpenCA screens via http.
- An RA operator processes the revocation requests whenever they occur. We have an automated process to mail the operator.
- An automatic routine creates a CRL daily

diginus

# Proposed Enhancements

- The method of creating anonymous certificates up front and then having them called off is not ideal.
- An on-line CA would be better with trusted requests being processed automatically. This would require automated RA signing of approvals.
- Hope to use the OpenCA shell interface of 0.9.3 to create an online CA. There will be a requirement for high trust personalised certificates.

diginus

# Enhancements (Cont)

- At the moment we have scripts that “scrape” the html screens, this would benefit from the shell interface.

diginus

# Where is the project now ?

- 2 Pilots in place so far.
- More than 5000 smart cards issued with digital certificates.
- NERSC actively looking for new pilots.

diginus