# 1. OpenCA Workshop
# OpenCA today and future


Core concepts and Future

# Overview

- Core concepts
  - Daemons
  - Objectorientation/Framework
  - Access control
  - I18n
- Future
  - General Plans
  - Design decision from yesterday

# Daemon concept

Apache <==>OpenCA Daemon <==> XML cache

- Apache frontend to OpenCA daemon
- XML cache - very simple and fast, hash based
- What's the job of the daemon?
  - Framework for the commands
  - Initialization cache (Performance)

# Objectorientation/Framework

- Modules for crypto stuff abstraction
- Libraries
- Pre-initialized Objects
- Examples:
  - OpenCA::X509, OpenCA::Token::*
  - export-import.lib, crypto-utils.lib
  - $cryptoShell, $crypto_layer

# Access Control

- Apache frontend collects connection infos
- Channel verification
- Login
  - None
  - X.509
  - Passwd
  - external
- Session management

# Access control - interfaces

- What is an interface?
  - Some entries in acl.xml
  - An own etc/access_control/interface.xml
  - A frontend CGI script to the OpenCA daemon
  - A configuration for the frontend CGI script

# Internationalization (i18n)

- Javascript
- Mails
- Central translation:
  - openca.pot
    - Automatic exctraction with exclusions made by hand
    - Additions by hand
  - Language code in Makefiles and initServer

# Good News

0.9.2.0 was tagged at 2004-Oct-11

# Future – Design Decision

- SQL only
- Logging
  - Audittrail for authentication and data manipulation
  - Syslog for authentication
- Cryptobackend
  - Transactional behaviour of OpenCA::OpenSSL
  - UTF8 support
- Keymanagement
- Safe (flexible) serial generation

# Future – Features

- No temporary files outside of OpenCA::OpenSSL
- Support for automated certificate rollover
- Batchsystem
  - Job oriented
  - Commandline interface
- Cronjob interface
- Private key usage counter

# Future – Features

- Online-CA
  - Automatic CRL generation
  - Automatic cert signing
  - Automatic CRR processing
  - Partially encrypted configuration
- Signed configuration