

African and Arab Regional Conference
on Electronic Transaction Security and PKI

The



And

The EuroPKI Infrastructure

Massimiliano Pala
OpenCA Project Manager

Tunis, 20th-22th June 2005

Introduction

- The OpenCA Project
 - **History**
 - **Goals of the project**
 - **Development Driving Principles**
 - **Current Core Features**
 - **Future Plans**

- The EuroPKI infrastructure
 - **History**
 - **Infrastructure Policies**
 - **Infrastructure Experience**

Introduction

- The OpenCA Project
 - **History**
 - **Goals of the project**
 - **Development Driving Principles**
 - **Current Core Features**
 - **Future Plans**

- The EuroPKI infrastructure
 - **History**
 - **Infrastructure Policies**
 - **Infrastructure Experience**

OpenCA History

- OpenCA is a spontaneous Open Source project born from the need of a group of people implementing a PKI in a real environment
- The project started in 1998 providing the software for setup and managing a PKI
- First versions of the software were simple script interfaces to the crypto library SSLeay (former name of the OpenSSL suite)
- From 0.6 versions the project adopted a modular structure by splitting its code base into modules, command and libraries
- Actual version of the project is 0.9.2.2
- Finally heading for 1.0 by the end of the year

Goals of the Project

- The project goals are:
 - **to provide a full featured PKI software for both critical infrastructures as well as research framework**
 - **to be compliant with standards**
 - **to provide a flexible and extendible tool**
 - **to build a community of users and developers which can help the project in its mission by providing feedback and new ideas (as well as code) to the project**
 - **to be free**

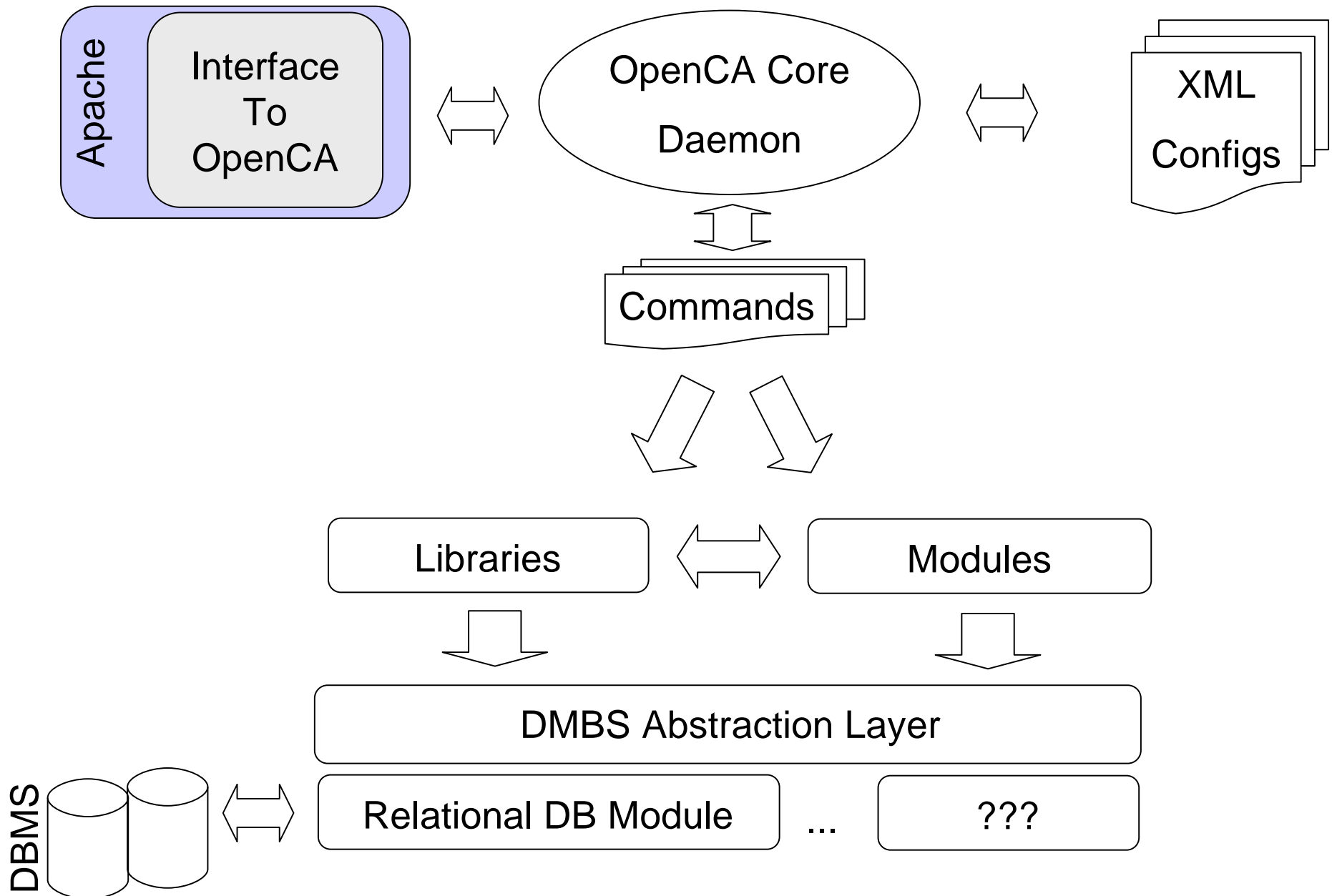
Development Driving Principle-1

- **Standard and flexible interfaces.** For this purpose we decided to use standard HTML from the very first version of the project
 - **All users and operators interaction with the CA/RAs components are accessible via standard browsers**
- **Portability and Productivity.** We wanted the project to be as much portable as possible, moreover we wanted new developers and users to be able to look into the project code and easily provide new code and/or patches, therefore the main programming language is PERL

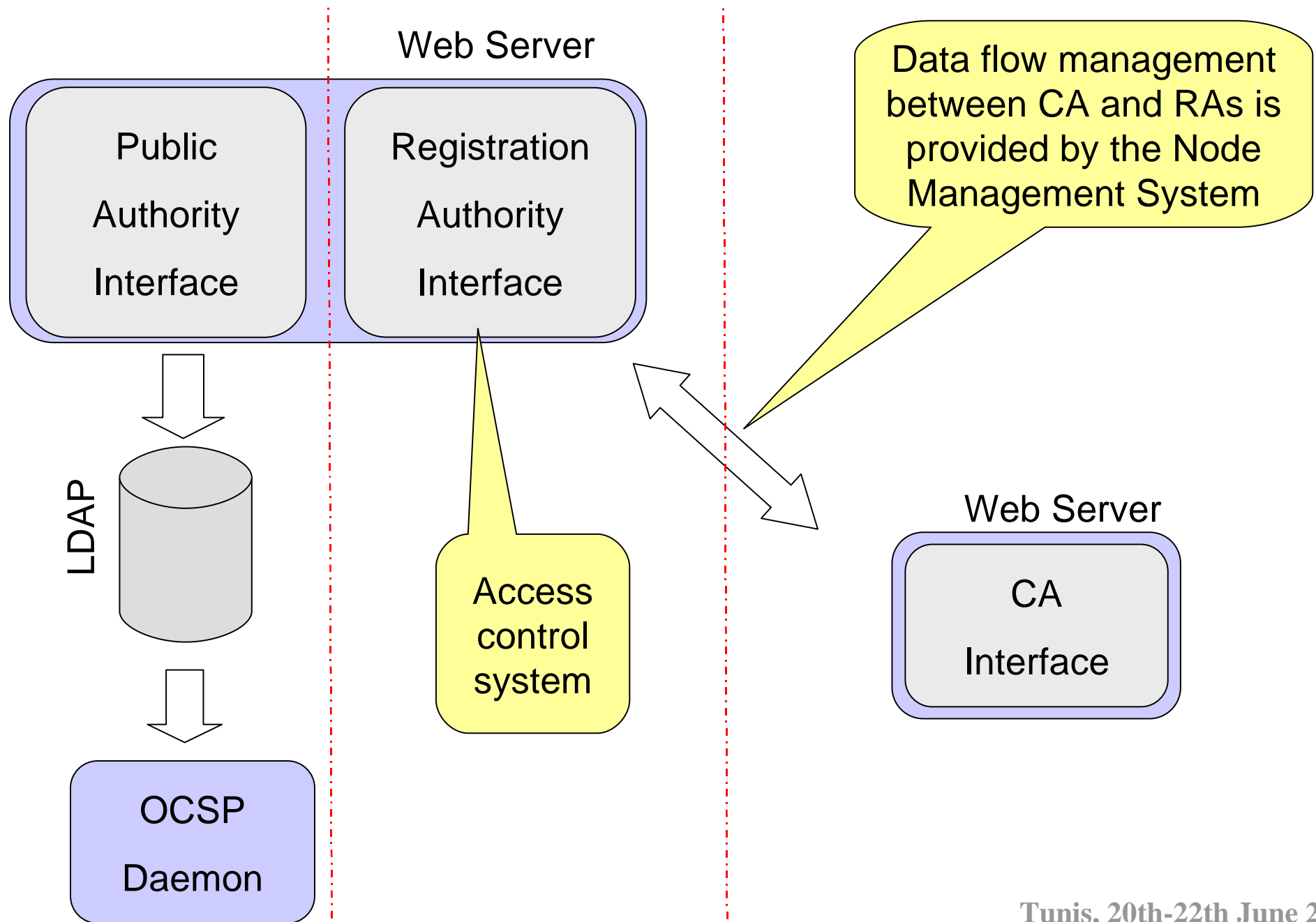
Development Driving Principles-2

- **Code modularity.** By providing libraries, modules and separated command files it is easy to modify functionalities and integrating new features at all levels from user interface to internals (e.g. integration of Hardware Accelerators usage, Data Base abstraction, etc.)
- The OpenCA project uses many different open source mature project as its basis:
 - **OpenSSL** provides the crypto libraries
 - **OpenLDAP** provides the LDAP server for certificates and CRLs publication
 - **Apache** provides the server used by Interfaces
 - **External PERL Modules** provide many useful features

OpenCA Internal Structure



CA – RAs Interactions



OpenCA Core Features-1

- **Access Control System** permits to restrict access by using different authentication methods:
 - **None, simple passwords, X.509 certificates**
 - **external (the system allows for additional authentication mechanisms to be integrated)**
- **Dataexchange System** manages the data flow between different nodes of the PKI, in particular it takes care of data flow between:
 - **CA and R**
 - **Different RAs (support for hierarchical RAs structure)**
- **Batch System** provides all the needed feature to automate the CA/RA operations at different levels (e.g. Key management, Certificate Issuing and Renewal, etc...). It supports the definition of new class of operations (extensible)

OpenCA Core Features-2

- **SCEP System** provides the interface to many network devices by supporting the SCEP protocol:
 - **Command line implementation**
 - **Supports access management by using the Access Management System provided by OpenCA (preventing access abuses from public networks)**
 - **Reported to work with many devices (e.g. Cisco PIX, Cisco VPN Client, NetScreen ScreenOS 4, F-Secure VPN+, SSCEP, Cisco 3640)**
- **LDAP System** manages all interactions between RAs and LDAP server (if one is installed/used). It publishes issued certificates and CRLs to LDAP repository.

OpenCA Core Features-3

- Support for internationalisation is provided, currently supported languages are:
 - **English**
 - **Italian**
 - **German**
 - **Japanese**
 - **Polish**
 - **Slovene (first UTF-8 based)**

OpenCA Future Plans-1

- Command Line API for CA and RA operations. This would hopefully lead to the possibility of enabling XKMS, SOAP and CMS clients
- Automation of processes to diminishing costs and efforts tied to staff (e.g. CRL and Certificate issuing)
- On-Line CA model support for ease of usage in environment where some kind of authentication is performed elsewhere (e.g. in universities students are usually authenticated when they subscribe their study course)
- Scalability and Mass Issuing
- High-Risk environment mode support (e.g. by using RO supports and dedicated hardware protected storage for private keys)

OpenCA Future Plans-2

- Audit of CA and/or RA operations to a tamper proof signed log. By implementing such an audit logging system it will probably be possible to achieve some form of certification (e.g. for special environments like bank systems)
- Automated CA rollover support
- TimeStamping services implementation and integration within OpenCA

OpenCA References

- OpenCA HomePage:
<http://www.openca.org>
- Project Manager Contact:
Project dot manager at openca dot org

The EuroPKI Infrastructure

Introduction

- The OpenCA Project
 - History
 - Goals of the project
 - Current Core Features
 - Future Plans

- The EuroPKI infrastructure
 - History
 - Infrastructure Policies
 - Infrastructure Experience

The EuroPKI History

- EuroPKI is a spontaneous aggregation of partners
- The project started in 1996 providing PKI services within the EC funded projects ICE-TEL and ICE-CAR
- In January 2000 the partners of ICE-CAR project decided to broaden the scope of the infrastructure. The Politecnico di Torino offered to run the Root at least until 2010
- The NASTEC project used EuroPKI to promote secure applications in the newly associated states (NAS) to the European Union
- The project continues to grow as new countries join the hierarchy:
 - **Romania**
 - **Poland**
 - **Greece**

EuroPKI Policies

- It is a non commercial infrastructure
- The root CA is run by the Politecnico of Turin (italy)
- Partners from everywhere are welcome to join the infrastructure
 - **The only requirement is to be compliant with the EuroPKI policy document**
- The EuroPKI infrastructure helps in providing an open environment where research and common usage of certificates have been deployed (the value of certificates resides in applications not in the certificate itself)
 - **Several partners developed certificates-enabled applications**
 - **EuroPKI provides a series of services to the partners (e.g. OCSP and TSA)**

EuroPKI Experience-1

- EuroPKI demonstrated its usefulness in supporting the security needs of end-users
- The project helped in providing a common ground where universal and frequent problems could be discussed and solved
- Experience shows that problems can be solved:
 - **Technical standards do exist**
 - **Products implement standards**
 - **Most of the times its just a matter of proper configuration and management**
- Real problems still lie in application and end-user sides.
Developers:
 - **have not security as a priority**
 - **have poor understanding of PKI**

EuroPKI Infrastructure Experience-2

- Several partners developed certificates-enabled applications
- EuroPKI provides a series of services to the partners
 - **OCSP**
 - **TSA**

EuroPKI References

- EuroPKI HomePage:
<http://www.europki.org>
- Project Contact:
security at polito dot it

Questions

