OpenCA and the PKI-LDAP Project

First OpenCA Workshop,

TU München, 12.10.2004

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International

Directory Applications
for Advanced Security
and Information Management

Agenda

- Introduction to PKI/LDAP-Project
- Central server components
- LDAP integration and OpenCA
- OpenCA evaluation

Project PKI-LDAP

- Aim: setup of a PKI on the basis of LDAP indexes for all Baden-Württemberg universities
- Work programm:
  - Evaluation of existing CAs and directories in Baden Württemberg Universities
  - Central Server components (see below)
  - Support and coordination of lokal directories and Identity Management projects
  - Implementation of PKI based value added services (S/MIME, SSL, VPN, Webauthorisierung, User-Interfaces)
  - Public relations

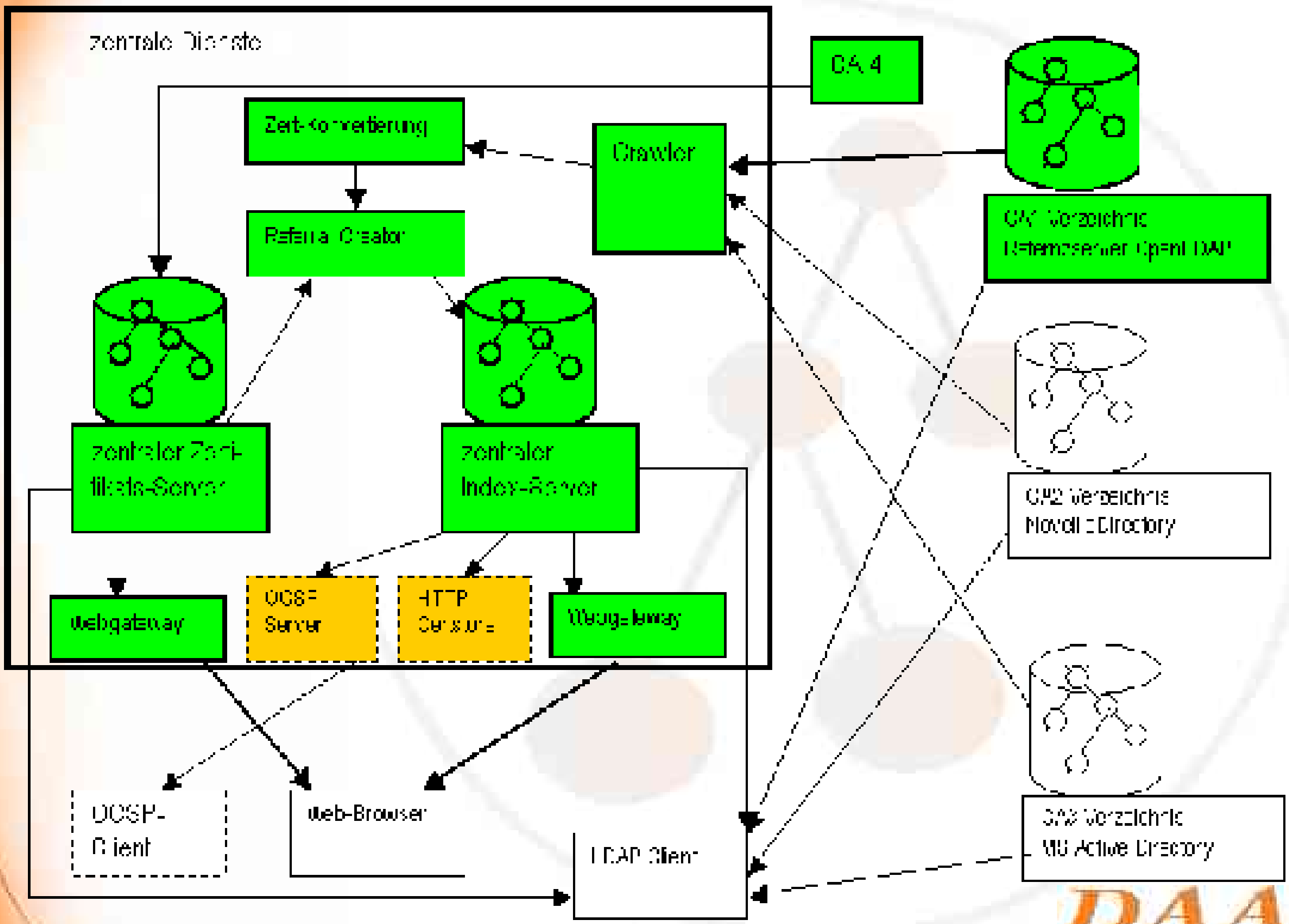
Project PKI-LDAP

- Duration: 2 years (one year is already over)
- Participants: Universities of Freiburg, Heidelberg, Hohenheim, Karlsruhe, Konstanz, Mannheim, Stuttgart, Ulm, und Tübingen, as well as DAASI International GmbH
- Effort allocation: 10 Person years
- Subdivision in autonomous project parts
- More info: www.pki-ldap.uni-tuebingen.de

Project part central server

- Tasks:
  - Central certificate directory for those local Cas that don't operate an own directory
  - Index directory server which contains data about all certificates of all Cas within the project
  - Reference LDAP server on basis of OpenLDAP
  - Specification of certificate profiles

Project part central server



DAASI International

Directory Applications for Advanced Security and Information Management

New LDAP schema for certificates

- IETF-Draft: Gietz, Klasen, Internet X.509 Public Key Infrastructure LDAP Schema for X.509 Certificates, draft-ietf-pkix-ldap-pkc-schema-00.txt
  - Every certificate is stored in a separate entry
  - In addition to the binary certificate, contents of the single certificate fields and extensions are stored in separate LDAP attributes to make them easily searchable („metadata approach")
- Related documents on CRLs and Attribute certificates:
  - Chadwick, D. W., Sahalayev, M. V., Internet X.509 Public Key Infrastructure LDAP schema for X.509 CRLs, draft-ietf-pkix-ldap-crl-schema-01.txt
  - Chadwick, D. W., Sahalayev, M. V., Internet X.509 Public Key Infrastructure LDAP Schema for X.509 Attribute Certificates, draft-ietf-pkix-ldap-ac-schema-02.txt

Examples of new attributes

X509serialNumber; x509signatureAlgorithm; x509issuer;
X509validityNotBefore; x509validityNotAfter;
x509authorityKeyIdentifier; x509authorityCertIssuer;
x509authorityCertSerialNumber;

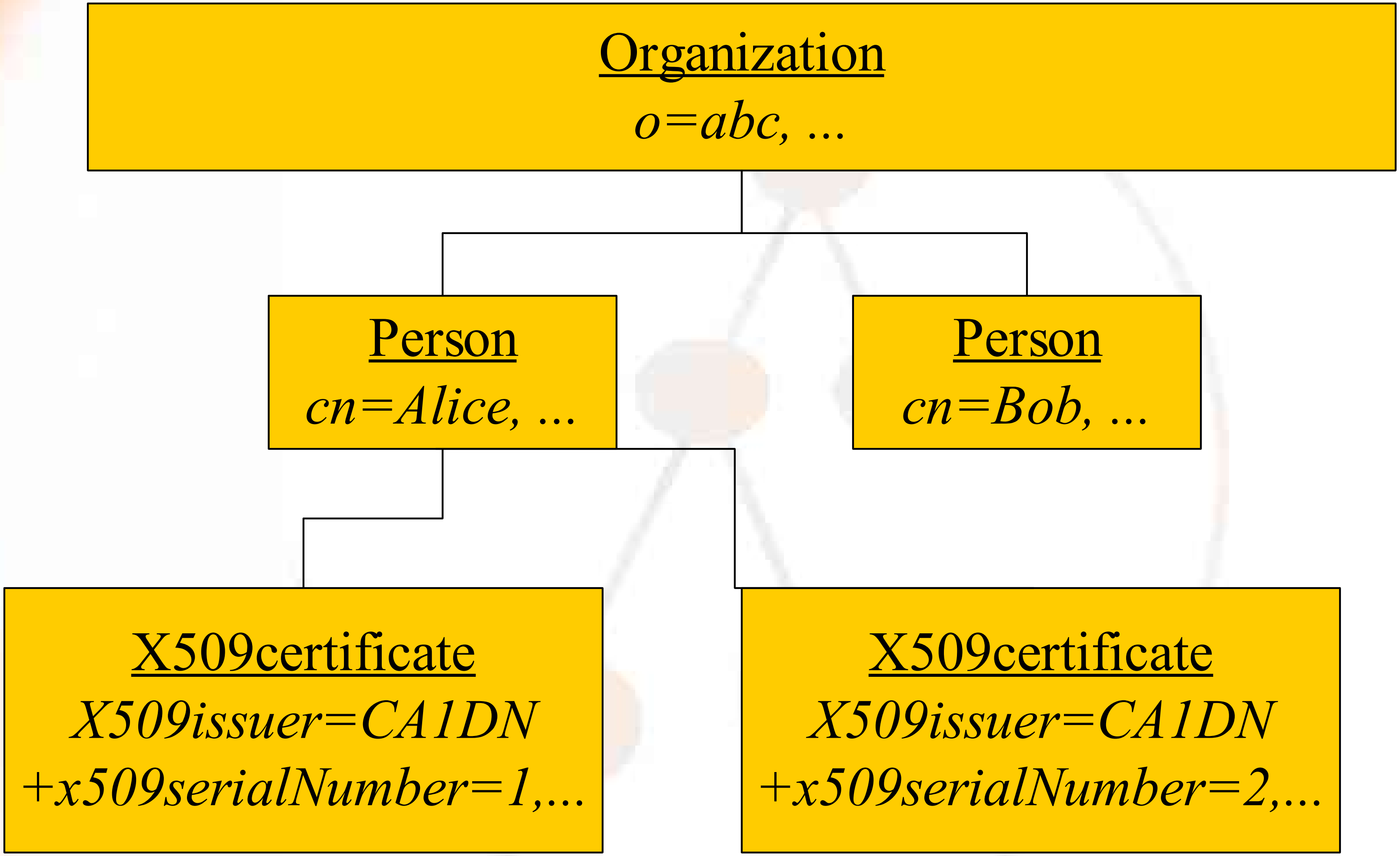
x509subjectKeyIdentifier;
x509keyUsage; x509policyInformationIdentifier;

x509subjectAltNameRfc822Name; x509subjectAltNameDnsName;
x509subjectAltNameDirectoryName; x509subjectAltNameURI;
x509subjectAltNameIpAddress; x509subjectAltNameRegisteredID;
x509isssuerAltNameRfc822Name; etc.

x509extKeyUsage; x509FullcRLDistributionPoint; x509certHolder

DAASI International
Directory Applications for Advanced Security and Information Management

DIT Structure in White Pages directory



Organization

o=abc, ...

Person

cn=Alice, ...

Person

cn=Bob, ...

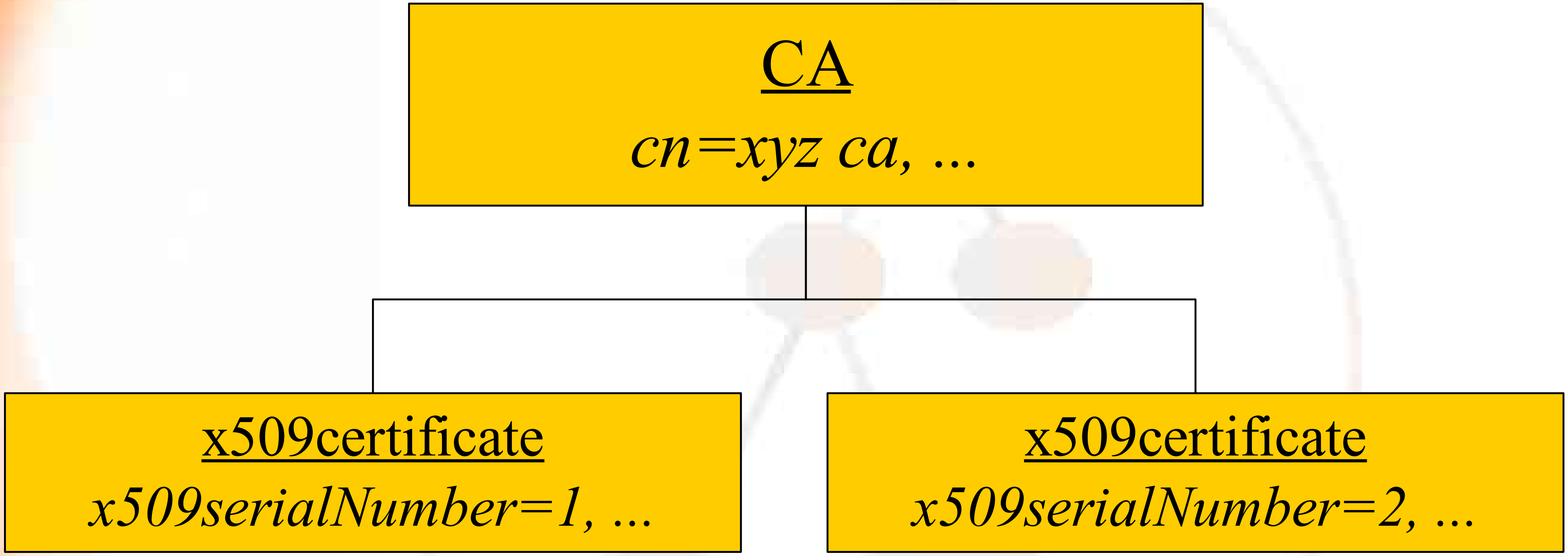
X509certificate

X509issuer=CA1DN +x509serialNumber=1,...

X509certificate

X509issuer=CA1DN +x509serialNumber=2,...

DIT Structure in a certificate only directory



CA

cn=xyz ca, …

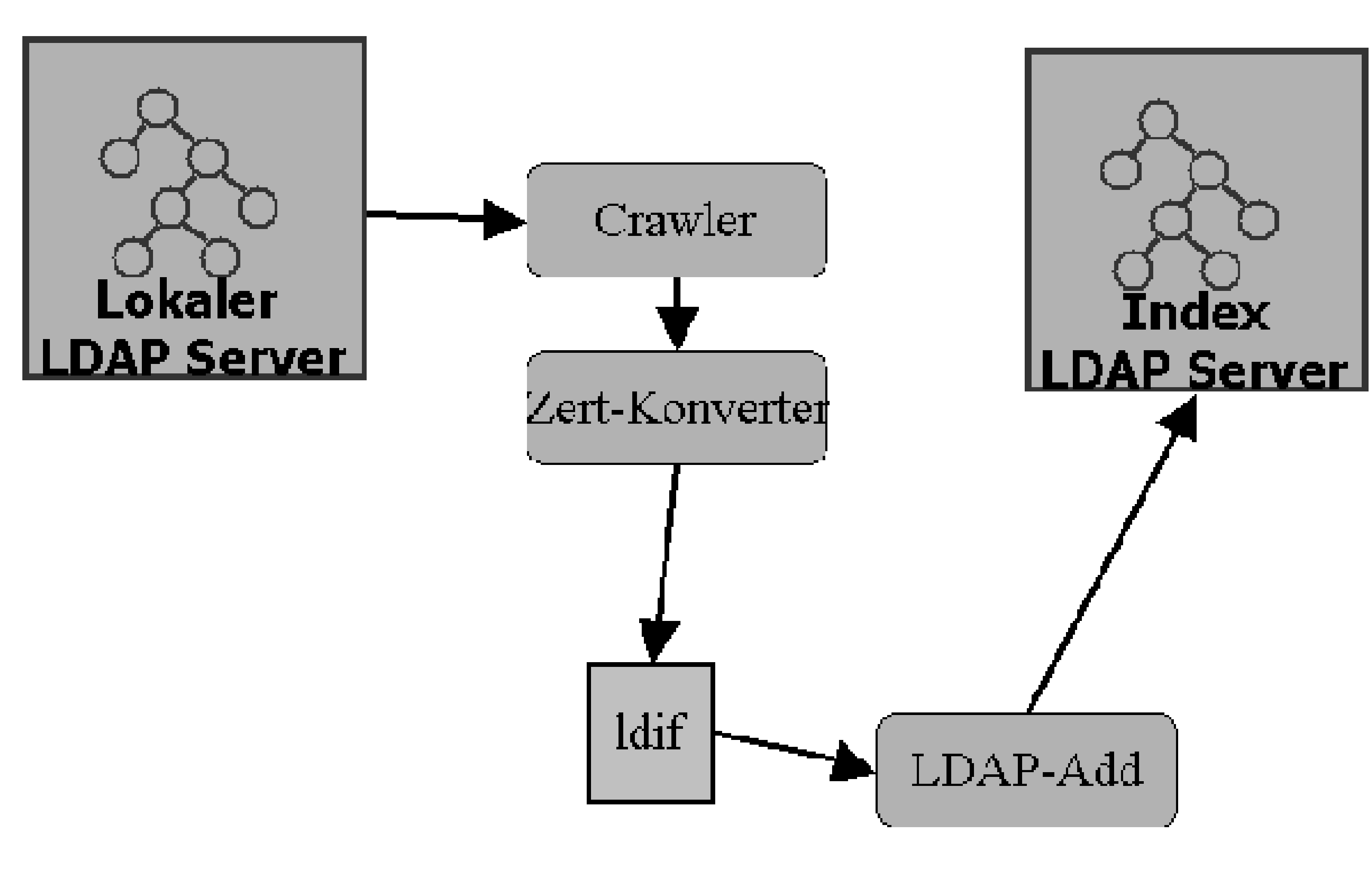
x509certificate

x509serialNumber=1, …

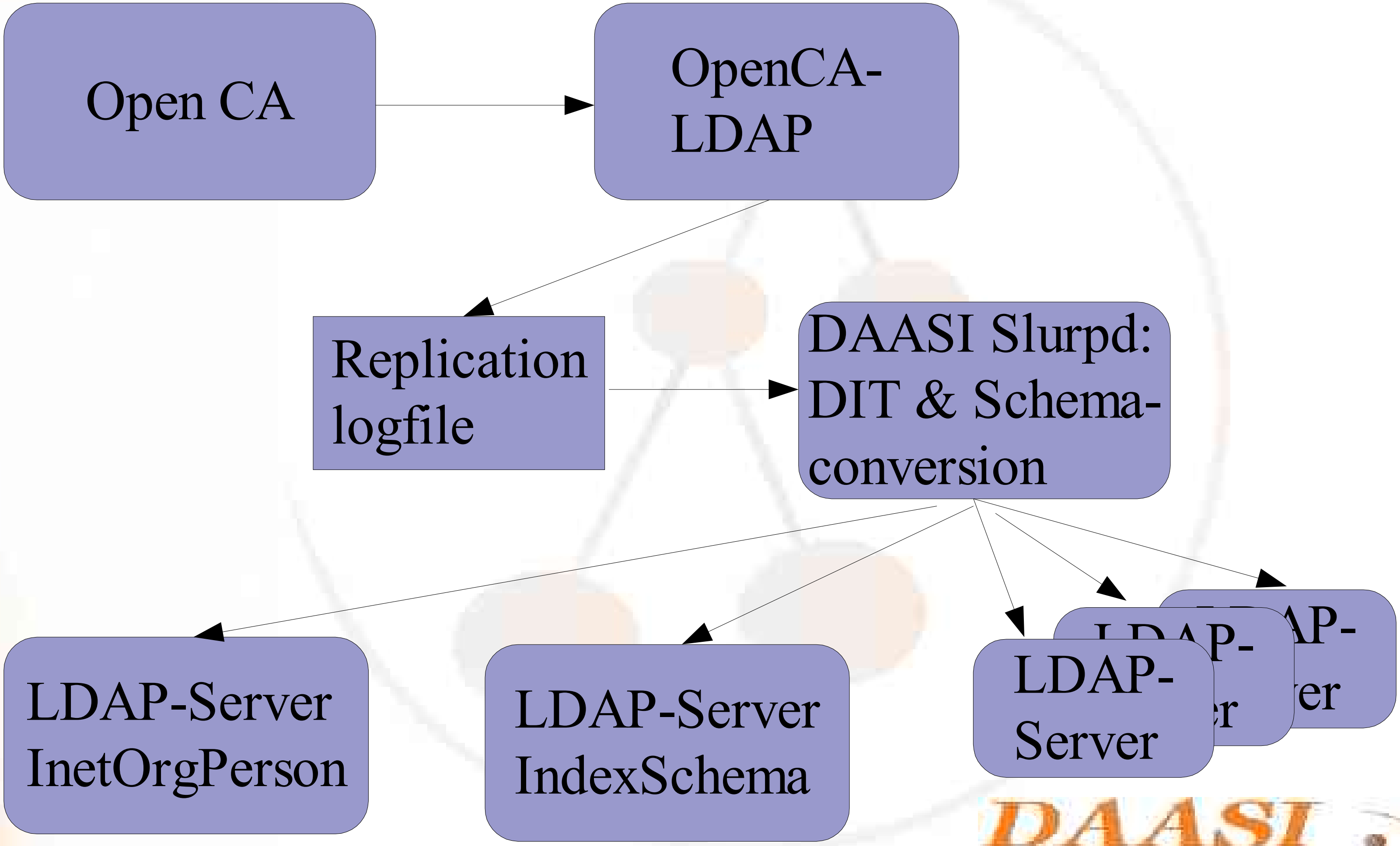
x509certificate

x509serialNumber=2, …

Index integration of local CAs



Integration of OpenCA



Open CA

OpenCA-LDAP

Replication logfile

DAASI Slurpd: DIT & Schema-conversion

LDAP-Server InetOrgPerson

LDAP-Server IndexSchema

AP- er

LDAP- r

LDAP-Server

OpenCA evaluation

- In the frame of the project part „Design and Implementation of user interfaces “
- Work items:
  - Evaluation of the OpenCA software - concludes
    - 0.9.1 does not fullfil all requirements of the universities
    - Concludes 0.9.2 RC 5 is already usefull in production environment
  - Documentation works
    - General Introduction in German
    - Documentation of projektspezific implementation
  - Development
    - Project specific web interface
    - Integration of the new LDAP Schema (certificate metadata)
    - Backup solution for CA keys (wasn't yet there in OpenCA)

Thanks for your attention

- Any questions?

- DAASI International GmbH
  - www.daasi.de
  - Info@daasi.de

DAASI International
Directory Applications
for Advanced Security
and Information Management