# The LDAP Schema Registry and its requirements on Slapd development

OpenLDAP Developers' Day
San Francisco
21 March 2003

Peter Gietz, DAASI International GmbH
Peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management

# AGENDA

- TERENA Project Directory Schema Registry
- What would have made my life easier



DAASI International
Directory Applications for Advanced Security and Information Management

# Project aims

- to set up a LDAP schema registry with
  - an easy browsable and searchable Web interface
  - an LDAP interface for retrieval
  - an interface based on MIME types defined in RFC 2927 for submissions of new schema
- to define a policy defining the standards for inclusion into the registry
- to search for all schema definitions made within the IETF and include them into the registry
- to develop a business model to keep the registry alive after the end of the project.

DAASI International

Directory Applications for Advanced Security and Information Management

# Project Funding body

- TERENA
  - (Trans-European-Research and Education Networkinc Association)
- JISC
  - (Joint Information Systems Committee, UK)
- REDIRIS
  - (Spanish National Research Network)
- CESNET
  - (Czech National Research Network)
- POZMAN SUPERCOMPUTING
  - (Poznan Supercomputing and Networking Center, Poland)
- DAASI International

DAASI International
Directory Applications for Advanced Security and Information Management

# Project Documentation

- Project Proposal
- Deliverable B: Survey of previous work on directory schema registry related technologies and existing LDAP schema, version 0.91
- Deliverable B-2: Bibliography for the Directory Schema Registry Project, version 0.91
- Deliverable D: Definition of an incorporation and usage policy for a Directory Schema Registry, version, version 0.9
- Deliverable C: Definition of a metadata format and DIT structure (coming very soon)
- Deliverable E: Software Spec (coming soon)

DAASI International

Directory Applications for Advanced Security and Information Management

# Work that could be used

- IETF WG schema
  - provided specifications for a schema listing service for the directory technologies LDAP, Whois, Whois++ and Rwhois.
  - The idea was to provide a single point of discovery, to promote reuse, reduce duplication of effort and to promote interoperability.
  - This work is based on a document [RFC 2425] that defines a MIME Content-Type for holding directory information.

DAASI International
Directory Applications for Advanced Security and Information Management

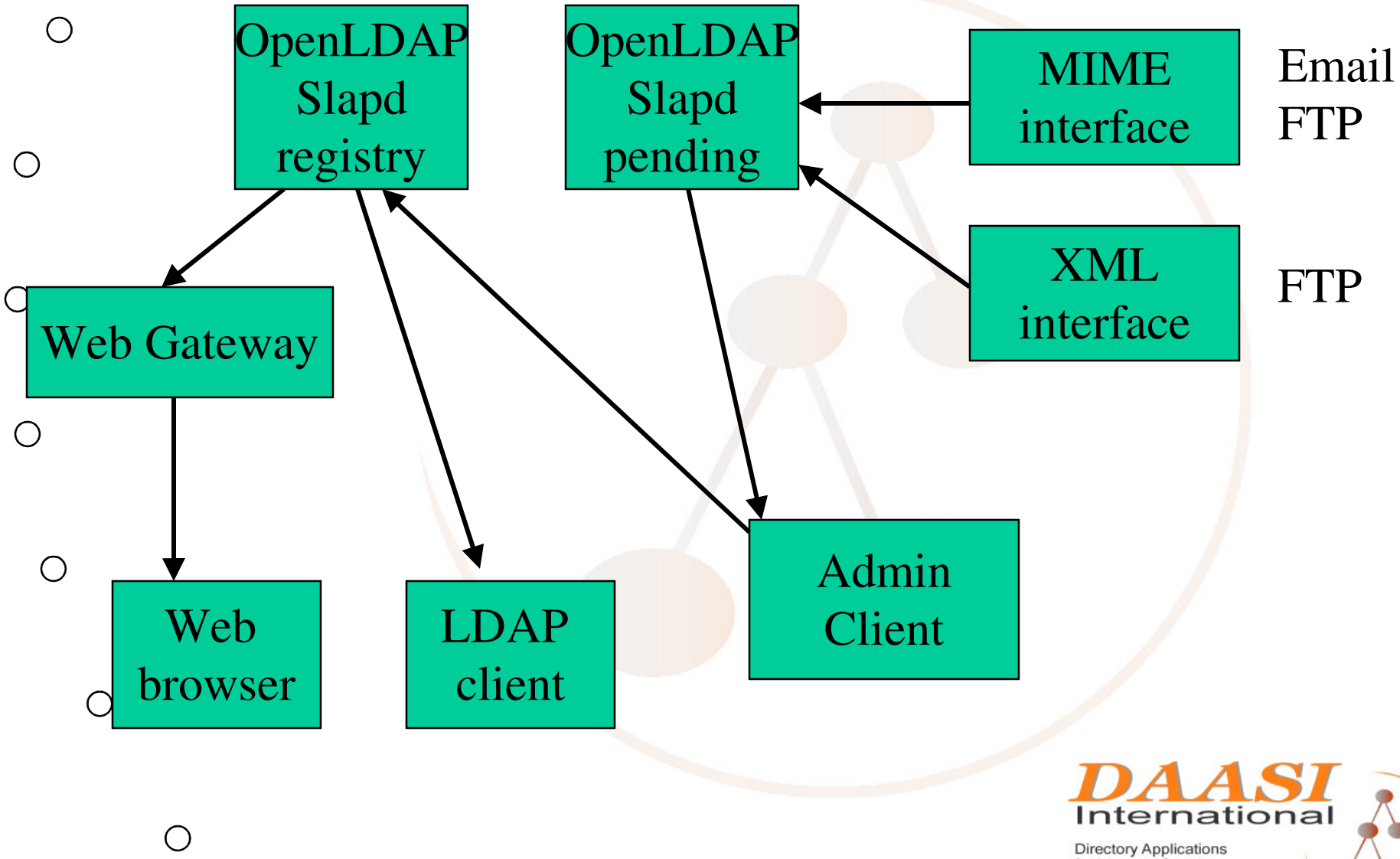
# Schema WG docs

- Apple, C., "Directory Schema Listing File Names", <draft-ietf-schema-file-list-01.txt>, April 1998 (expired), http://www.watersprings.org/pub/id/draft-ietf-schema-file-list-01.txt
- Apple, C., "Directory Schema Listing Meta Data", <draft-ietf-schema-mime-metadata-01.txt>, April 1998, (expired), http://www.watersprings.org/pub/id/draft-ietf-schema-mime-metadata-01.txt
- Apple, C., "Directory Schema Listing Procedures", <draft-ietf-schema-proc-list-01.txt>, April 1998 (expired), http://www.watersprings.org/pub/id/draft-ietf-schema-proc-list-01.txt
- Apple, C., "Requirements for the Initial Release of a Directory Schema Listing Service", <draft-ietf-schema-rqmts-list-01.txt>, April 1998 (expired), http://www.watersprings.org/pub/id/draft-ietf-schema-rqmts-list-01.txt

DAASI International

Directory Applications for Advanced Security and Information Management

# Architecture simplified



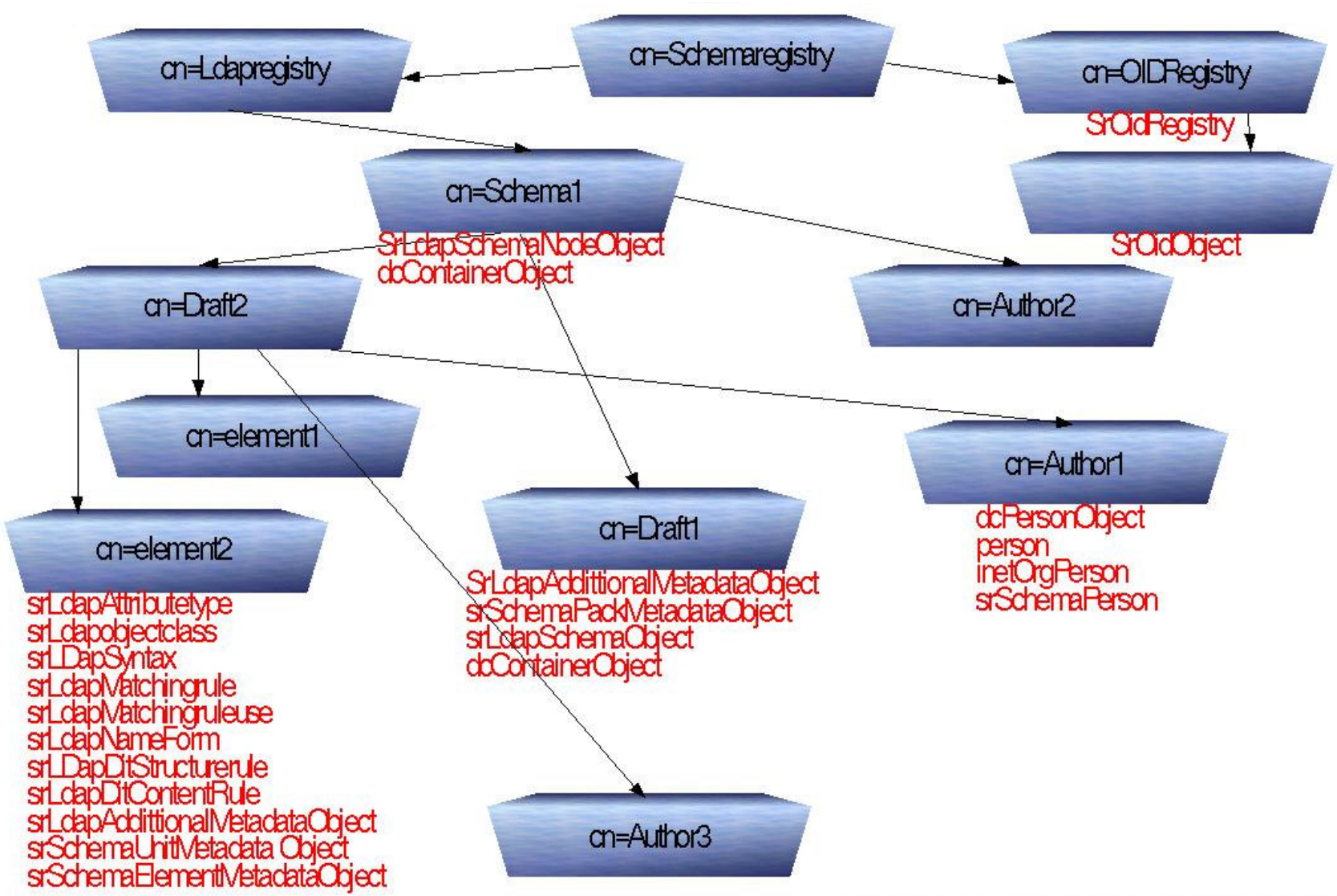

DAASI International
Directory Applications
for Advanced Security
and Information Management

# What info will be stored

- Metadata on specification document
- LDAP compliant definitions of the schema elements
- Single parts of schema element definitions, e.g., MUST attributes in Object Classes
- Metadata as specified by the IETF WG schema
- Separate OID tree
- Additional metadata

DAASI International
Directory Applications for Advanced Security and Information Management

# DIT




Shemaregistry Tree Overview 2003-03-19 BW

# LDAP Schema specified

- Metadata for bibliographical references
  - The Dublin Core Metadata set and its LDAP representation
  - Additional schema for person information
  - The front matter elements of RFC 2629
- Metadata specified by the IETF schema WG
  - MIME types for schema metadata and their LDAP representation (draft-ietf-schema-mime-metadata-01.txt)
  - MIME types for LDAP schema elements and their LDAP representation (RFC 2927)
- Additional schema for the DSR
  - Schema for additional schema elements not specified in RFC 2927
  - Schema for storing an OID tree
  - Schema for storing the single parts of schema element definitions
  - Schema for additional metadata

DAASI International
Directory Applications for Advanced Security and Information Management

# RFC 2629 Frontmatter

```
<?xml version="1.0"?>
<!DOCTYPE rfc SYSTEM
 "rfc2629.dtd">
<rfc>
    <front>
        <title ...>
        <author ...>
        <author ...>
        <date ...>
        <area ...>
        <workgroup ...>
        <keyword ...>
        <keyword ...>
        <abstract ...>
        <note ...>
    </front>
    ...
</rfc>
```

DAASI International
Directory Applications for Advanced Security and Information Management

# Requirements on Slapd

- The schema defined needs not to be standardized. This might be the only application
- None-the-less it would be very neat to have tags and operational attributes be flexible deployable in Slapd

DAASI International
Directory Applications for Advanced Security and Information Management

# Example for Dublin Core

- **DC.Relation**
- "A reference to a related resource".

```
attributetype ( 1.3.6.1.4.1.10126.1.7.3.16
    NAME 'dcRelation'
    DESC 'A reference to a related resource'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

- For specification documents 5 relation types make sence: "obsoletes", "obsoleted-by", "updates", "updated-by", and "inherits
- Ideally, the DSR will use the LDAP attribute description tagging option method for storing these tags. Since tags other than the language tags specified in [RFC 2596]. are not implemented in the LDAP-Server used by the DSR (OpenLDAP), it will either have to be implemented by the project, or an alternative method will be used, namely by specifying subtypes of the attribute dcRelation:

```
attributetype ( 1.3.6.1.4.1.10126.1.7.3.17
    NAME 'dcObsoletes'
    SUP dcRelation`
```

DAASI International
Directory Applications for Advanced Security and Information Management

# name descriptor options

- name descriptor options (;binary and ;lang-*) are hard coded in OpenLDAP
- Since this tagging can be very interesting e.g. in the frame of LDAP and Dublin Core, a generalized way of handling such tags would be very handy
- How about a config file for specifying tags?
- the server does not necessarily have to know the semantics of such tags.

DAASI International
Directory Applications for Advanced Security and Information Management

# Example additional Metadata

- **syntax ok**
- In the DSR automatic Syntax checks will be performed. In the following attribute the result of this check will be stored:

```
attributetype ( 1.3.6.1.4.1.10126.1.14.3.2
    NAME 'srSyntaxOK'
    DESC 'the syntaxcheck was successfull'
    EQUALITY booleanMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
    SINGLE-VALUE )
```

- It would be nice to have this as an operational Attribute

DAASI International
Directory Applications for Advanced Security and Information Management

# Operational Attributes

- In OpenLDAP it is impossibility to add operational attributes via schema file.
- I know that most operational attributes would have special semantics that the server has to know.
- But imagine there are also some that would only have to be known by the client.
- the feature to add RootDSE attributes by a special LDIF file didn't work because of not allowing self defined operational attributes.
- I wrote a work around patch, but no real solution to this problem.

DAASI International
Directory Applications for Advanced Security and Information Management

# Schema Configuration via LDAP

- Once the LDAP Schema Registry is running, instead of using .schema files in OpenLDAP, the schema configuration could be retrieved via LDAP from the registry

# Questions?

- Thank you for your attention
- More information at:
  - http://www.daasi.de/services/SchemaReg
  - Info@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management