Metadirectory und Personenschemata - Nationale und internationale Entwicklungen

ZKI Workshop:
Meta-Directory und Identity Management,
an der Fachhochschule Köln, 10.7.2003

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

DAASI International
Directory Applications for Advanced Security and Information Management

AGENDA

- Metadirectory und Personenschema
- Standardisierte Personenschemata
- Neue internationale Entwicklungen
- Personenschemata und Directory Schema Registry
- Projektvorschlag Metadirectory

DAASI International

Directory Applications for Advanced Security and Information Management

DAASI International GmbH

- Directory Applications for Advanced Security and Information Management
- Nachfolgeinstitution der DFN-Forschungsprojekte zu Verzeichnisdiensten
  - eigentlich gegründet zum Betrieb der in den Projekten entwickelten Dienste
- Offizielles Spin-Off der Universität Tübingen
- International tätig
- Forschung ist wichtiger Bestandteil des Konzeptes
- Hauptzielgruppen:
  - Deutsche Forschungseinrichtungen
  - Behörden auf allen Ebenen
  - Gesundheitswesen

DAASI International

Directory Applications for Advanced Security and Information Management

Standardisierte Personenschemata

DAASI International

Directory Applications
for Advanced Security
and Information Management

Metadirectory und Personenschema

- Konzept Metadirectory verwendet einen Verzeichnisdienst zur Synchronisierung von Datenbeständen aus verschiedenen Datenbankquellen
- Vorraussetzung ist, dass alle zu synchronisierenden Daten im Verzeichnisdienst abbildbar sind
- Das entsprechende Schema muss standardisiert sein, damit verschiedene Anwendungen darauf zugreifen können
- Internationale Standards sollten mindestens den Ausgangspunkt bilden

Personenschema im X.500 Standard

- X.500 wurde in der Version 1 1988 als weltweiter Verzeichnisdienst spezifiziert
- Erste Anwendung war internationales Telefonbuch (White-Pages und Yellow Pages)
- Deshalb wurde im Standard selbst bereits Schema u.a. zur Abbildung von Personen spezifiziert
- Diese Standard-Schemaspezifikationen wurden in LDAP übernommen (RFC 2256)

LDAPv3 Personenschema

Objektklasse person:

(2.5.6.6 NAME 'person' SUP top STRUCTURAL
MUST (sn $ cn)
MAY (userPassword $ telephoneNumber $ seeAlso $ description))

Objektklasse organizationalPerson:

(2.5.6.7 NAME 'organizationalPerson' SUP person STRUCTURAL
MAY (title $ x121Address $ registeredAddress $ destinationIndicator $
preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
telephoneNumber $ internationaliSDNNumber $
facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l))

Probleme mit organizationalPerson

- Attributtyp title ist nur für Firmenfunktion gedacht
  - „title, such as "Vice President", of a person in their organizational context“
- personalTitle ist zwar in RFC 1274 spezifiziert aber nicht ins LDAP-Schema übernommen
- Zur vollständigen Abbildung der postalischen Adresse in Einzelattributen fehlt Attributtyp countryName / c
- Internettypische Attribute fehlen ganz

Objektklasse inetOrgPerson (RFC 2798)

(2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson'
SUP organizationalPerson STRUCTURAL
MAY (audio $ businessCategory $ carLicense $ departmentNumber
displayName $ employeeNumber $ employeeType $ givenName $
homePhone $ homePostalAddress $ initials $ jpegPhoto $
labeledURI $ mail $ manager $ mobile $ o $ pager $
photo $ roomNumber $ secretary $ uid $ userCertificate $
x500uniqueIdentifier $ preferredLanguage $
userSMIMECertificate $ userPKCS12))

- inetOrgPerson ist anerkannter Standard und wird von allen entsprechenden Anwendungen genutzt
- Problem: Es fehlen Spezialattribute für Forschungs-Personen

DAASI International
Directory Applications for Advanced Security and Information Management

Neuere Entwicklungen

DAASI International

Directory Applications
for Advanced Security
and Information Management

Objektklasse eduPerson 1.5

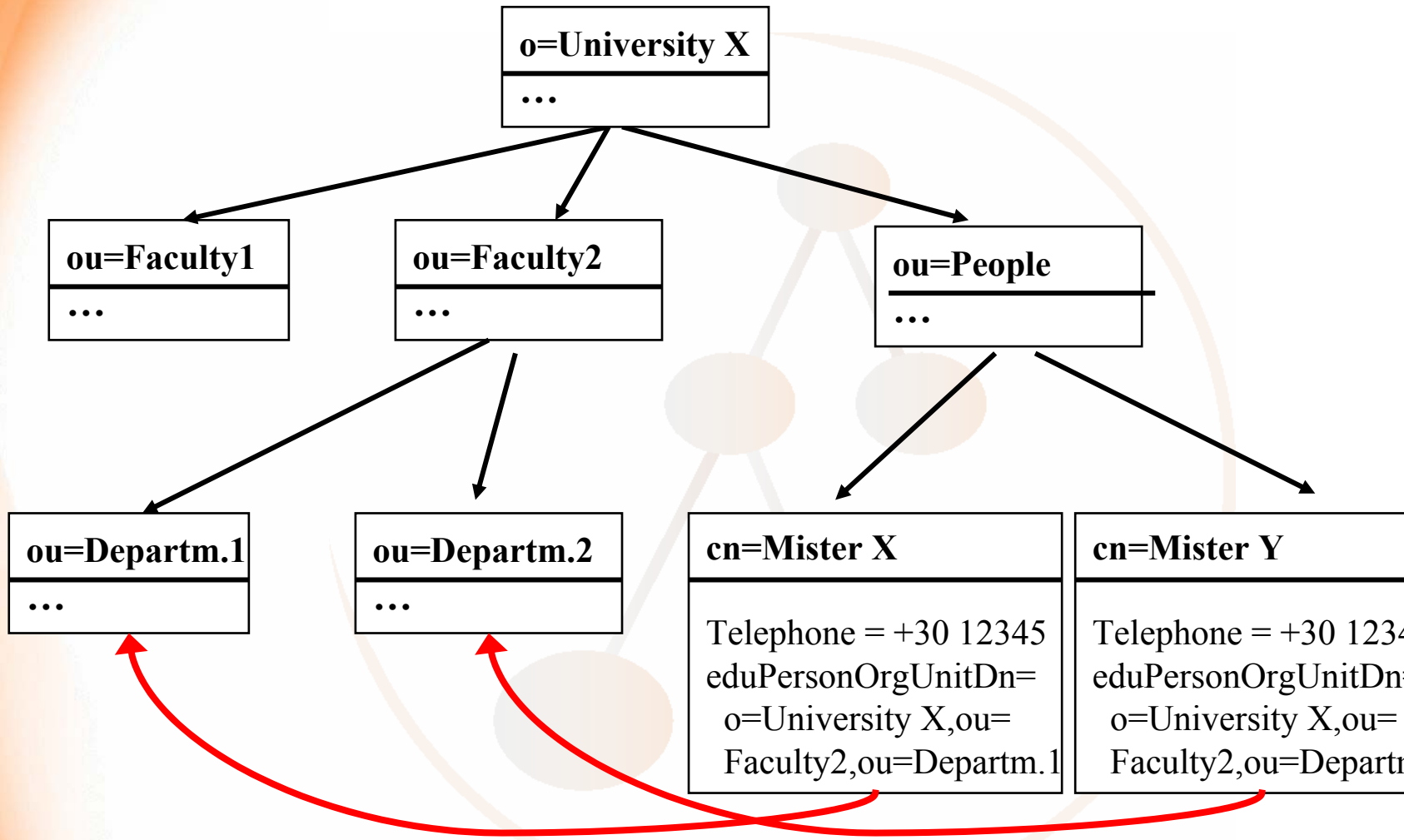
- Von Internet2 MACE Dir entwickelt
- Als Ergänzung zu inetOrgPerson gedacht

```
( 1.3.6.1.4.1.5923.1.1.2 NAME 'eduPerson'
        AUXILIARY
        MAY ( eduPersonAffiliation $ eduPersonNickname $
                eduPersonOrgDN $ eduPersonOrgUnitDN $
                eduPersonPrimaryAffiliation $
                eduPersonPrincipalName $
                eduPersonEntitlement $
                eduPersonPrimaryOrgUnitDN )
```

Diskussion über eduPerson

- Attributtypen z.T. USA-lastig spezifiziert
  - Kontrolliertes Vokabular für eduPerson(Primary)Affiliation:
    - faculty, student, staff, alum, member, affiliate, employee
- eduPersonPrincipalName ist als Identitäts-Token gedacht:
  - „The "NetID" of the person for the purposes of inter-institutional authentication“
- eduPersonEntitlement zur Abbildung von Rechten:
  - „URI (either URN or URL) that indicates a set of rights to specific resources“
- eduPersonOrgDN/eduPerson(Primary)OrgUnitDN zur Abbildung der Organisationszugehörigkeit bei einem flachen Personenbaum

eduPersonOrgUnitDn



DAASI International

Directory Applications for Advanced Security and Information Management

Objektklasse dfnOrgPerson

- Wurde im Rahmen des DFN-Forschungsprojekts entwickelt
- Nicht als deutscher Standard gedacht, sondern für den Dienst AMBIX entwickelt
- Datenschutzrechtliche Attribute könnten für andere interessant sein

```
( 1.3.6.1.4.1.5062.1.1.4.1
      NAME 'dfnOrgPerson'
      DESC 'inetOrgPerson augmented with dfn attributes'
      SUP  inetOrgPerson
      STRUCTURAL
      MUST ( dfnOptInStatus $ dfnDistribution $
         dfnOriginalSource $ dfnMaintainedBy )
      MAY  ( personalTitle $ dfnEndOfObjectionPeriod $
         dfnContactHistory $ dfnOrgPersonAffiliation $
         dfnOrgPersonPrimaryAffiliation ) )
```

DAASI International

Directory Applications for Advanced Security and Information Management

TERENA Projekt DEEP

- TERENA: Europäische Vereinigung der Nationalen Forschungsnetze
- Projekt DEEP
  - Development of an European EduPerson
  - Idee: über eduPerson hinausgehende Bedürfnisse in europäischen Hochschulen zu ermitteln
  - Bedarfsanalyse via Webfrageboden
  - Wurde von DAASI durchgeführt
  - http://www.daasi.de/projects/DEEP

DAASI International

Directory Applications for Advanced Security and Information Management

DEEP Ergebnisse

- 18 Organisationen aus 12 Ländern haben den ca. 10 seitigen Fragebogen ausgefüllt.
- Die Fragen waren unterteilt in:

1. Contact Data
2. General questions on the topic
3. Current and future directory deployment
4. Relevance of person attributes: Objectclasses person, organizationalPerson, inetOrgPerson, eduPerson 1.5.
5. Relevance of organizational attributes: Objectclasses organization, organizationalUnit, Objectclass eduOrg
6. Desired schema extensions
7. Desired new attributesgeneral

DEEP Ergebnisse - 2

- 88% hielten Interoperabilität zwischen Organisationen für wesentlich
- Nur 12% fanden eduPerson ausreichend
- Alle sahen Bedarf an Attributen zur Wahrung des Datenschutzes
- LDAP wichtigste Verzeichnisdiensttechnologie, OpenLDAP wichtigste Implementierung
- Wichtigste Anwendungen: White Pages (82%), Authentication service (71%), Email user management (65%) and User login management (53%)

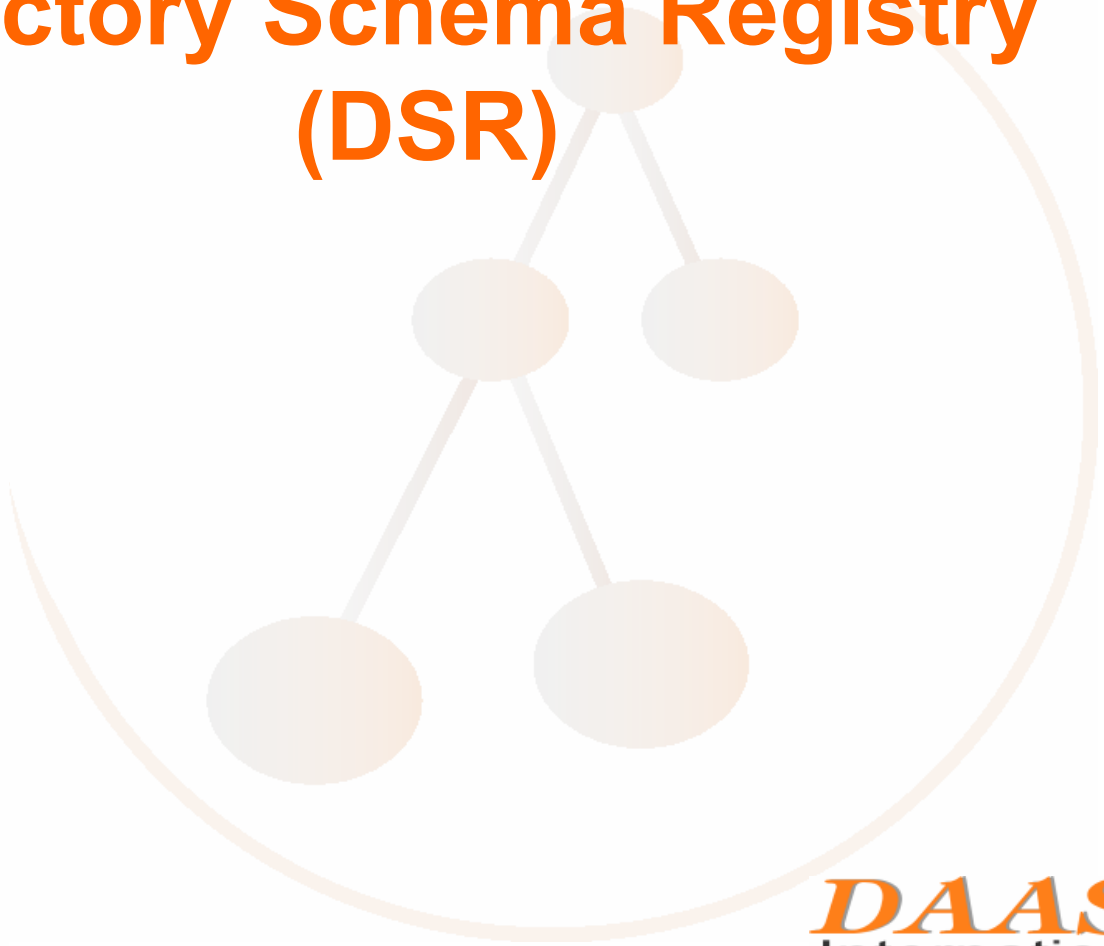
DEEP Ergebnisse - 3

- Als relevante Attribute wurden angesehen:
  - Alle Attribute der Objektklasse person
  - 7 der 17 Attribute von organizationalPerson
  - 16 der 28 Attribute von inetOrgPerson
  - 6 der 8 Attribute von eduPerson
- Folgende Attribute wurden in den Standards vermisst:
  - socialSecurityNumber, personalTitle, areaOfInterest, unique_userid, birthdate, cv, studentnumber, classificationScheme, user_class, gender, fedID or netID, expertice, position, releasePolicy, studyBranch, expirationdate, indexingPolicy, accountstatus

Reaktionen auf DEEP

- Internet2 haben DEEP intensiv beobachtet und haben Interesse an Mitarbeit zu internationalEduPerson gezeigt
- Im Rahmen von TERENA hat sich eine Arbeitsgruppe entwickelt, die europäischen Standard entwickeln will
- In einigen Ländern gibt es nationale Initiativen, die z.T. von DEEP beeinflusst wurden
- Verschiedene Schemata werden nicht alle als IETF-RFC standardisiert
- Alternative ist eine Registry

TERENA Projekt
Directory Schema Registry (DSR)



DAASI International

Directory Applications
for Advanced Security
and Information Management

Motivation for DSR

- Common schema (attributes and object classes) are vital for directory interoperability
- There are a lot of standards allready out there, people may not know about
- There are even more good schema proposals not (yet) standardized
- People still tend to reinvent he wheel
- You can find information on the web but at different places
- Applications cannot retrieve schema information via LDAP

DSR 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

DSR 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

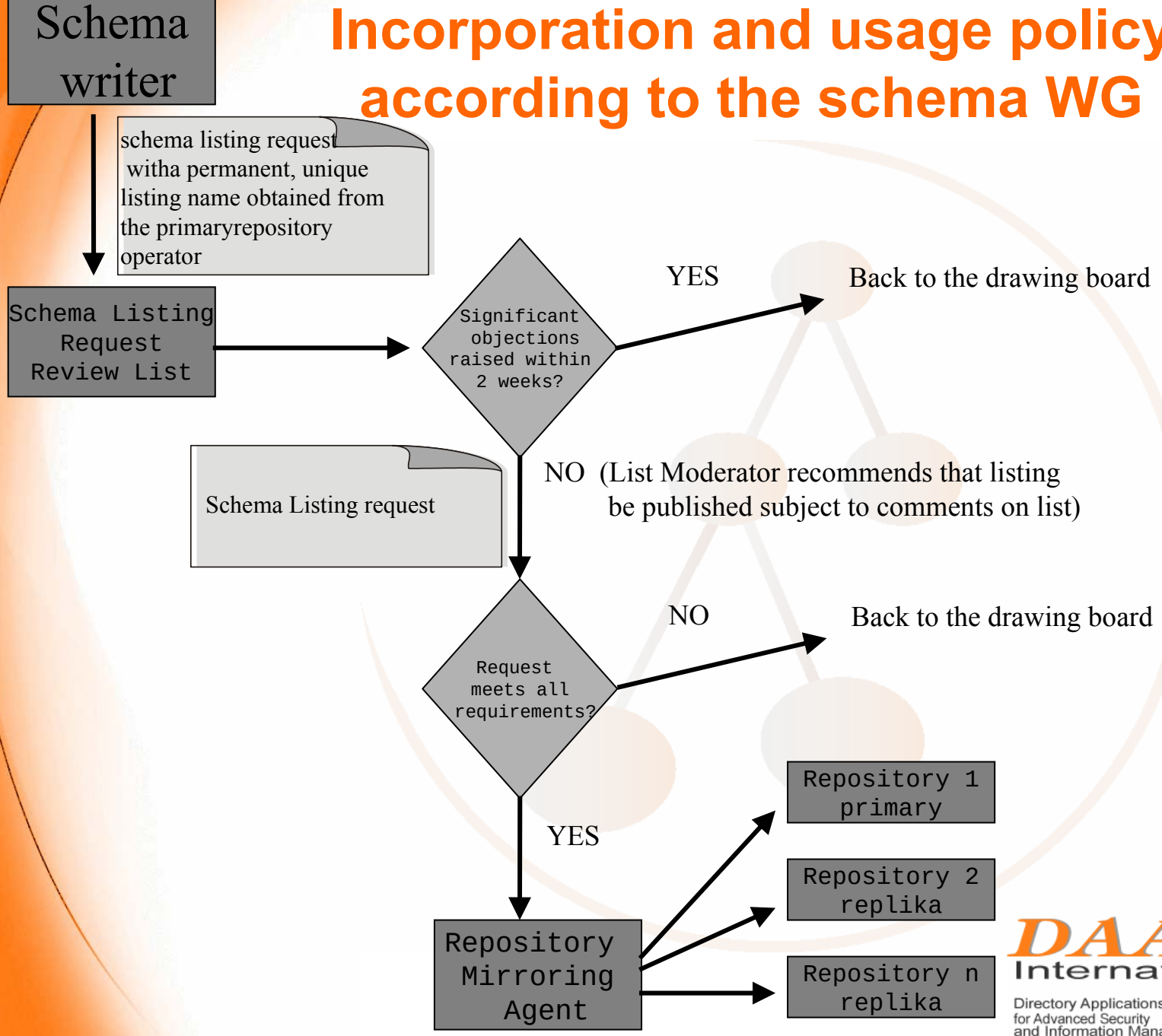
DAASI International

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, version 0.9
- Deliverable E: Software Spec

Incorporation and usage policy according to the schema WG



DAASI International
Directory Applications for Advanced Security and Information Management

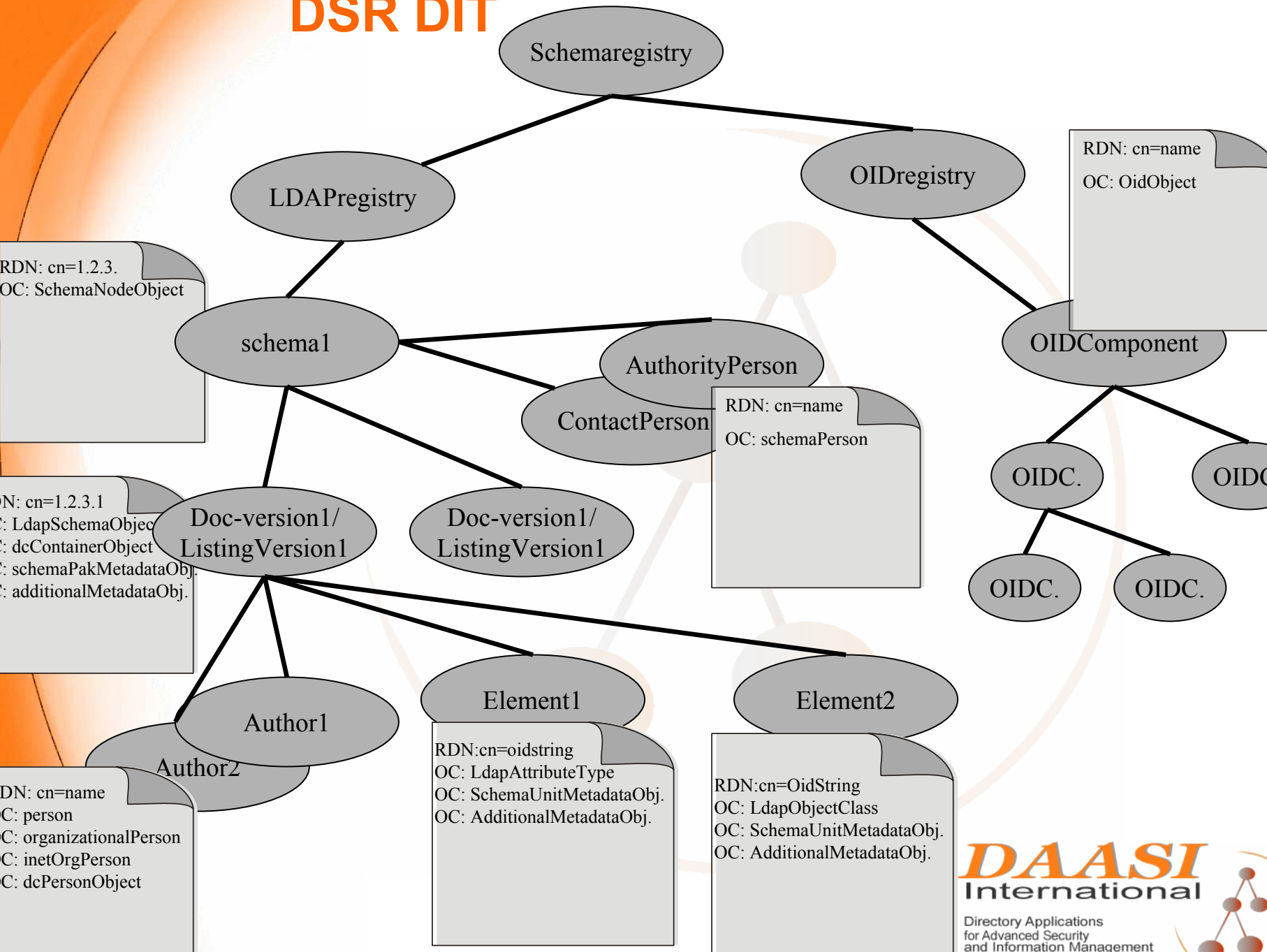
What info will be stored

- 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

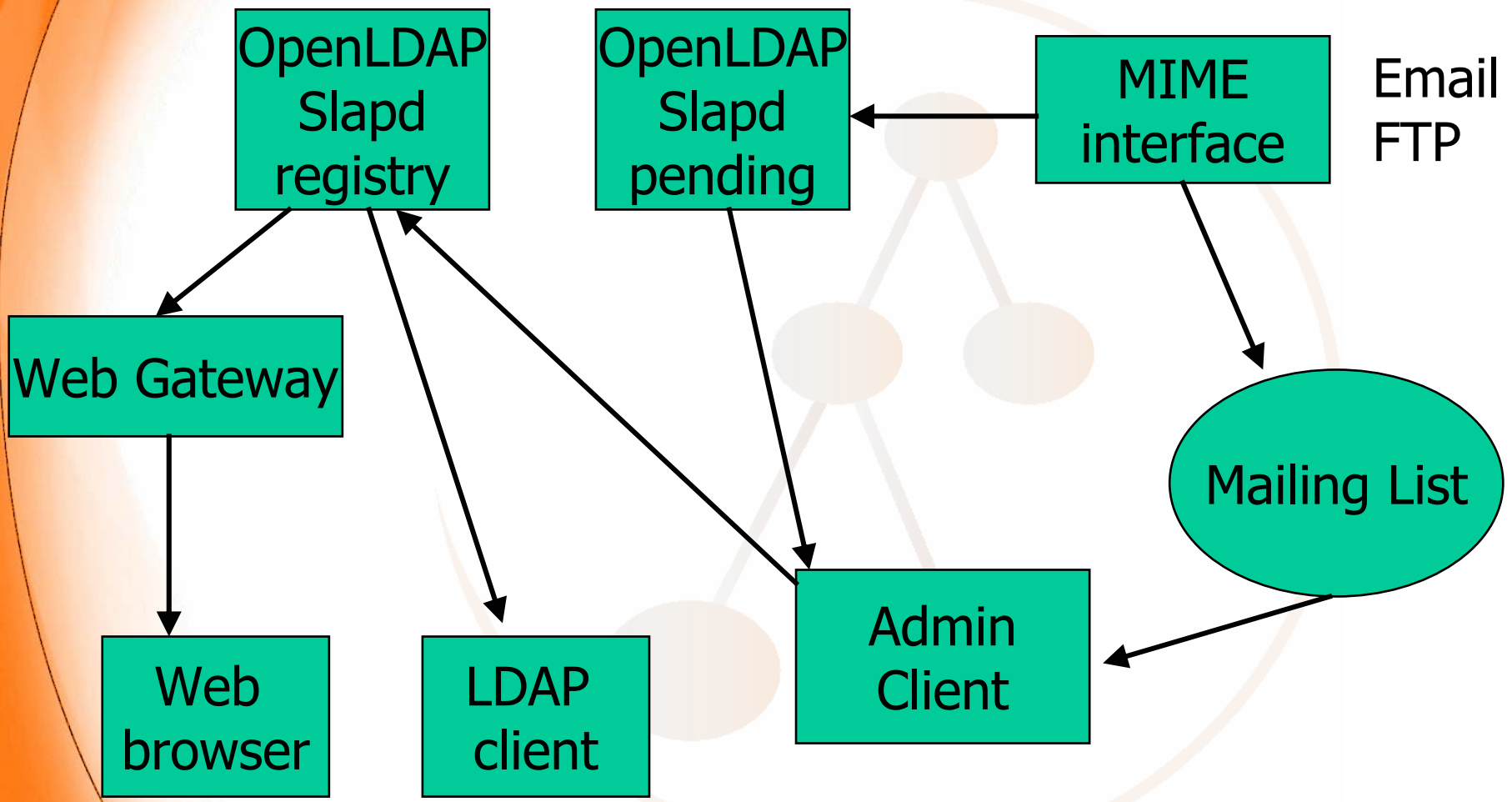
DSR DIT



DAASI International

Directory Applications for Advanced Security and Information Management

DSR Workflow



DAASI International

Directory Applications for Advanced Security and Information Management

Projektvorschlag Metadirectory

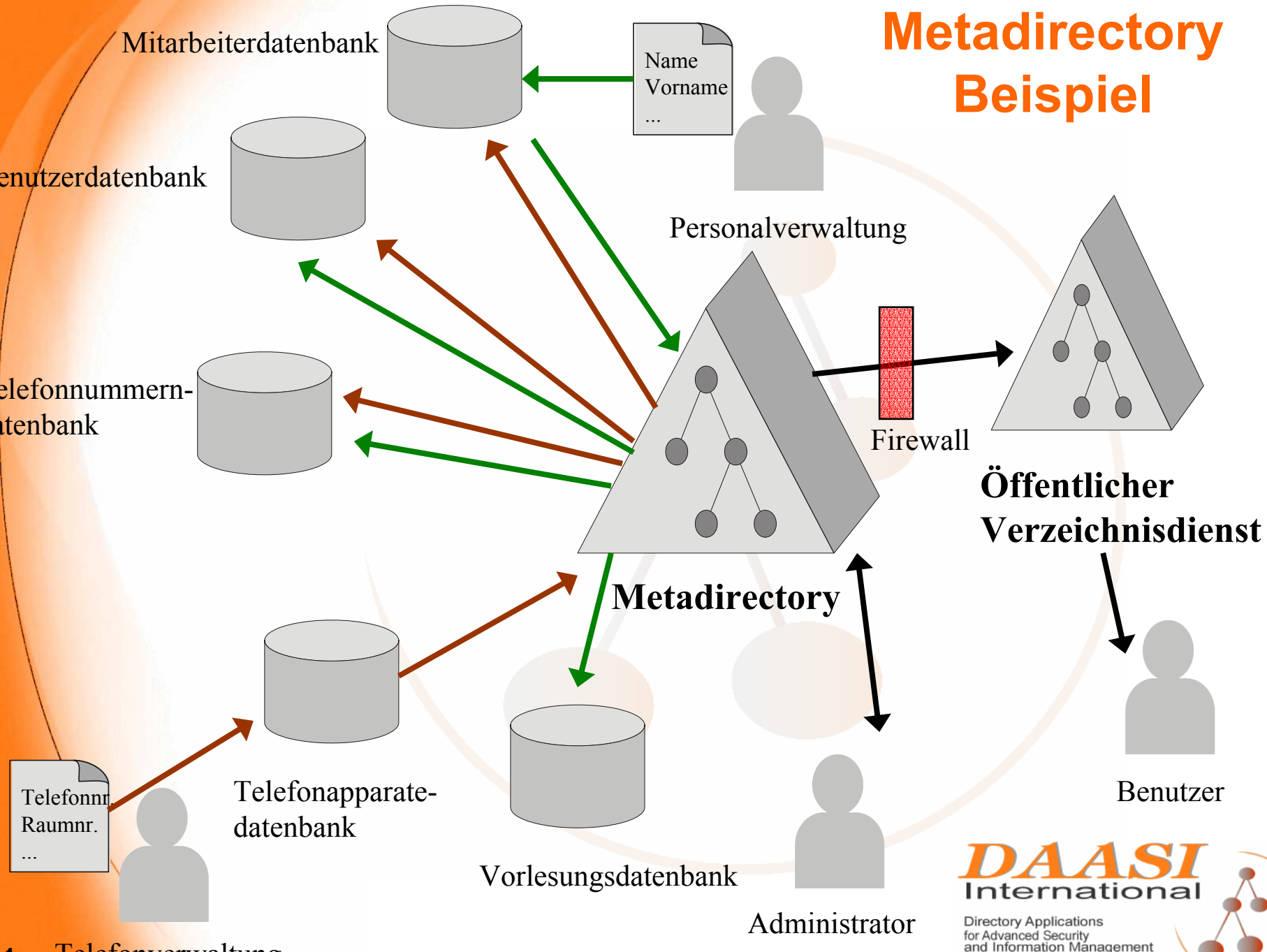
DAASI International

Directory Applications
for Advanced Security
and Information Management

Metadirectory

- Verknüpfung verschiedener Datenbanken, die verwandte Daten enthalten, z.B.:
  - Emailbenutzerdatenbank
  - Personaldatenbank
  - Telefondatenbank
- Die gleichen Daten müssen nur einmal eingegeben, bzw. gepflegt werden
- In den verknüpften Datenbanken werden sie automatisch angelegt bzw. geändert
- Eine übergreifende Sicht auf alle Daten
- Prozesse sind flexibel an Organisationsabläufe anpassbar

Metadirectory Beispiel



DAASI International

Directory Applications for Advanced Security and Information Management

Metadirectory Implementierungen

- Verschiedene Implementierungen (alphabet. Ordnung)
  - IBM Tivoli Identity Manager
  - Microsoft Metadirectory Service
  - Novell DirXML
  - Siemens DirX Metahub
  - SUN One Directory Server Metadirectory Lösung
- OpenLDAP kann Grundlage für eine OpenSource-Lösung sein
- Bei allen Lösungen fehlen hochschulspezifische Konnektoren

Metadirectory-Projektidee

- Erhebung der spezifischen Hochschulanforderungen
- Erstellung von allgemeinen Richtlinien zum Aufbau von Metadirectories
  - Anpassung an Organisationsprozesse
  - Datenstrukturen
  - gemeinsames Datenschema
    - Auch für Interdomain-Authentifizierung wichtig
- Herstellerunabhängige Evaluation verschiedener kommerzieller Produkte
- Entwicklung von Konnektoren für OpenLDAP
- Erstellung von Implementierungsspezifischen „Kochbüchern“

DAASI International

Directory Applications for Advanced Security and Information Management

Metadirectory Initiative

- Verschiedene Hochschulen haben sich mit Metadirectories beschäftigt
- Andere sehen Bedarf an Metadirectories
- Gemeinsames Projekt wäre für alle vorteilhaft
  - Kostenminimierung
  - Erfahrungsaustausch
  - Einfache lokale Implementierung

DAASI International

Directory Applications
for Advanced Security
and Information Management

Referenzen

- RFC 1274: Barker, P., Kille, S.: The COSINE and Internet X.500 Schema, November 1991
- RFC 2256: Wahl, Mark: A Summary of the X.500(96) User Schema for use with LDAPv3, December 1997
- RFC 2798: Smith, M.: Definition of the inetOrgPerson LDAP Object Class, April 2000
- MACE Dir: http://middleware.internet2.edu/dir/

Vielen Dank für Ihre Aufmerksamkeit

- DAASI International GmbH
  - http://www.daasi.de
  - Info@daasi.de

- DEEP: http://www.daasi.de/projects/DEEP
- DSR: http://www.daasi.de/services/SchemaReg

- DFN Directory Services
  - http://www.directory.dfn.de
  - Info@directory.dfn.de

DAASI International

Directory Applications
for Advanced Security
and Information Management