- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit

Verzeichnisdienste für Hochschulen auf Open Source Grundlage

Workshop
Informations- und Verzeichnisdienste in Hochschulen,
Heinrich-Heine-Universität Düsseldorf, 11.10.2002

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

DAASI International
Directory Applications for Advanced Security and Information Management

Agenda (1/3)

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit

- Einführung in LDAP
  - Informationsmodell
  - Funktionsmodell
  - Open Source Implementierung OpenLDAP
- Anwendungen
  - Klassische Anwendungen: Kontaktinformationsdienst, Authentifizierung
  - Metadirectory
  - Indexsystem
  - LDAP und PKI
  - LDAP im Bereich Digital Libraries
  - LDAP und Grid Computing
  - LDAP und Policy Daten

DAASI International
Directory Applications for Advanced Security and Information Management

Agenda (2/3)

- Einführung in LDAP
- Anwendungen
- Internat. For-schungsumfeld
- DFN Umfeld
- DAASI International
- Universitäts-projekte
- Fazit

- LDAP im internationalen Forschungsumfeld
  - TERENA Projekte
    - TF-LSD
    - DEEP
    - Schema Registry
  - Nordunet Projekt NEEDS
  - Verzeichnisdienstaktivitäten im Rahmen von Internet2

DAASI International
Directory Applications for Advanced Security and Information Management

Agenda (3/3)

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit

- LDAP im DFN Umfeld
  - AMBIX
  - PKI Verzeichnisdienst
  - LDAP basierte Authentifizierung
  - DFD Directory Services
- DAASI International GmbH
- LDAP-Projekte an deutschen Universitäten
  - Universität Tübingen
  - Universität Münster
- Fazit

DAASI International
Directory Applications for Advanced Security and Information Management

DAASI International GmbH

- Seit 1994 Verzeichnisdienstbezogene DFN Projekte mit Förderung durch BMBF (s.u.)
- Wegen Aufbau und Betrieb von Diensten, die nicht durch Forschungsmittel Förderungsfähig sind musste neue Organisationsform gefunden werden
- Januar 2001 wurde deshalb die DAASI International GmbH gegründet
  - Directory Applications for Advanced Security and Information Management
  - Forschung ist wichtiger Bestandteil des Konzeptes
  - Langsam und kontinuierlich wachsen
  - Jetzt Insges. 8 Mitarbeiter

DAASI International
Directory Applications for Advanced Security and Information Management

Was ist ein Verzeichnisdienst?

- *Informationen in einem hierarchischen System, z.B.:*
  - Dateiverzeichnis im Betriebssystem (MS/DOS, Unix)
  - Domain Name Service (DNS)
  - Network Information System (NIS)
  - X.500 – *das* Verzeichnis
  - Lightweight Directory Access Protocol (LDAP)
  - Novell Directory Service (NDS)
  - Microsoft Active Directory (AD)

DAASI International
Directory Applications for Advanced Security and Information Management

Konzept von X.500/LDAP

- **Eine Datenbank**
  - Hierarchische Datenstruktur
  - Optimiert für schnelles lesen
  - Einfache Updatemechanismen – keine Transaktionen
- **Netzwerkprotokoll**
  - Verteilung der Daten im Netz
  - Spiegelung der Daten im Netz

DAASI International
Directory Applications for Advanced Security and Information Management

Was kann gespeichert werden?

- Alphanumerische Daten
  - Namen, Adressen, Beschreibungen, Zahlen, etc.
- Zeiger auf andere Daten
  - Innerhalb des Datenbaums, Zeiger auf externe Daten, URI, Dateinamen
- Zertifikate im Rahmen einer PKI
- Andere Binärdaten
  - Grafiken, Photos, Diagramme, ...
- Offenes Modell für beliebige Daten

DAASI International
Directory Applications for Advanced Security and Information Management

Directory Information Tree (DIT)

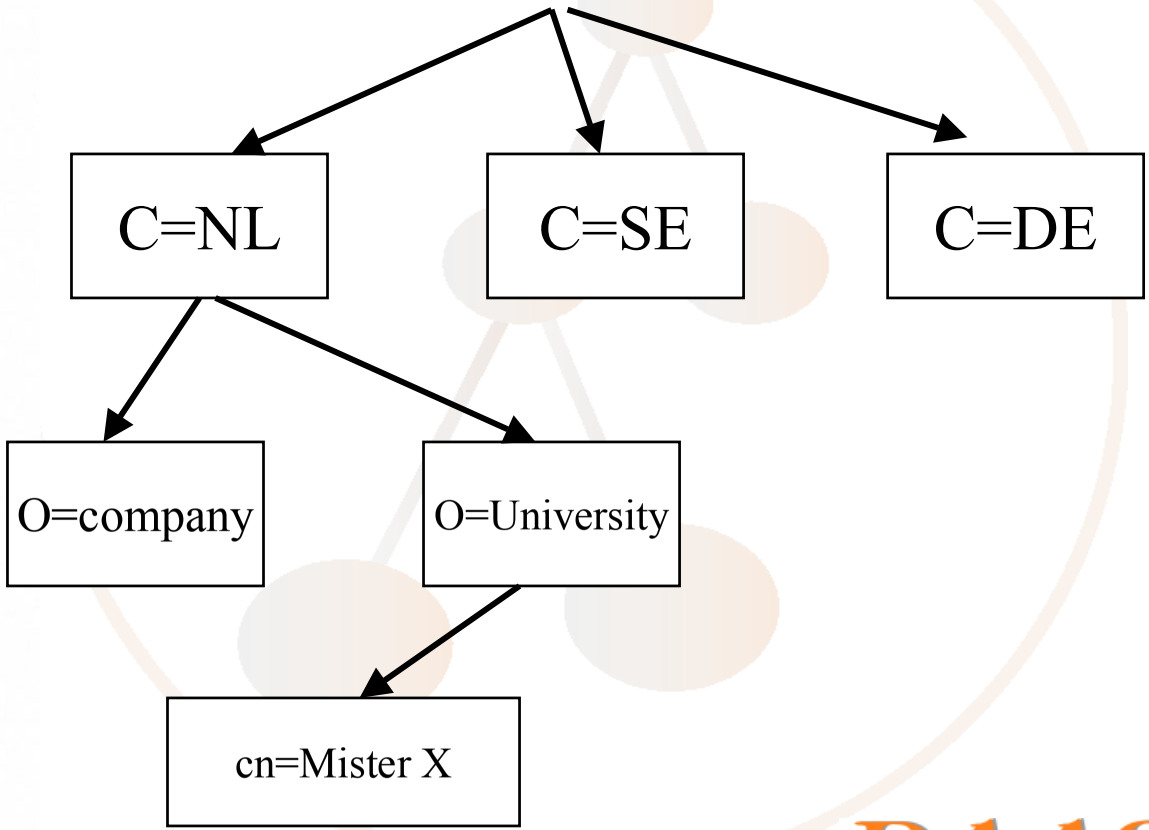
- Daten werden in Einträgen gespeichert
- Einträge werden als Baumknoten gespeichert
  - Jeder Knoten hat 0 bis n Kinderknoten
  - Jeder Knoten hat genau 1 Elternknoten
    - Mit Ausnahme des Wurzelknotens

DAASI International

Directory Applications for Advanced Security and Information Management

Directory Information Tree (DIT)

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit



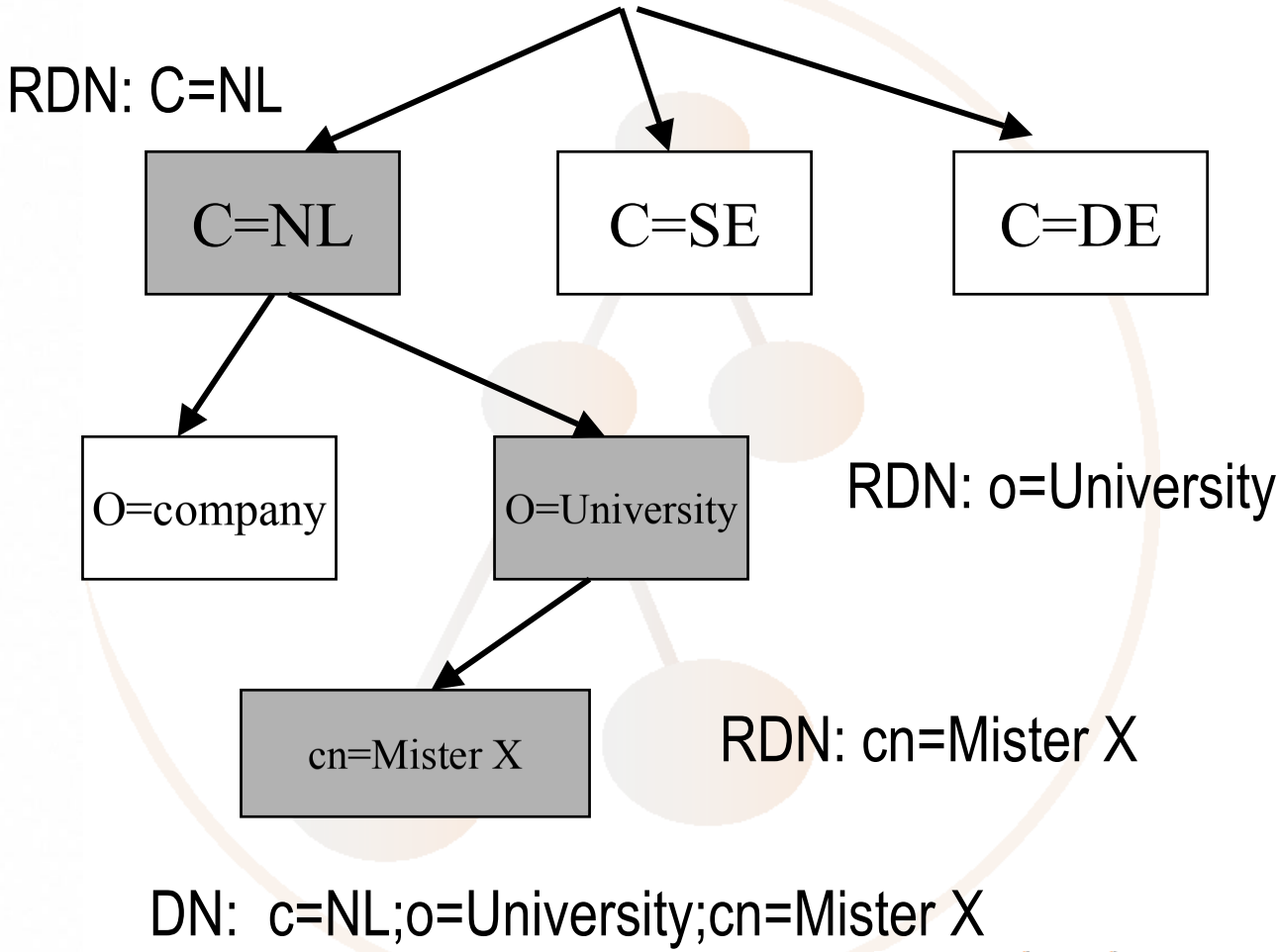
DAASI International

Directory Applications for Advanced Security and Information Management

Distinguished Name (DN)

- Jeder Eintrag hat einen eindeutigen Namen
  - In der eigenen Hierarchieebene: Relative Distinguished Name (RDN)
  - Alle RDNs auf dem Pfad von der Wurzel zum Eintrag bilden zusammen den Distinguished Name (DN)
- Keine zwei Geschwistereinträge (also mit gemeinsamen Elternknoten) dürfen den gleichen RDN haben
- Demnach hat kein Eintrag imgesamten Baum einen gleichen Namen

Relative Distinguished Name (RDN)
Distinguished Name (DN)



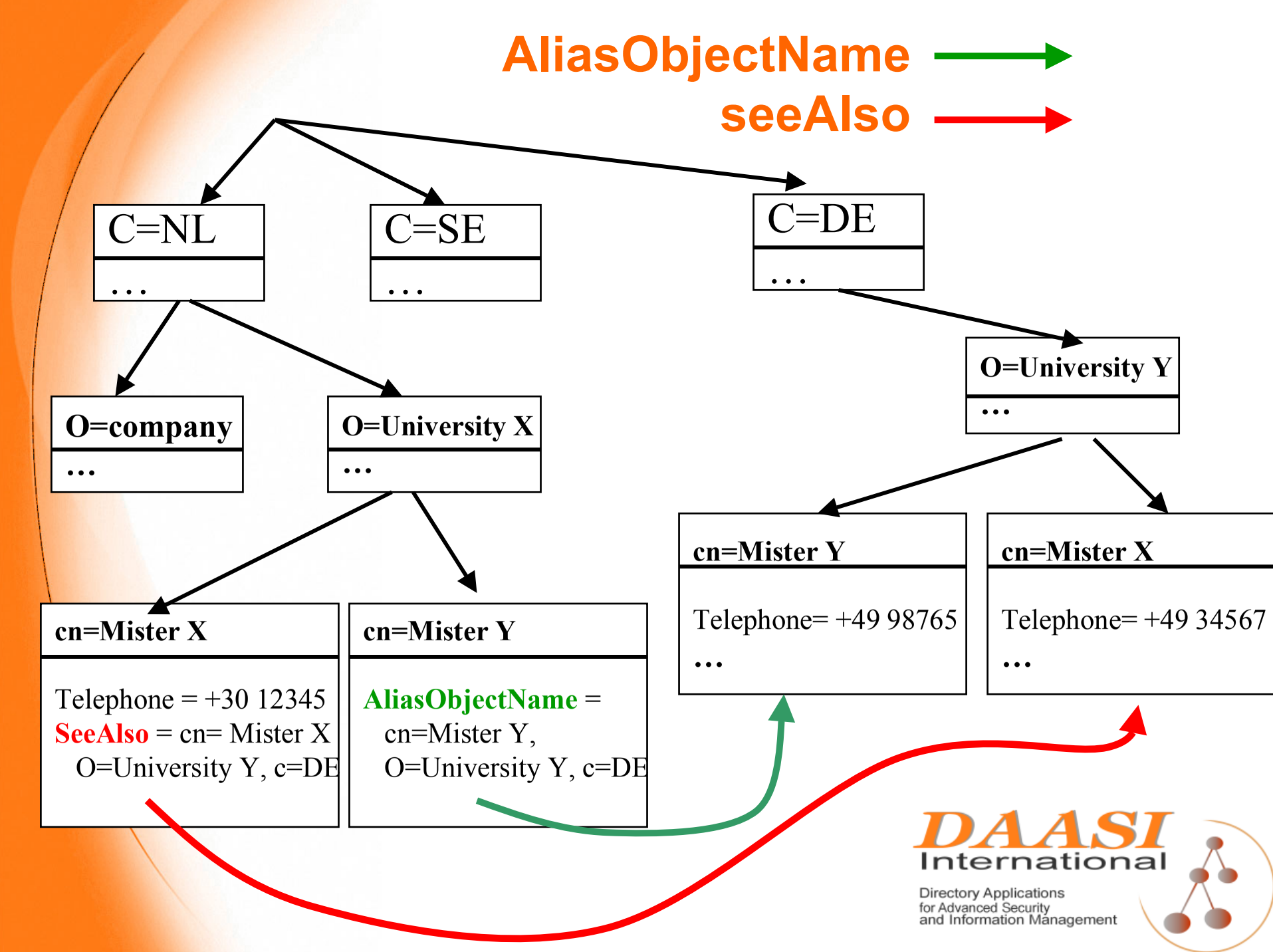
DAASI International
Directory Applications for Advanced Security and Information Management

DN Zeiger

- Alias Einträge haben einen DN zeigen auf einen weiteren DN
- seeAlso Einträge enthalten eigene Daten und zusätzlich einen DN Zeiger auf einen weiteren Eintrag

DAASI International

Directory Applications for Advanced Security and Information Management



DAASI International

Directory Applications for Advanced Security and Information Management

LDAP Informationsmodell

- Ein Datensatz wird *Eintrag (entry)* genannt
- Ein Eintrag besteht aus *Attributen*
- Ein Attribut besteht aus *Attributtyp* und *Attributwert*
- Es kann als *Single-* oder *Multivalued* definiert werden
- Ein Attributtyp hat eine zugehörige *Attributsyntax*
- Der Attributwert unterliegt dieser Syntax
- Zusätzlich kann ein Attributtyp verschiedene *Vergleichsregeln (Matching Rules)* haben:
  - *Equality*
  - *Substring*
  - *Ordering*
  - *Extensible* (selbstdefiniert)

DAASI International
Directory Applications for Advanced Security and Information Management

Spezielle Attribute

- Ein oder mehrere Attribut-Typ-Wert-Paare bilden den RDN
  - *Naming Attribute* oder
  - *Distinguished Attribute*
- Jeder Eintrag muss mindestens ein *Objektklassen-Attribut* haben, welches
  - Den gesamten Eintrag charakterisiert
  - Einen Satz zu verwendender Attributtypen spezifiziert (*Must und May-Attribute)*
- Objektklassen können Attributtypen von übergeordneten Objektklassen ererben

DAASI International

Directory Applications for Advanced Security and Information Management

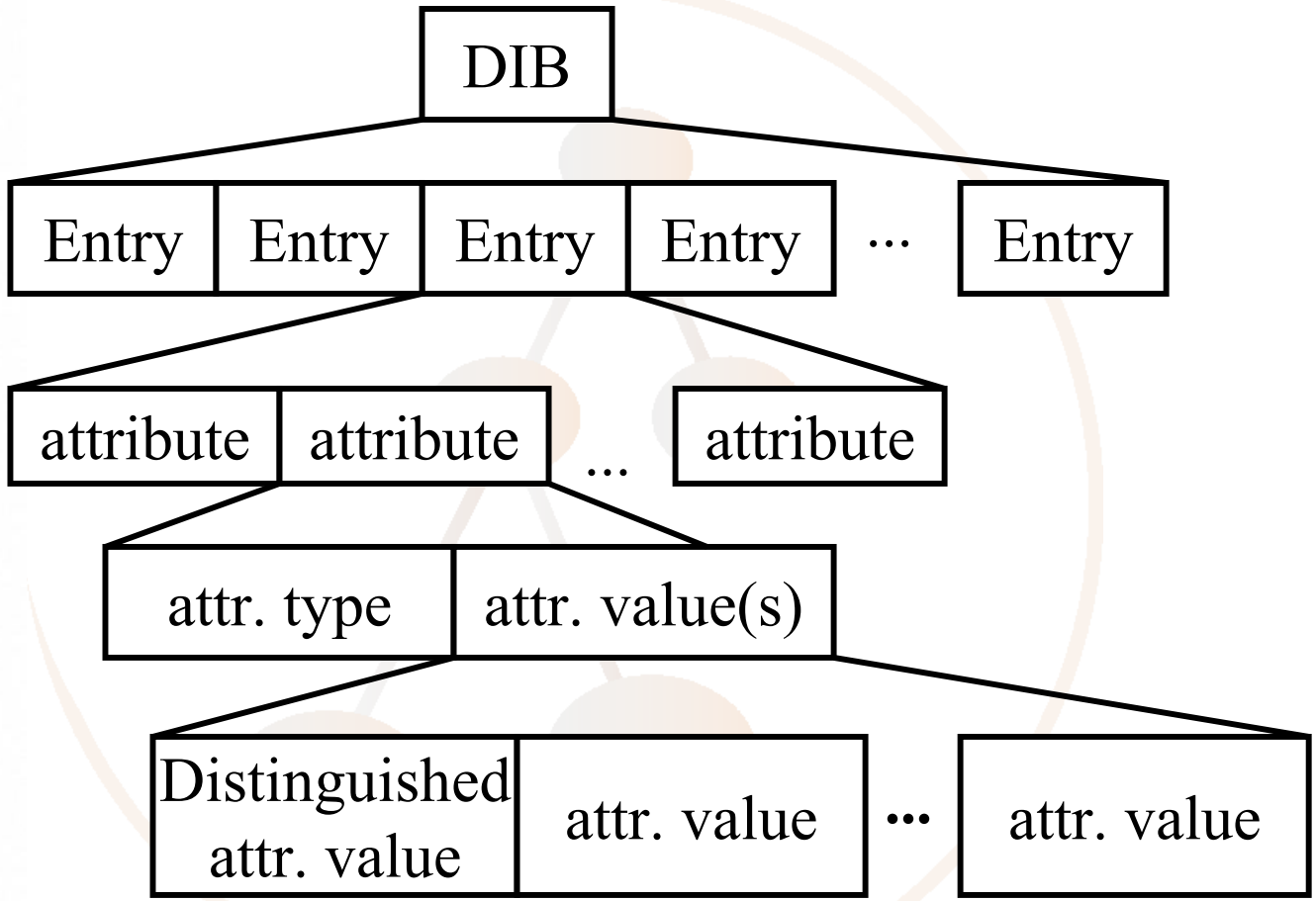
Schema

- **Eine Ansammlung von Objektklassen, Attributen, Syntaxen und Matching Rules, die für einen bestimmten Zweck definiert wurden, werden *Schema* genannt**

DAASI International

Directory Applications for Advanced Security and Information Management

Directory Information Base



DAASI International

Directory Applications for Advanced Security and Information Management

Standardisierte Objektklassen

ObjectClass	distinguished Attr. and abbreviation	other Attributes
country	countryName or c	description, searchGuide, ...
locality	localityName or l	description, ...
organization	organizationName or o	description, postalAdress, ...
organizational Unit	organizationalUnit-Name or ou	description, postalAdress, ...
person	commonName or cn	surname, title, ...

DAASI International

Directory Applications for Advanced Security and Information Management

Beispiel

DN: cn=Mister X, o=University, c=NL

Objectclass=top
Objectclass=person
Objectclass=organizationalPerson
cn=Mister X
cn=Xavier Xerxes
mail=X@dot.com
mail=Mister.X@dot.com
telephoneNumber=1234567

DAASI International
Directory Applications for Advanced Security and Information Management

Offene Struktur

- Mann kann eigenes Schema definieren
  - Objektklassen
  - Attribute
  - [Syntaxen]
  - [Matching Rules]
- Lokal kann man selbstdefiniertes Schema einfach verwenden
- Wenn das Schema global genutzt werden soll muss man es
  - Standardisieren (IETF-RFC)
  - Oder wenigstens registrieren (s.u.)

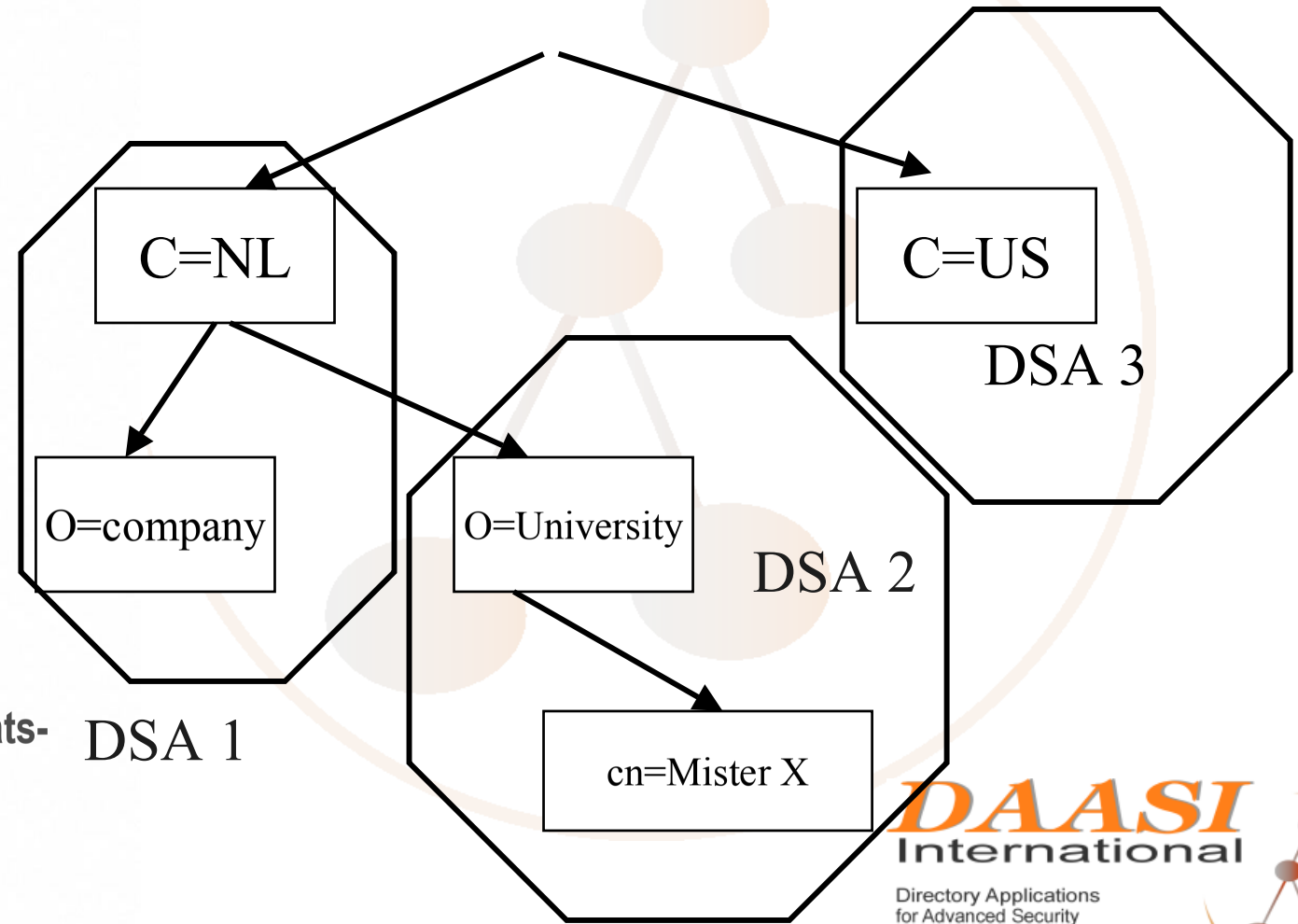
DAASI International

Directory Applications for Advanced Security and Information Management

Verteilung der Daten

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit

➢ **Daten können auf verschiedene Server, sog. *Directory Service Agents (DSA)* verteilt werden:**



DAASI International
Directory Applications for Advanced Security and Information Management

Funktionsmodell

- Authentifizierungs-Operationen:
  - bind
  - unbind
  - abandon
- Abfrage-Operationen:
  - search
  - compare
- Update-Operationen:
  - add
  - delete
  - modify
  - modifyDN

DAASI International

Directory Applications for Advanced Security and Information Management

Authentifizierung

- Simple Bind
  - Mann authentifiziert sich über einen Eintrag mittels DN und Passwort
  - Passwort geht ungeschützt über das Netz!
- Simple Bind + TLS (Transport Layer Security ~= SSL)
  - Vor dem Bind-Vorgang wird die gesamte Session verschlüsselt
  - StartTLS-Operation
- Alternative Authentifizierung mittels SASL
  - Simple Authentication and Security Layer
  - Vorgeschrieben: Digest MD5 (challenge response)
  - Andere SASL-Mechanismen möglich

DAASI International
Directory Applications for Advanced Security and Information Management

LDIF

- LDAP Data Interchange Format
- ASCII-Format zum Datenaustausch
- Beispiel:

```
dn: cn=Mister X, o=University, c=NL
objectclass=top
objectclass=person
objectclass=organizationalPerson
cn=Mister X
cn=Xavier Xerxes
mail=X@dot.com
mail=Mister.X@dot.com
telephoneNumber=1234567

dn: cn=next entry, ...
```

DAASI International
Directory Applications for Advanced Security and Information Management

LDAPv3 Standard

- **Fertige Standards:**
  - Das Informationsmodell
  - Ein Namensraum
  - Ein Netzwerkprotokoll (Client-Server)
  - Sichere Authentifizierungs- und Verschlüsselungsmechanismern
  - Ein Referierungsmodell (Referral)
  - Erweiterungsmechanismen
  - LDAP URL
  - Datenaustauschformat (LDIF)
  - APIs für C und Java (de facto)
- **In Arbeit**
  - Replikationsmodell
  - Zugriffskontrolle

DAASI International
Directory Applications for Advanced Security and Information Management

Replikation

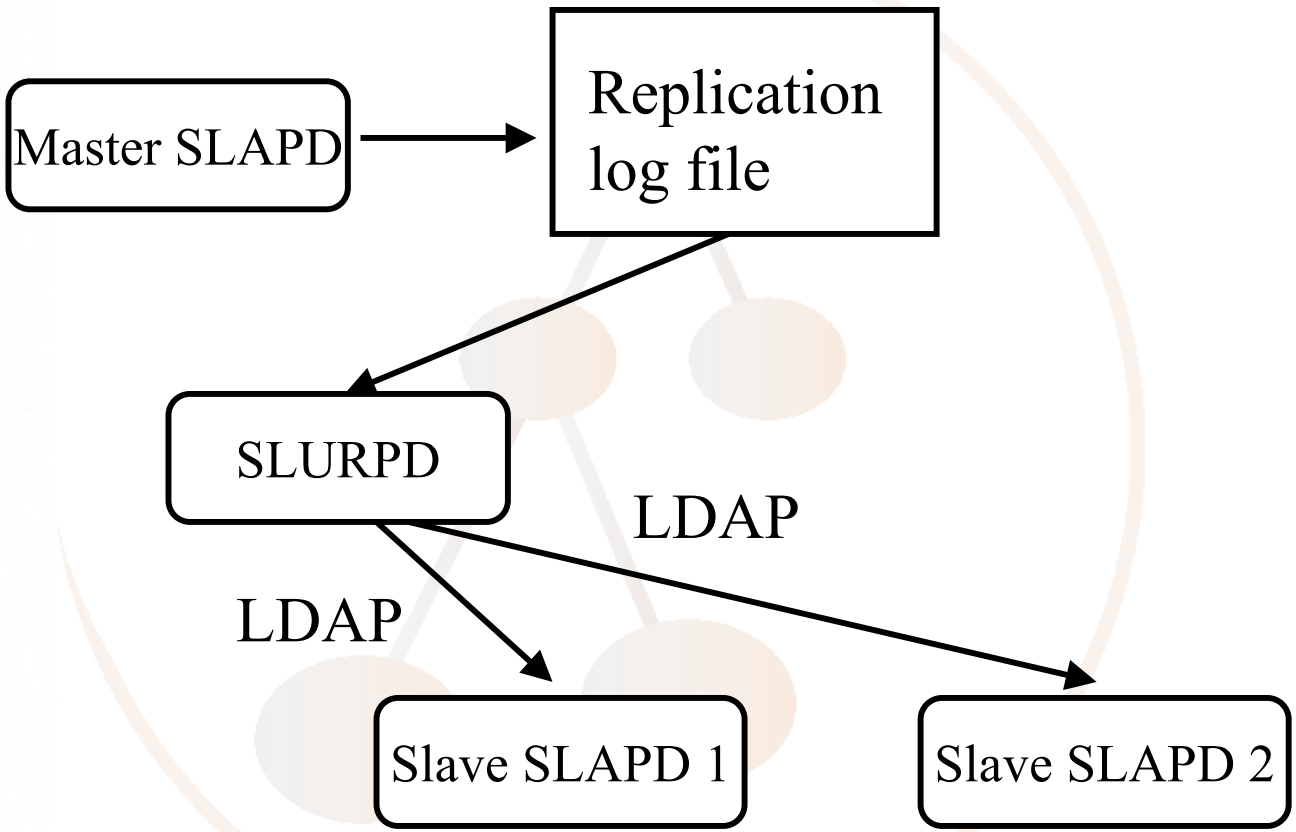
- Standardisierungsbemühungen seit 1998
- IETF WG LDUP
  - LDAP Duplication / Replication / Update Protocols
- Ohne Standard keine Implementierungsübergreifende Replikation möglich
- Augenblickliche Lösungen:
  - Datenaustausch via LDIF-Dateien
  - Defacto Standard der Open Source Lösung (s.u.)
  - XML-Ansätze
  - Proprietäre Lösungen

DAASI International

Directory Applications for Advanced Security and Information Management

Replikationslösung in Open Source Implementierung

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit



DAASI International
Directory Applications for Advanced Security and Information Management

Format des Replication log file


```
replica: host1.com:9999
replica: host2.com:8888
time: 960373276
dn: cn=Mister X, o=University, c=HU
changetype: delete

replica: host1.com:9999
replica: host2.com:8888
time: 960373277
dn: cn=Mister X, o=University, c=HU
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Xavier Xerxes
mail=X@dot.com
mail=Mister.X@dot.com
telephoneNumber=1234567
```

Wer Spricht LDAP

- Alle heutigen Verzeichnisdienst-Implementierungen
  - Alle X.500(93) Implementierungen
  - Novell Directory Service (NDS)
  - Microsoft Active Directory (AD)
- Viele Clientanwendungen
  - Mailagenten (für Emailrecherche)
  - Browser (LDAP-URL)
  - Verschlüsselungsprogramme
- In vielen Standardimplementierungen berücksichtigt
  - IMAP, SMTP Auth, etc.
  - Apache Webserver

DAASI International
Directory Applications for Advanced Security and Information Management

Open LDAP

- Open Source Implementierung von LDAPv3
- Aus der Open Source Implementierung der University of Michigan entwickelt
- Internationales Entwicklerteam
  - Hauptentwickler Kurt Zeilenga von IBM finanziert
  - Sehr nah an Standardisierungsgremien
  - Stetige Weiterentwicklung
- Wird in vielen Projekten im Produktionsbetrieb eingesetzt
  - Im Forschungsbereich
  - Im kommerziellen Bereich
- http://www.openldap.org

DAASI International
Directory Applications for Advanced Security and Information Management

Vorteile von OpenLDAP

- Voll LDAPv3 kompatibel
  - Einschließlich TLS
- Stabil
- Relativ performant
- Gute Zugriffskontrollmechanismen
  - Atomar definierbar (einzelne Attribute eines Eintrags)
  - Kann abhängig gemacht werden vom Authentifizierungsgrad
  - Aber auch von z.B. IP-Adresse
- Stabiler Replikationsmechanismus (s.o.)

DAASI International

Directory Applications for Advanced Security and Information Management

Zusammenfassung: Vorteile von LDAP

- Objektorientierte Datenmodellierung
- Offener Standard ermöglicht Unabhängigkeit von Herstellern
- Verteilung ermöglicht beliebige Skalierbarkeit
- Replikation ermöglicht beliebig hohe Ausfallssicherheit
- Hohe Sicherheit durch Zugriffskontrolle und Authentifizierung
- Daten sind über TCP/IP basiertes Netzwerkprotokoll zugänglich
- Die selben Daten können von verschiedenen Anwendungen verwendet werden
- Es gibt eine stabile Open-Source-Implementierung

DAASI International
Directory Applications for Advanced Security and Information Management

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit

Anwendungsmöglichkeiten

DAASI International

Directory Applications for Advanced Security and Information Management

Kontaktdateninformationsdienste

- Die klassische Anwendung (ITU)
- Entsprechendes Schema bereits im Standard definiert
  - Personendaten (White Pages)
  - Organisationsdaten (Yellow Pages)
- Organisationsstruktur abbildbar
- Elektronisches Telefonbuch
- Elektronisches Emailverzeichnis
- Grundlage für viele weitere Anwendungen, z.B: elektronisches Vorlesungsverzeichnis

DAASI International

Directory Applications for Advanced Security and Information Management

Unix-Benutzerverwaltung

- Standardisierte LDAP Objektklassen zur Abbildung von NIS
  - UNIX user (/etc/passwd and shadow file)
  - Groups (/etc/groups)
  - IP services (/etc/services)
  - IP protocols (/etc/protocols)
  - RPCs (/etc/rpc)
  - IP hosts and networks
  - NIS network groups and maps
  - MAC addresses
  - Boot information

DAASI International

Directory Applications for Advanced Security and Information Management

Authentifizierungsdienst (1/4)

- **Problem:**
  - Benutzer haben Zugriff auf viele Rechner
  - Auf jedem Rechner eigene LoginID und Passwort
  - Benutzer muss sich viele Passwörter merken
  - Unterschiedliche Password-Policies
  - ➔ sehr hoher Administrationsaufwand

DAASI International

Directory Applications for Advanced Security and Information Management

Authentifizierungsdienst (2/4)

- **Lösung:**
  - **Zentraler verzeichnisdienstbasierter Authentifizierungsdienst**
  - **Unix-Clients**
    - **Können mittels NSS / PAM-LDAP direkt auf LDAP-Server zugreifen**
    - **Aber auch Anbindung an MS Active Directory (AD) möglich mit Kerberos**
  - **Windows-Clients**
    - **Einfache Integration in AD**
    - **Aber auch über SAMBA Anbindung an LDAP-Server möglich**

DAASI International

Directory Applications for Advanced Security and Information Management

Authentifizierungsdienst (3/4)

- Mit dem Authentifizierungsdienst lässt sich nicht nur das Login realisieren
- Er lässt sich auch in verschiedene Netzanwendungen integrieren, z.B.:
  - IMAP, POP, SMTP auth, FTP, HTTP auth, RSH, SSH, etc. etc.
- Single Sign On (SSO)

DAASI International
Directory Applications for Advanced Security and Information Management

Authentifizierungsdienst (4/4)

- **Vorteil:**
  - **Ein Passwort für alle Rechner**
    - Der User muss sich weniger merken
    - Der Administrator wird erheblich entlastet
- **Nachteil:**
  - **Ein Passwort für alle Rechner**
    - Single point of failure
    - Größerer Schaden bei Komprimittierung

DAASI International
Directory Applications for Advanced Security and Information Management

Gleiche Daten - Verschiedene Dienste

- Z.B. Kombination Kontaktdatendienst, Benutzerverwaltung und Authentifizierungsdienst, Elektronisches Vorlesungsverzeichnis
- Einfach weitere Objektklassenattribute zum Eintrag hinzufügen und neues Benutzerinterface implementieren
- Dies führt zu erheblichen Kosteneinsparungen

DAASI International

Directory Applications for Advanced Security and Information Management

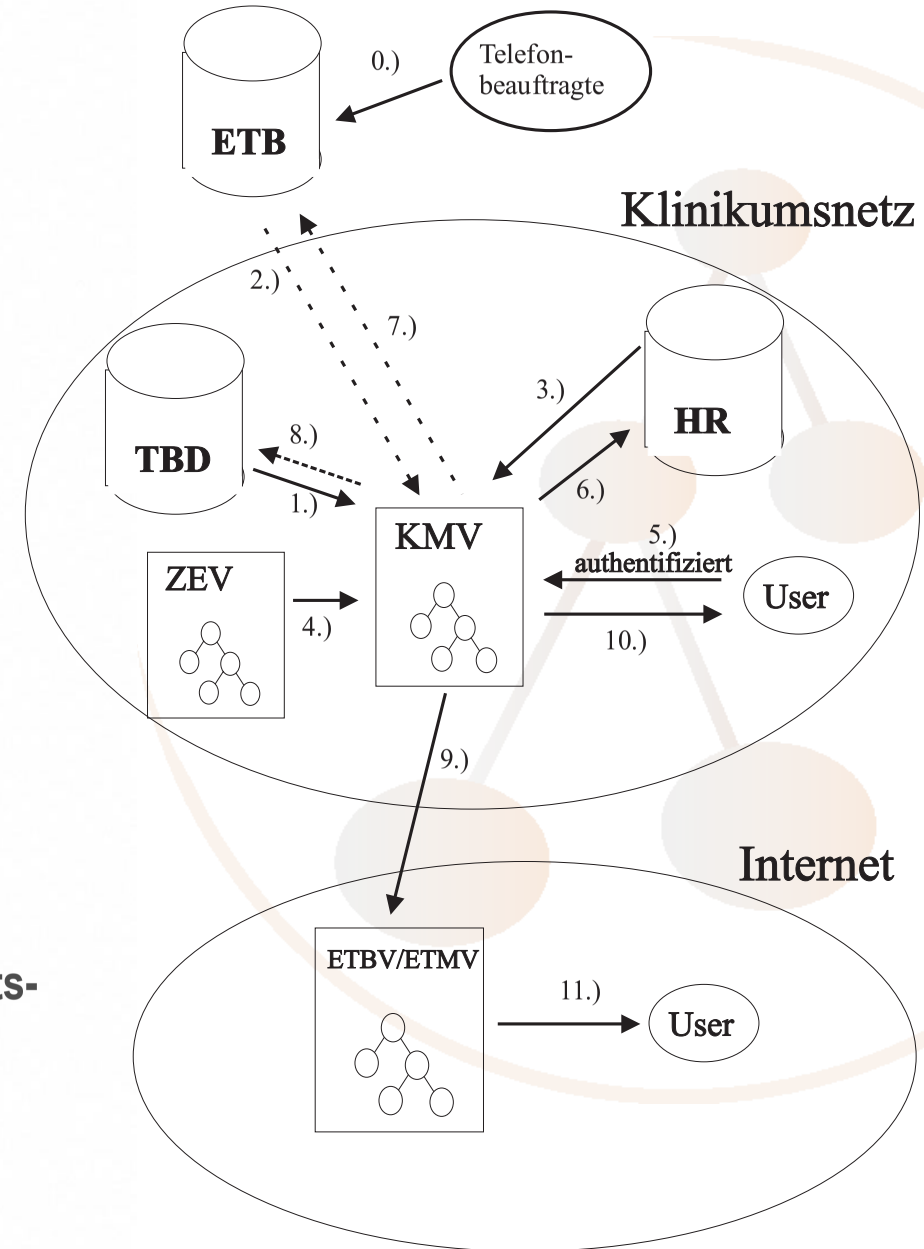
Metadirectory

- 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

DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory Beispiel

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit



DAASI International

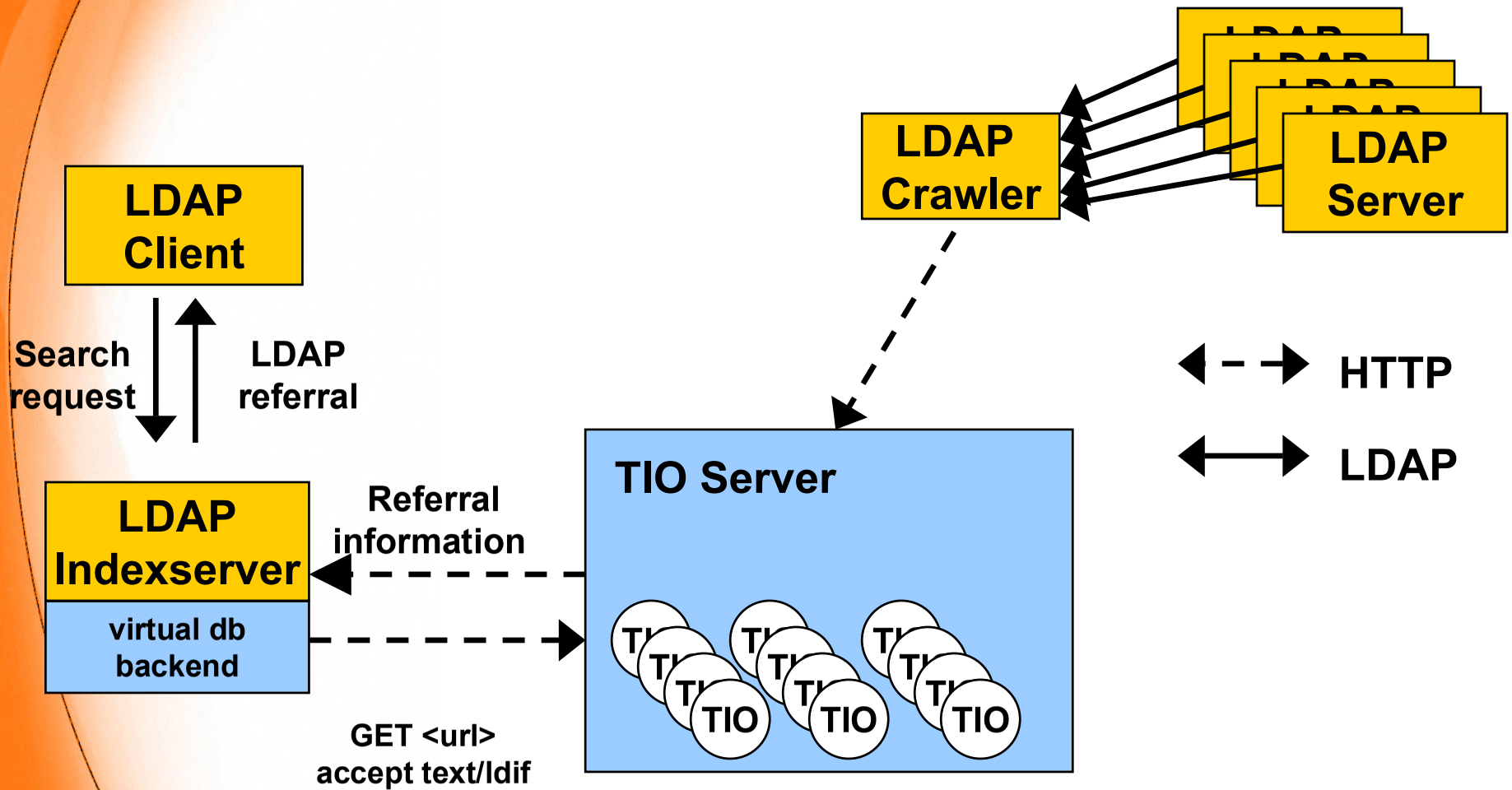
Directory Applications for Advanced Security and Information Management

Indexsystem (1/2)

- Hoch skalierbare LDAP-Dienste können mittels eines Indexsystems aufgebaut werden
- Baut auf Referral auf
- IETF Standard Common Indexing Protocol
  - Flexible Index Architektur
  - MIME Definitionen
  - Verschiedene Transportprotokolle (email, FTP, HTTP)
  - Verschieden Index-Objekt-Formate (u.a.: Tagged Index Object, TIO)

DAASI International
Directory Applications for Advanced Security and Information Management

Index-System (2/2)



DAASI International
Directory Applications for Advanced Security and Information Management

Zertifikatsserver für PKI

The Burton Group:

Network Strategy Report, PKI Architecture, July 1997: (Quoted after: S. Zeber, X.500 Directory Services and PKI issues, http://nra.nacosa.nato.int/pki/hdocs/pkiahwg30/index.htm)

"... Customers should always consider PKI a directory-enabled set of services and infrastructure. Without directory services, PKI will be exponentially harder to implement and manage. Consequently, customers should't deploy PKI widely without an accompanying directory plan"

DAASI International

Directory Applications for Advanced Security and Information Management

Zertifikatsserver für PKI

- Veröffentlichungsmedium für öffentliche Schlüssel bzw. Zertifikate
  - Um ohne vorherige Kommunizierung von Schlüsseln für jemanden ein Dokument zu verschlüsseln das nur mit dessen privaten Schlüssel entschlüsselt werden Kann
  - Um eine mit dem privaten Schlüssel generierte digitale Signatur überprüfen zu können
- Im Zertifikat wird die zu einem öffentlichen Schlüssel zugehörige Identität von einer vertrauenswürdigen Stelle (Certification Authority, CA) durch digitale Signatur bestätigt

DAASI International
Directory Applications for Advanced Security and Information Management

Zertifikatsserver für PKI

- Der Verzeichnisdienst
  - hält Zertifikate im Netz vor, auf die Standardanwendungen (S/MIME und PGP) zugreifen können
  - Dokumentiert zurückgerufene Zertifikate in sog. Certificate Revocation Lists (CRL)
  - Kann somit Grundlage eines Online Certificate Status Protocol (OCSP) Dienst bilden
- Entweder betreibt eine CA den Verzeichnisdienst selber, oder liefert Zertifikate auf einem gesicherten Weg an den Betreiber

DAASI International

Directory Applications for Advanced Security and Information Management

Neuer Vorschlag

- userCertificate ist das bereits standardisierte Attribut zum Speichern des Zertifikats
- Problem:
  - bei vielen Zertifikaten einer Person muss der Client alle Zertifikate holen und einzeln analysieren, um das richtige Zertifikat (z.B. das mit Key usage: encryption) zu finden
- Unsere Lösung:
  - Metadaten-Ansatz: Zusätzlich zum Zertifikat werden Inhalte der wichtigsten Zertifikatsfelder in LDAP Attributen abgelegt

DAASI International

Directory Applications for Advanced Security and Information Management

Vorteile

- Lösung lässt sich mit bestehenden Servern implementieren
- Anpassung der Clients ist einfach, da nur der Suchfilter modifiziert werden muss
- Die Zertifikate können im Rahmen eines Indexsystems indiziert werden

DAASI International

Directory Applications for Advanced Security and Information Management

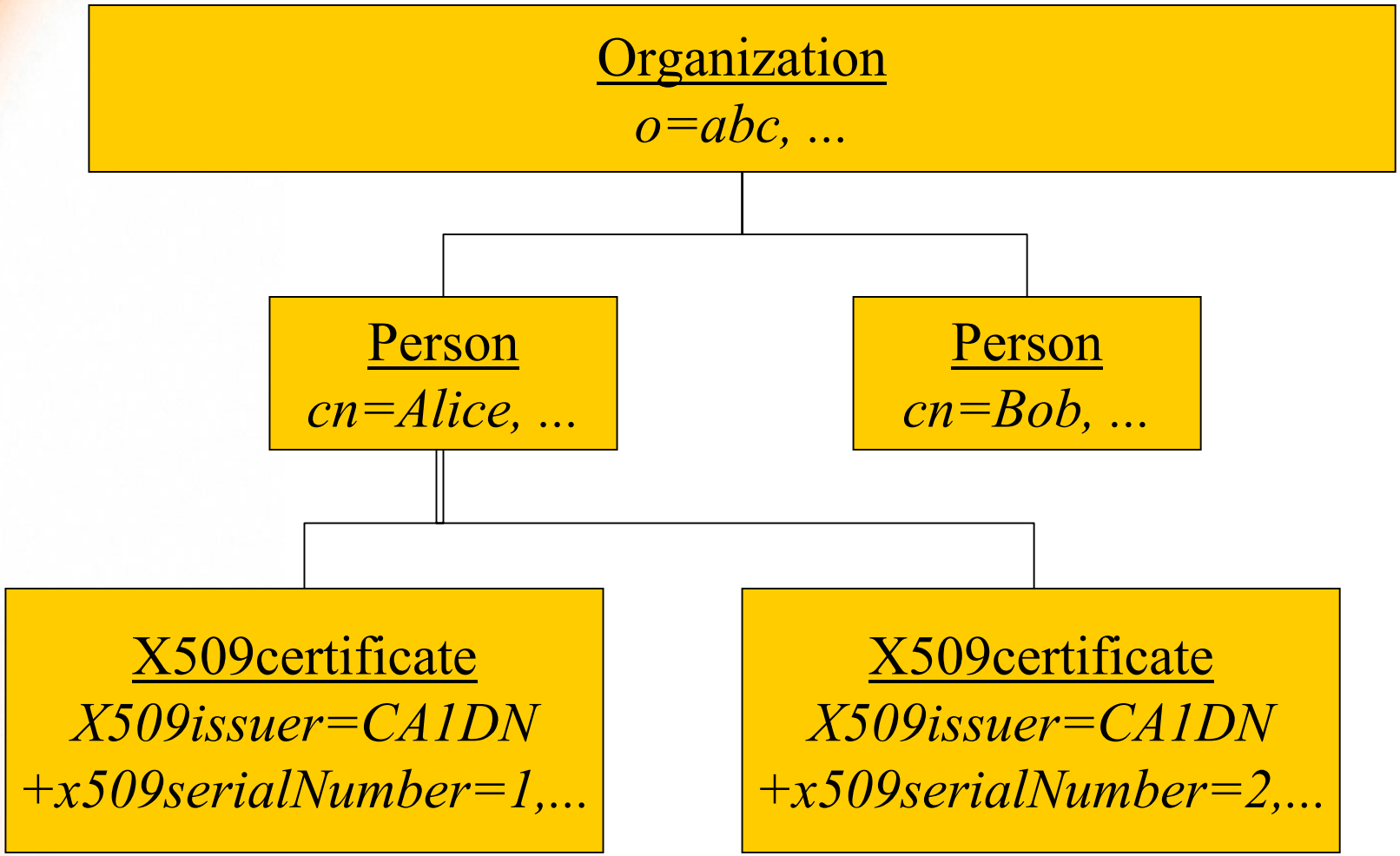
Objektklasse: x509certificate

(1.3.6.1.4.1.10126.1.5.4.2.1 NAME 'x509certificate'

MUST (x509serialNumber $ x509signatureAlgorithm $ x509issuer $
x509validityNotBefore $ x509validityNotAfter $
x509subject $ x509subjectPublicKeyInfoAlgorithm)

MAY (mail $ x509subjectKeyIdentifier $ x509keyUsage $
x509policyInformationIdentifier $
x509subjectAltNameRfc822Name $
x509subjectAltNameDnsName $
x509subjectAltNameDirectoryName $
x509subjectAltNameURI $
x509subjectAltNameIpAddress$
x509subjectAltNameRegisteredID $
x509isssuerAltNameRfc822Name $
x509isssuerAltNameDnsName $
x509isssuerAltNameDirectoryName $
x509isssuerAltNameURI $
x509isssuerAltNameIpAddress $
qx509isssuerAltNameRegisteredID $

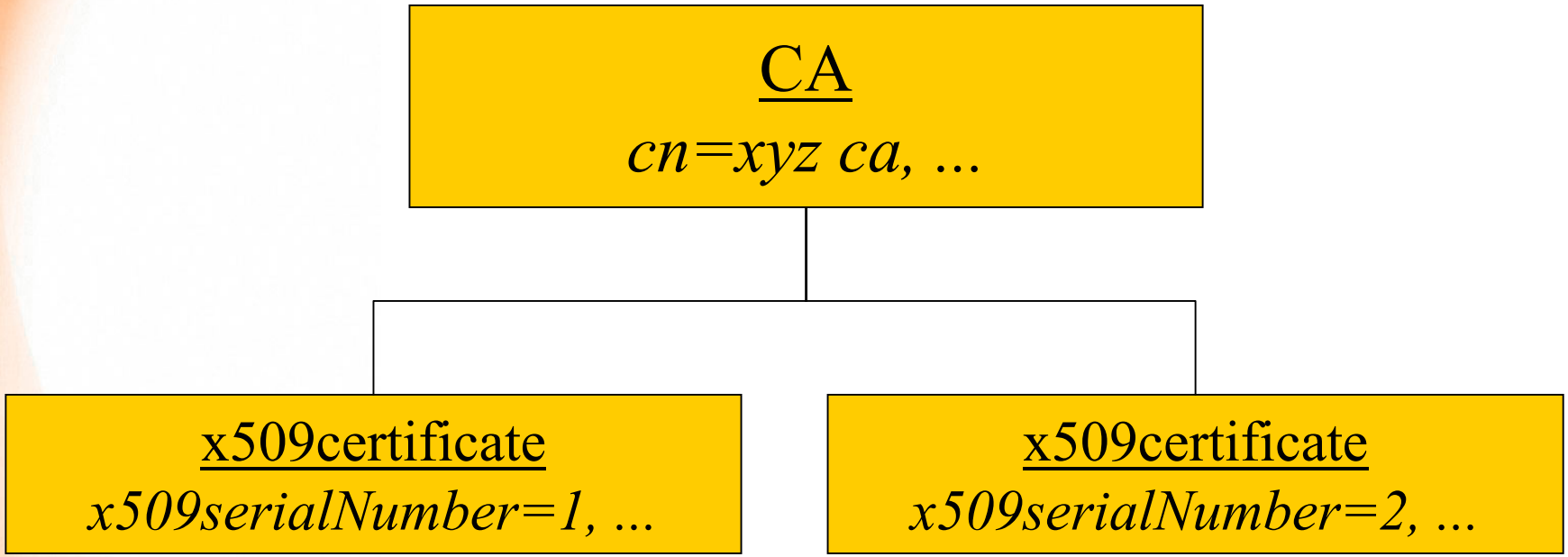
DIT-Struktur im Personenverzeichnis



DAASI International

Directory Applications
for Advanced Security
and Information Management

DIT-Struktur im Zertifikatsverzeichnis



DAASI International
Directory Applications
for Advanced Security
and Information Management

Verzeichnisdienste Im Bereich Digital Libraries

- Metadaten sind in der einfachsten Definition Daten über Daten,
  - also z.B. Daten über einen Text, wie
  - Author, Titel, Erscheinungsjahr, etc.
- Schwierige Metadaten sind Verschlagwortungsdaten
  - Wie kann man sicherstellen das selbe Schlagwort für dasselbe Thema zu verwenden?
  - Kontrolliertes Vokabular

DAASI International

Directory Applications for Advanced Security and Information Management

Kontrolliertes Vokabular

- Klassifikationssysteme
  - Z.B. Dewey Decimal Classification (DDC)
  - Klassen, Subklassen, Subsubklassen, ...
  - Eine Beziehungsart zwischen den Begriffen
- Thesaurus
  - Ansammlung von Homonymen
  - Kann auch Antinyme und einige weitere Relationen enthalten
  - Begrenzte Anzahl von Beziehungsarten zwischen den Begriffen

DAASI International

Directory Applications for Advanced Security and Information Management

Ontologien

- Wiederum Begriffe und die Beziehungen zwischen den Begriffen
- Aber Keine Limitierung der Anzahl der Beziehungsarten
  - Einschließlich Unterklasse/Oberklasse
  - Einschließlich Homonyme und Antinyme
  - ...

- Ontologien sind perfekte Wissenspeicher
- Metadaten und Ontologien können mit LDAP verwaltet werden, mit allen Vorteilen von LDAP

DAASI International

Directory Applications for Advanced Security and Information Management

Metadaten und Ontologien

- Nicht nur im Bereich Digital Libraries interessant:
  - *Semantic Web* mit Suchmaschienen, die Begriffe kennen und nicht nur Strings
  - Content Management Systeme
  - E-Learning
  - Intelligente Agentenprogramme, die Daten von Portalen beziehen via Web Services (SOAP, WSDL)

DAASI International

Directory Applications for Advanced Security and Information Management

Ressourcen-Verwaltung

- Daten über Computer, Drucker, Netzknoten, etc. können mit LDAP verwendet werden
- Software Lizenzmanagement, Updateverwaltung
- Dieses Nutzungspotential wird im Grid Computing genutzt

DAASI International

Directory Applications for Advanced Security and Information Management

Grid Computing

- Problem: Petabyte von Daten müssen mit komplexen Algorithmen auf tausenden CPUs analysiert werden (Kernphysik, Metereologie, etc.)
- Grid Computing will dieses Problem mit einer Infrastruktur lösen, deren Komplexität vor dem Benutzer versteckt wird (in Analogie zum Stromnetz / Steckdose)
- Wichtigste Implementierung Globus (www.globus.org) basiert auf OpenLDAP (Grid Information System und Replika Management System)

DAASI International
Directory Applications for Advanced Security and Information Management

Netzwerk-Verwaltung

- Verzeichnisdienstbasiertes Netzwerk-Policy-Repository
  - Regeln für Routen und zum Prioriesieren von IP-Packeten
  - Regeln und Informationen für Authentizitätsprüfungen
- Basiert auf Common Information Model (CIM)
- Directory Enabled Networks (DEN)
- IPSec Policy
- Mit diesen Technologien lassen sich aber auch beliebige andere Policy Daten verwalten

DAASI International
Directory Applications for Advanced Security and Information Management

Internationales Forschungsumfeld

DAASI International
Directory Applications for Advanced Security and Information Management

TERENA

- Europäische Vereinigung der Nationalen Forschungsnetze (DFN, SurfNet, etc.)
- Forschung und Pilotierung von Netztechnologien und –Anwendungen
  - Konferenzen
  - Projekte
  - Task Forces
- www.terena.nl

TERENA und Verzeichnisdienste

- TF-LSD: Task Force LDAP Service Deployment
  - Charter: www.terena.nl/task-forces/tf-lsd
  - Koordiniert Aktivitäten zu
    - LDAP-Index-basierten Europäischen White-Pages-Verzeichnisdienst
    - PKI-Koordinierung (in Zusammenarbeit mit TF-AACE, Authentication and Authorisation Coordination in Europe
- Projekt DEEP (DAASI International)
  - Development of an European EduPerson
  - Phase 1 Bedarfsanalyse via Webfrageboden
  - www.daasi.de/surveys/DEEP

DAASI International

Directory Applications for Advanced Security and Information Management

TERENA und Verzeichnisdienste

- **Projekt LDAP Schema Registry (DAASI Int.)**
  - **Informationssystem zum Auffinden bzw. Registrieren von definiertem Schema**
  - **Policy für Datenaufnahme**
    - **Bedingung gute Information**
    - **OpenLDAP basierte Datenbank**
    - **Standardschema basiert**
  - **WWW.daasi.de/projects/Schemaregistry**

DAASI International

Directory Applications for Advanced Security and Information Management

USA: Internet2

- MACEDir
- EduPerson
- LDAP Recipie
- Shiboleth
  - Domainübergreifendes Authentifizierungssystem
- Groups
- Metadirectory
- www.internet2.org

DAASI International

Directory Applications for Advanced Security and Information Management

DFN Umfeld

DAASI International
Directory Applications for Advanced Security and Information Management

DFN Directory Services

- Kompetenzzentrum zur Beratung von Forschungsinstituten in Deutschland
- Betrieb der deutschen X.500-Countrylevel Server im Rahmen des Europäischen Projekts NameFLOW
- Konzeption von und Beratung zu Problemlösungen:
  - Zentrales Authentifizierungssystem für zentrales Login
  - Zertifikatsverzeichnis für PGP und X.509
- Projekt läuft voraussichtlich Januar 2003 aus
  - Modelle des Weiterbetriebs in Diskussion

DAASI International

Directory Applications for Advanced Security and Information Management

DFN Projekt AMBIX

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit

- Aufnahme von Mailbenutzern in das X.500-Directory
- Emailverzeichnis für die Forschung in Deutschland mit Webfrontend (ca 60.000 Datensätze)
- Zentraler Verzeichnisdienst für Organisationen, die nicht selbst Verzeichnisdienste betreiben
- Einfache ASCII-Basierte Datenlieferungsformate

DAASI International

Directory Applications for Advanced Security and Information Management

AMBIX und Datenschutz

- Datenschutz von Vorneherein berücksichtigt
  - Wiederspruchslösung mit Minimalset von Datenfeldern
  - Kein Export an Länder mit unzureichender Datenschutzgesetzgebung)
- Crawler von potentiellen Spammern werden erkannt und abgewiesen
- Spamfänger
  - Spezielle Scheineinträge eingefügt deren Emailadresse sonst nirgends veröffentlicht sind
  - Bisher haben wir kein Spam auf diesen Adressen erhalten!

DAASI International

Directory Applications for Advanced Security and Information Management

AMBIX 2002

- Neudesign der Software und Weboberfläche
- LDAPv3 auf OpenLDAP-Basis
- Neues Schema: DFNPerson
- Integration neuer Sichtbarkeitsoption
  - Nur in eigener Domain
  - Nur in Deutschland
  - Nur in Datenschutztreibende Länder
  - Weltweit
- In Kürze „PR-Aktion“ um für neue Teilnehmerorganisationen zu werben

DAASI International
Directory Applications for Advanced Security and Information Management

Deutschlandweiter Index

- Deutschlandweitem X.500/LDAP Index
- Crawler holt regelmäßig neue Daten der integrierten Verzeichnisdienste
- Insgesamt ca. 120.000 Datensätze
- Integration des AMBIX Systems
- Wir integrieren gerne Ihr LDAP oder X.500-Verzeichnis: Email genügt

DAASI International

Directory Applications for Advanced Security and Information Management

DAASI International GmbH

- Einführung in LDAP
- Anwendungen
- Internat. Forschungsumfeld
- DFN Umfeld
- DAASI International
- Universitätsprojekte
- Fazit

- **Wir bieten:**
  - Consulting
  - Design
  - Implementierung
  - Schulung
- **Aber auch:**
  - Serverhosting
  - Datenmanagement
- **Technologische Expertise in:**
  - Verzeichnisdiensttechnologien
  - PKI
  - Informationsmanagement (XML)

DAASI International
Directory Applications for Advanced Security and Information Management

Forschung

- **Weitere Beteiligung an der Forschung und Standardisierung**
  - **TERENA**
  - **IETF**
  - **Global Grid Forum**
  - **Digital Library Bereich**
  - **Forschungs- und Entwicklungsprojekte**
    - **In Europa, im Bund und in den Ländern**
  - **PKI Initiativen der deutschen Industrie (Teletrust)**
  - **Verzeichnisdienstkonzept der PKI-1 der Verwaltung**

DAASI International

Directory Applications for Advanced Security and Information Management

Technologie-Unabhängigkeit

- Offene Standards
- Open Source Software
- Produktunabhängigkeit
- Aber auch Expertise in anderen Verzeichnisdiensttechnologien
  - X.500 Implementierungen
  - Andere LDAP Implementierungen (Sun, Netscape, IBM)
  - Active Directory
  - Novell Directory Services

DAASI International

Directory Applications for Advanced Security and Information Management

Kundenzielgruppen

- Durch Kontakte und Erfahrungen sind deutsche Forschungseinrichtungen Hauptzielgruppe
  - Wir kennen die Probleme der Organisatorischen Abläufe an Universitäten
  - Wir kennen die Bedürfnisse und zu integrierende Altsysteme
  - Durch OpenSource Software können wir Ihnen günstige Angebote machen
- Gesundheitswesen
- Behörden auf allen Ebenen
- Mittelständische Betriebe

DAASI International

Directory Applications for Advanced Security and Information Management

Universitätsprojekte

- Elektronisches Telefon- und Mitarbeiterverzeichnis an der Universität Tübingen
  - X500.uni-tuebingen.de
  - Datenmanagement
  - Produktion des gedruckten Telefonbuchs
- Aufbau eines Mitarbeiterverzeichnis an der Universität Münster
- Bedarfsanalyse zu einem Metadirectory am Universitätsklinikum Tübingen

DAASI International

Directory Applications for Advanced Security and Information Management

Projekt an der Universität Münster

- Ausgangslage, wie überall heterogene Datenbanklandschaft
- Ein erstes Projekt verabredet
  - Aufbau eines Mitarbeiterverzeichnisses
  - Definition des LDAP Schemas und LDIF Datenformat
  - Implementierung auf Grundlage von OpenLDAP
  - Dokumentation, die einen Betrieb ermöglicht
  - Einpflegen der über LDIF zur Verfügung gestellten LDIF-Daten
  - Installation und Konfigurierung von webformularbasierten Datenänderungsmöglichkeiten

DAASI International

Directory Applications for Advanced Security and Information Management

Projekt Universität Münster (2)

- Gesamtprojekt auf Open Source Basis
- Uni Münster ist offen für Abstimmungsprozesse mit anderen Hochschulen in NRW
- Wird dieses in der nächsten Rechenzentrumsleitersitzung zum Thema machen

Fazit

Ich glaube, wir können auch Ihnen behilflich sein

- DFN Directory Services
  - Ambix2002.directory.dfn.de
  - Directory.dfn.de
  - Info@directory.dfn.de
- DAASI International
  - www.daasi.de
  - Info@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management