Verzeichnisdienstanwendungen für Hochschulen auf OpenSource Basis

6. Tagung der DFN-Nutzergruppe
Hochschulverwaltung –
Verwaltung@eUniversity

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

DAASI International
Directory Applications
for Advanced Security
and Information Management

Agenda

- DFN-Verzeichnisdiensprojekte und DAASI International
- Eigenschaften von LDAP
- Anwendungen
  - Kontaktinformationsdienst, Authentifizierung
  - Metadirectory
  - LDAP und PKI
  - LDAP im Bereich Digital Libraries

DAASI International

Directory Applications
for Advanced Security
and Information Management

DFN Projekte als Keimzelle der DAASI International GmbH

- Seit 1994 vom BMBF finanzierte DFN-Forschungsprojekte zu Verzeichnisdiensten an der Universität Tübingen
- 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
- Das letzte DFN-Projekt wurde von DAASI International durchgeführt

DAASI International

Directory Applications
for Advanced Security
and Information Management

DFN-Projektergebnisse

- **AMBIX – 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**
  - **Datenschutzkonformität gewährleistet:**
    - **Wiederspruchslösung mit Minimalset von Datenfeldern**
    - **Kein Export an Länder mit unzureichender Datenschutzgesetzgebung)**

Projektergebnis AMBIX

- 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!
- Integration neuer Sichtbarkeitsoption:
  - Nur in eigener Domain
  - Nur in Deutschland
  - Nur in Datenschutztreibende Länder
  - Weltweit

DFN-Projektergebnisse

- IDEV
  - Index Deutscher Email-Verzeichnisse
  - Deutschlandweiter 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
- AMBIX und IDEV könnten zur Unterstützung von DFN-Videokonferenzdienst dienen

DAASI International GmbH

- Directory Applications for Advanced Security and Information Management
- Nachfolgeinstitution zum Betrieb der entwickelten Dienste
- Offizielles Spin-Off der Universität Tübingen
- International tätig
- Forschung ist wichtiger Bestandteil des Konzeptes
- Augenblicklich 7 Mitarbeiter
- Kooperation mit anderen Firmen und Freelancern für größere Projekte

DAASI International

Directory Applications
for Advanced Security
and Information Management

DAASI: 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

DAASI: Universitätsprojekte

- Elektronisches Telefon- und Mitarbeiterverzeichnis an der Universität Tübingen
  - http://X500.uni-tuebingen.de
  - Datenmanagement
  - Produktion des gedruckten Telefonbuchs
- Aufbau eines Mitarbeiterverzeichnis an der Universität Münster
  - Authorisierungsstruktur
  - Maillistenanbindung
- Bedarfsanalyse zu einem Metadirectory am Universitätsklinikum Tübingen
- PKI Consulting
- Verzeichnisdienst-Consulting am LRZ München
- Weitere Projekte in Vorbereitung

DAASI International

Directory Applications
for Advanced Security
and Information Management

Eigenschaften von LDAP

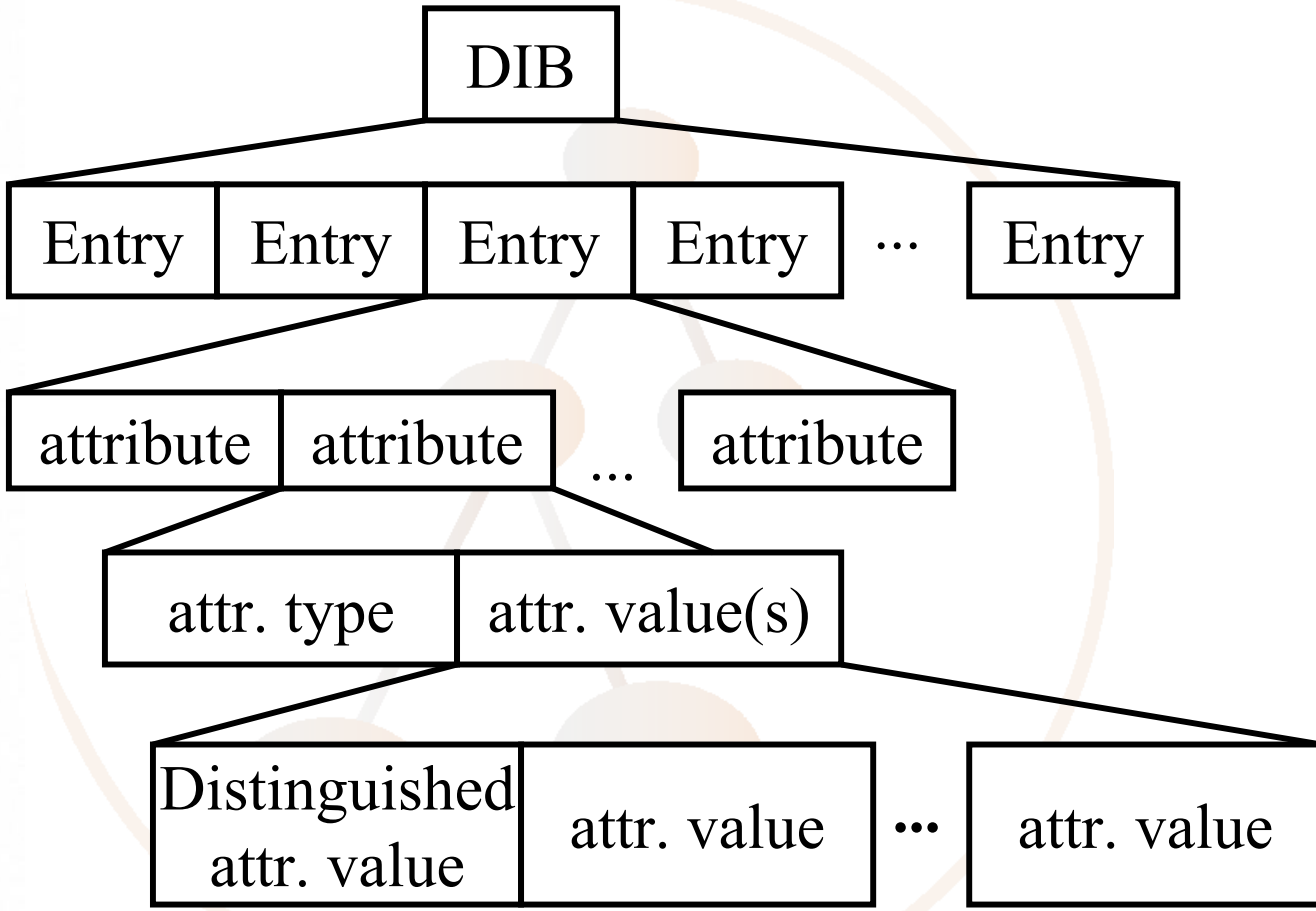
DAASI International

Directory Applications
for Advanced Security
and Information Management

Was ist LDAP?

- Lightweight Directory Access Protocol
- Ein Datenbankmodell (X.500)
  - Hierarchische Datenstruktur
  - Objektorientierter Ansatz
  - Erweiterbar für beliebige Daten
- Ein Netzwerkprotokoll
  - Internetstandard
  - Flexibel erweiterbar
  - Verteilung der Daten im Netz
  - Spiegelung der Daten im Netz

Directory Information Base



Möglichkeit der modularen Datenmodellierung durch Objektklassen

- Strukturelle Objektklassen: jeder Eintrag hat eine strukturelle Objektklassen und davon abgeleitete
  - Objektklasse person
    - Name, Vorname, ...
  - Davon abgeleitet organizationalPerson
    - Raumnummer, ...
  - Davon abgeleitet inetOrgPerson
    - Mailadresse, ...
- Hilfs-Objektklassen: können beliebig viele zu einem Eintrag hinzugefügt werden
  - Objektklasse PKI user
    - X.509 Zertifikat
  - Objektklassen für spezielle Anwendungen z.B. Objektklasse Student
    - Immatrikulationsnummer

Directory Information Tree (DIT)

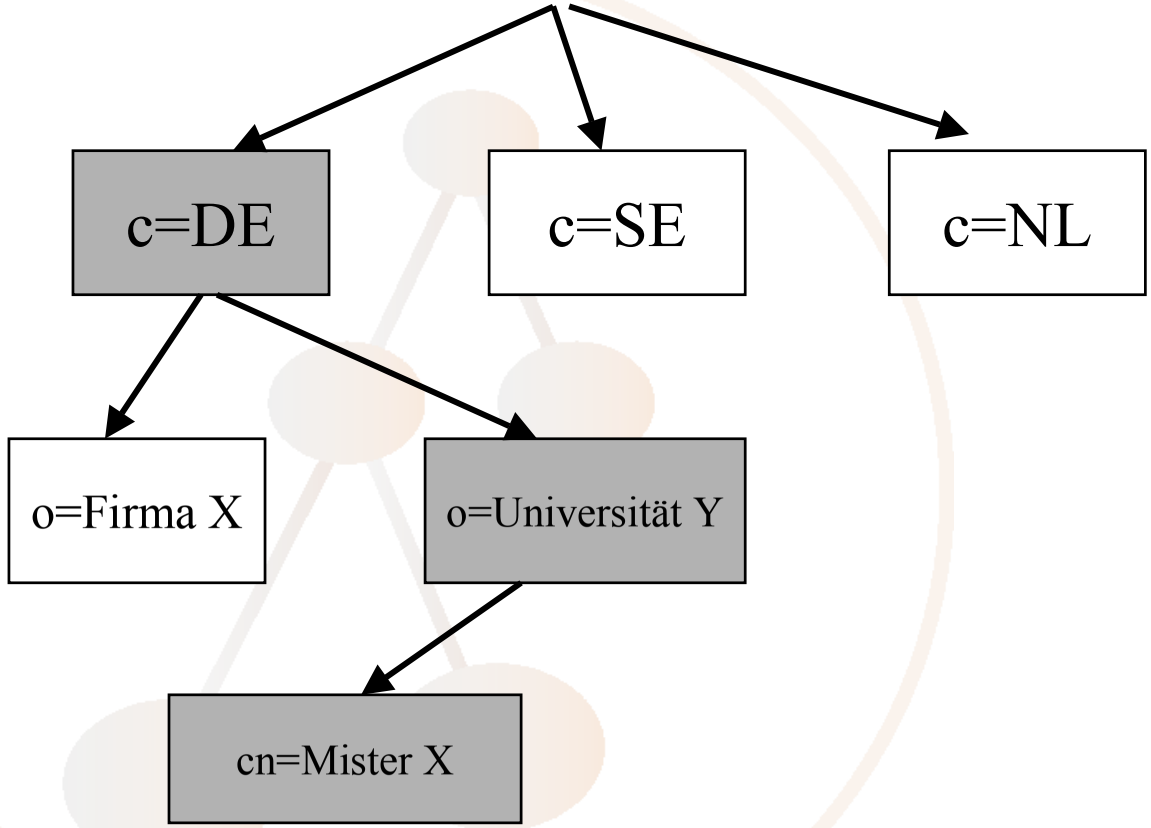
- Daten werden in Einträgen gespeichert
- Einträge werden als Baumknoten gespeichert
  - Jeder Knoten hat 0 bis n Kinderknoten
  - Jeder Knoten hat genau 1 Elternknoten
    - Mit Ausnahme des Wurzelknotens
- Jeder Knoten hat einen eindeutigen Namen
  - RDN (Relative Distinguished Name)
  - DN (Distinguished Name)

DIT, RDN, DN

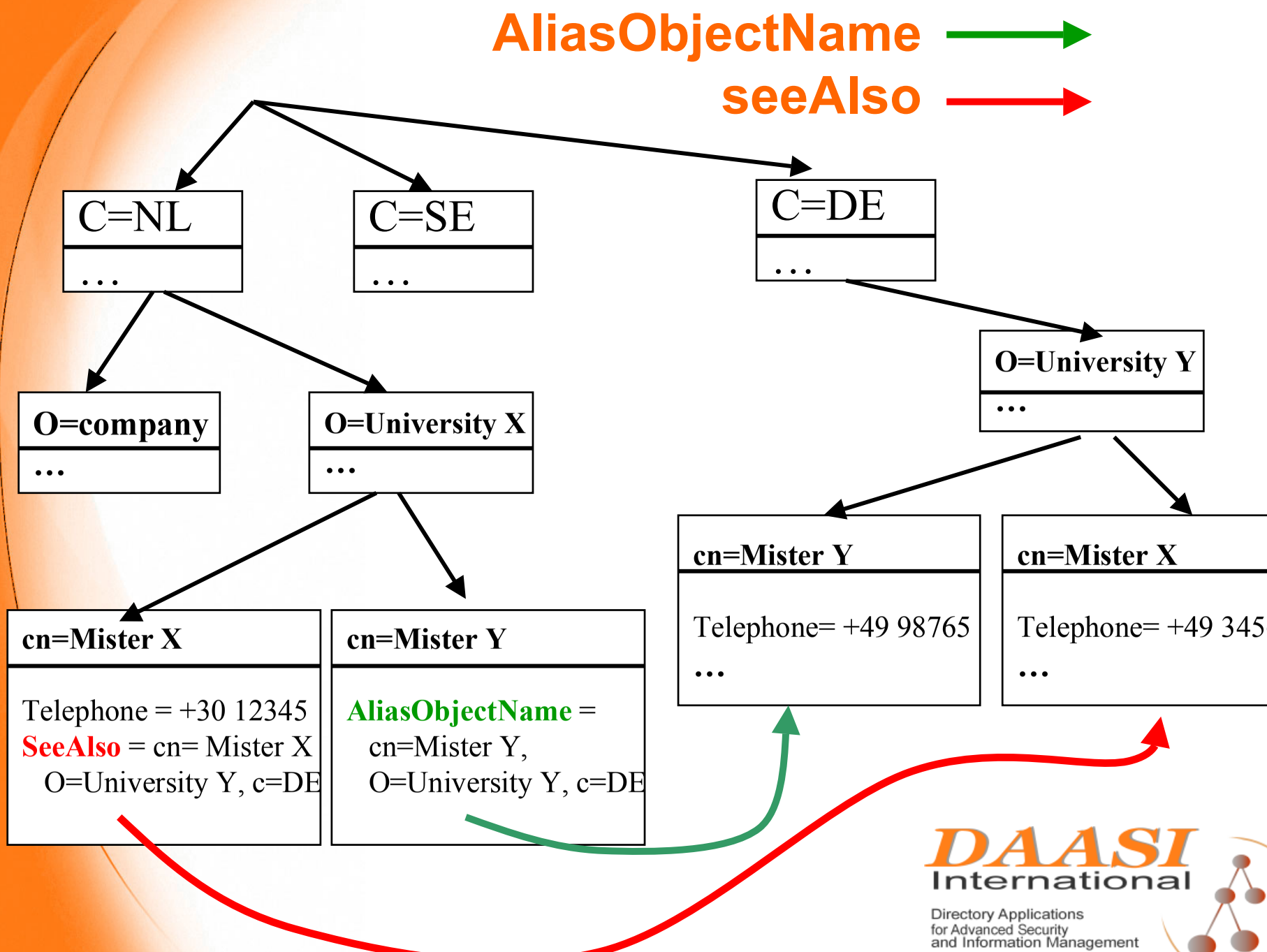
RDN: c=DE
(countryName)

RDN: o=Universität Y
(organizationName)

RDN: cn=Mister X
(commonName)



DN: cn=Mister X, o=Universität Y, c=DE

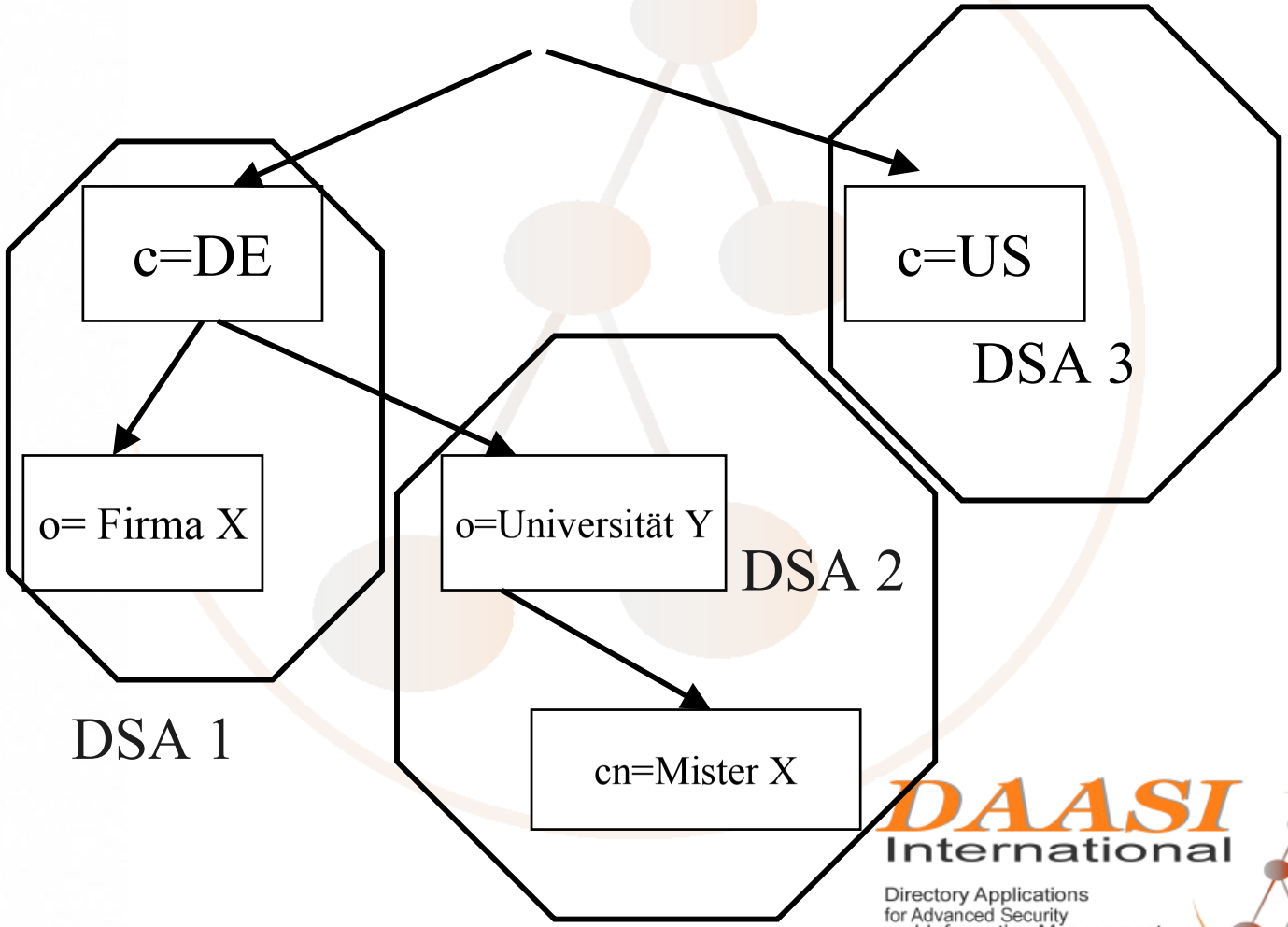


DAASI International

Directory Applications for Advanced Security and Information Management

Verteilung der Daten

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



Funktionsmodell

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

LDAPv3 Standard

- Fertige IETF 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)

LDAP-Server-Implementierungen

- Native LDAP-Server
  - OpenLDAP (Open Source)
  - Netscape Directory Server
  - SUN One Directory Server
  - IBM Secure Way
- X.500(93) Implementierungen
  - Siemens DirX
  - ISODE
- Novell Directory Service (NDS): eDirectory
- Microsoft Active Directory

Clients mit LDAP-Schnittstelle

- Mailagenten (für Emailrecherche)
- Browser (LDAP-URL)
- Verschlüsselungsprogramme
  - S/MIME, PGP
- In vielen Standardimplementierungen berücksichtigt
  - IMAP, SMTP Auth, etc.
  - Apache Webserver
  - ...

Open LDAP

- Open Source Implementierung von LDAPv3
- 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

Vorteile von OpenLDAP

- LDAPv3 Standardkonform
- Stabil und performant
- Verschiedene Datenbank-Backends einsetzbar
- Gute Sicherheitsmechanismen (TLS, etc.)
- Gute Zugriffskontrollmechanismen, z.B. abhängig von:
  - Subtree
  - Einzelnen Attributen
  - Authentifizierungsgrad
  - IP-Adresse
- Stabiler Replikationsmechanismus
  - Auch Teilreplikation möglich

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 gleichen Daten können von verschiedenen Anwendungen verwendet werden
- Es gibt eine stabile Open-Source-Implementierung

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

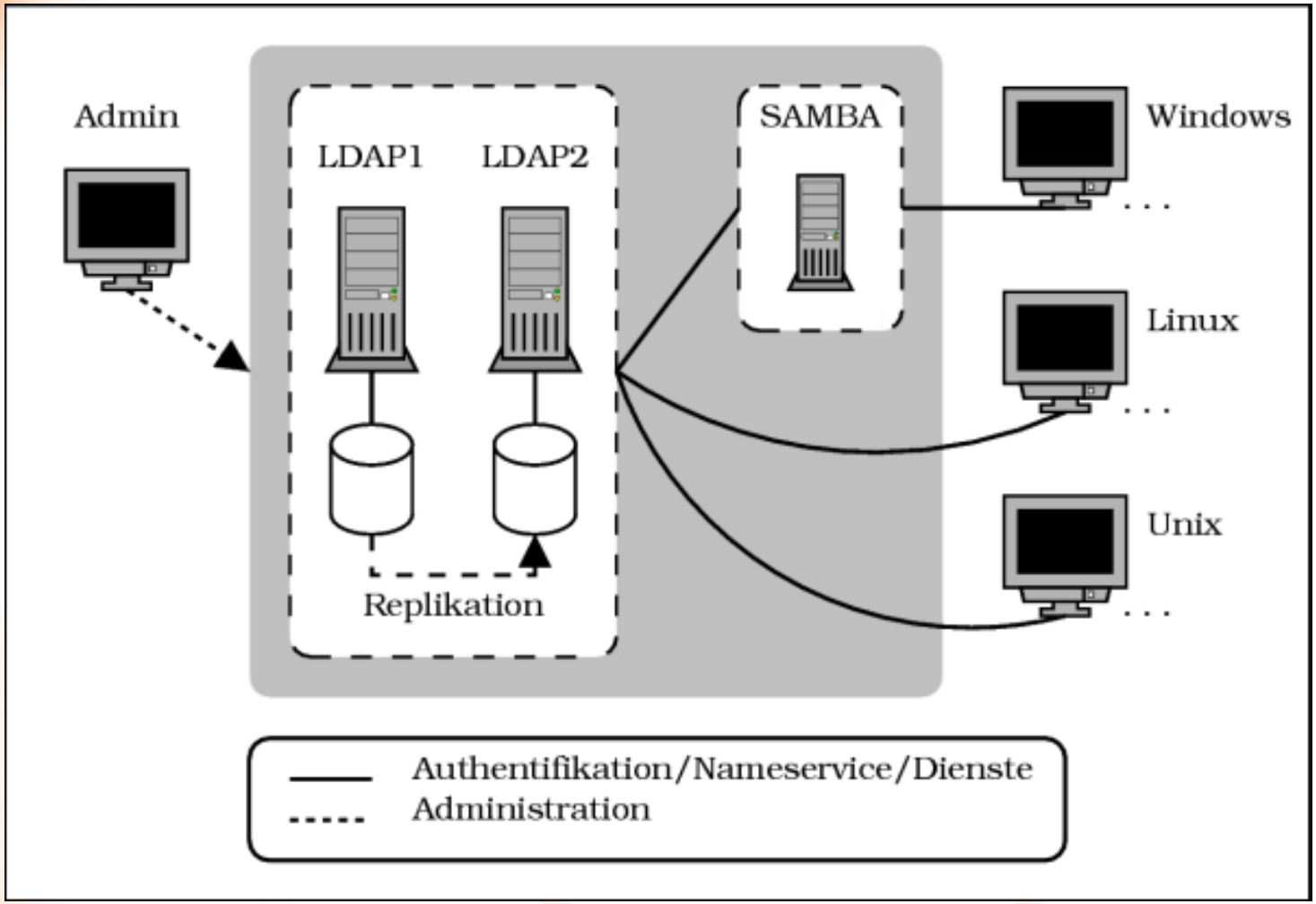
Authentifizierungsdienst

- 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
- Lösung:
  - Unified Login durch zentralen verzeichnisdienst-basierten Authentifizierungsdienst

Zentraler verzeichnisdienstbasierter Authentifizierungsdienst

- Unix-Clients
  - Können mittels NSS / PAM-LDAP direkt auf LDAP-Server zugreifen
  - Kann gecashed werden: nscd (Name Service Caching Daemon)
  - 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
    - NT4 Domäne (Samba 2.x)
    - AD-Simulation (Samba 3.0)

Architektur im Überblick



DAASI International

Directory Applications
for Advanced Security
and Information Management

Single Sign On (SSO)

- 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, SSH, ...
- Viele Produkte bereits „LDAP-Enabeled“
- Wo noch nicht vorhanden, lassen sich LDAP-Schnittstellen einbauen (Voraussetzung: Open Source)
- SSO-Lösung: Unified Login mit OpenLDAP mit Einbindung von Kerberos

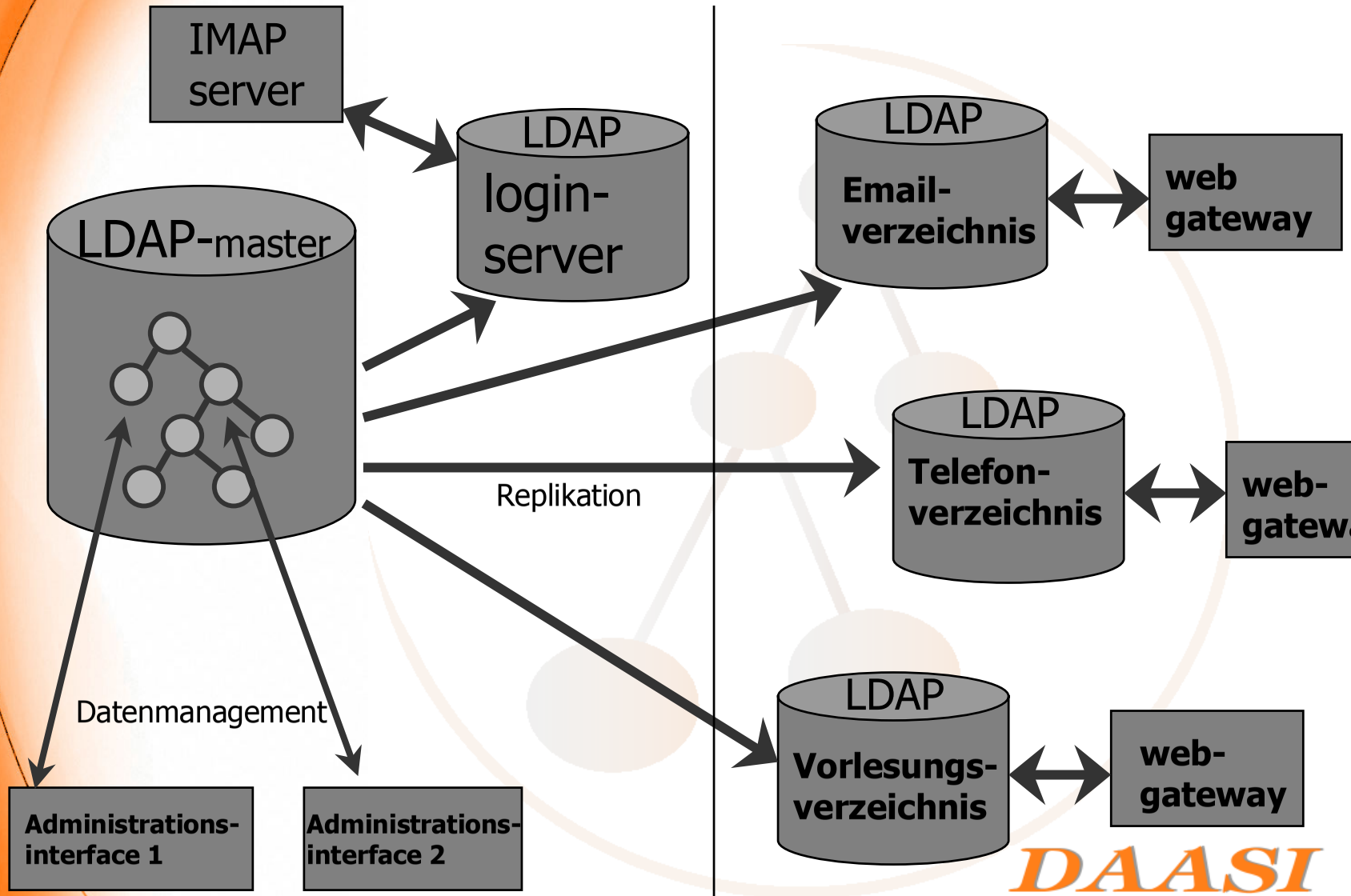
Zusammenfassung Authentifizierungsdienst

- Vorteil: Ein Passwort für alle Rechner
  - Der User muss sich weniger merken
  - Der Administrator und Help Desk wird erheblich entlastet
  - Passwortqualität zentral kontrollierbar
  - Vereinheitlichung der Authentifizierungsschnittstellen
  - Zwingt zu einem Gesamtkonzept
- Nachteil: Ein Passwort für alle Rechner
  - Single point of failure
  - Größerer Schaden bei Kompromittierung

Erweiterbarkeit von Verzeichnisdiensten

- Gleiche Daten - Verschiedene Dienste
  - Z.B.: Eine Datenstruktur, beliebig verteilt und/oder (teil)repliziert für:
    - Emailverzeichnis
    - elektronisches Telefonbuch
    - Benutzerverwaltung und Authentifizierungsdienst
    - Elektronisches Vorlesungsverzeichnis
  - Einfach weitere Objektklassenattribute zum Eintrag hinzufügen und neues Benutzerinterface (z.B. über das WWW) implementieren
  - Dies führt zu erheblichen Kosteneinsparungen

Beispiel für zentrales Verzeichnis



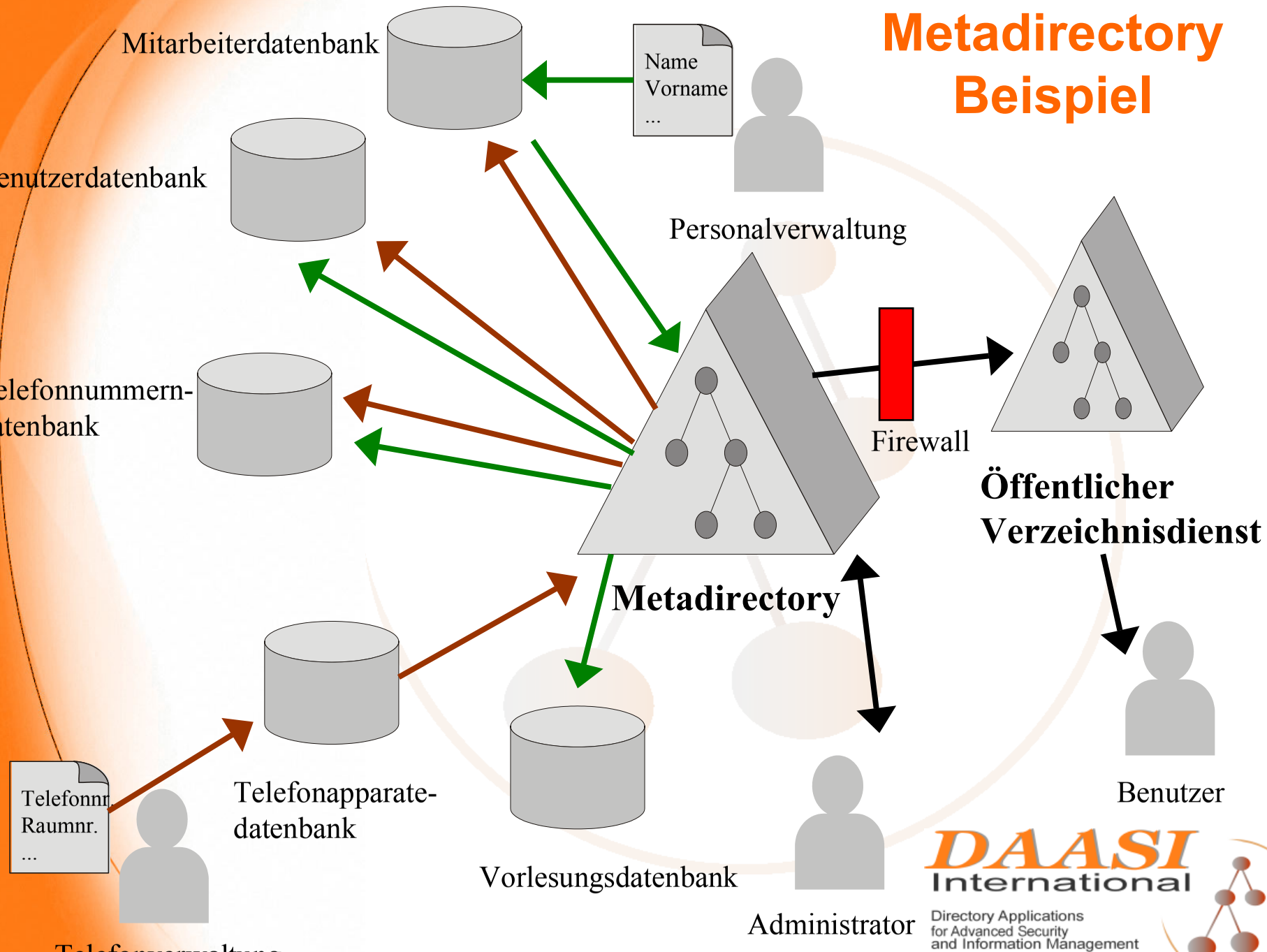
DAASI International

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
- In Planung ist eine ZKI-Arbeitsgruppe zu Metadirectory

DAASI International

Directory Applications
for Advanced Security
and Information Management

Zertifikatsserver für PKI

- Der Verzeichnisdienst
  - hält Zertifikate im Netz vor
  - Ermöglicht Zugriff durch Anwendungen
  - 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

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.
  - LDAP-Datenmodell für Dublin Core
- Schwierige Metadaten sind Verschlagwortungsdaten
  - Wie kann man sicherstellen das selbe Schlagwort für dasselbe Thema zu verwenden?
  - Kontrolliertes Vokabular

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

Ontologien

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

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

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 via Web Services (SOAP, WSDL) beziehen
- Kann auch z.B. zur Erschließung des elektronischen Vorlesungsverzeichnis verwendet werden

Ressourcen-Verwaltung

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

- Auch diese Anwendungen lassen sich in ein zentralen Verzeichnisdienst integrieren

Zusammenfassung

- LDAP-Implementierungen stellen verlässliche und perfomante Lösungen zur Verfügung auch mit
  - Replikation
  - Authentifizierung
  - Granulare Zugriffskontrolle
  - Zugriff über standardisiertes Netzprotokoll
- Verzeichnisdienst kann Basis für verschiedenste Anwendungen sein.
- OpenSource-Lösungen mit Supportvertrag, die preiswertere Alternative

Vielen Dank für Ihre Aufmerksamkeit

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

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

DAASI International

Directory Applications
for Advanced Security
and Information Management