Tutorium
Identity Management

18. DFN-Arbeitstagung über Kommunikationsnetze

Düsseldorf, 1.6.-2.6.2004

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management

i 2004 (c) DAASI International

Agenda Überblick

- Dienstag 1.6.2004
  - 13:15-14:00 1.) Einführung in Identity Management
  - 14:00-14:45 2.) Grundbausteine in Identity Management Systemen
  - 15 Minuten Pause
  - 15:00-17:00 3.) Relevante Technologien
  - 15 Minuten Pause
  - 17:00-17:30 4.) Schemata im Hochschulbereich
- Mittwoch 2.6.2004
  - 09:00-09:45 5.) Produktübersicht Identity Management
  - 09:45-10:30 6.) Identity Management an deutschen Hochschulen
  - 30 Minuten Pause
  - 11:00-12:00 Bericht aus der Praxis (Dr. Christa Radloff, Univ. Rostock)
  - 12:00-12:30 Abschlußdiskussion

DAASI International

Directory Applications for Advanced Security and Information Management

1.) Einführung in Identity Management

- Begriffsdefinitionen
- Problemstellung
- Organisatorische Workflows
- Abbildung in EDV-Prozessen
- Rollen, Gruppen, Berechtigungen, Policy

DAASI International

Directory Applications
for Advanced Security
and Information Management

2.) Grundbausteine in Identity Management Systemen

- Datenbanken vs. Verzeichnisdienste
- Metadirectory vs. Provisioning
- Policy, Passworte, Workflow, Auditing
- Identity Management Architekturen

DAASI International

Directory Applications
for Advanced Security
and Information Management

3.) Relevante Technologien

- Einführung in Verzeichnisdiensttechnologien
  - X.500, LDAP
- Technologien für zentrale Authentifizierungssysteme
  - SASL, GSSAPI, PAM, NSS, RADIUS
  - X.509 PKI
- Föderierte Identitäten und andere Unique Identifiers
  - Passport, Liberty Alliance, URN, OID
- Technologien für Authentifizierung und Autorisierung
  - LDAP, Kerberos, AAA, X.509 PMI,
- Implementierungen für Domainübergreifende AA
  - Permis, Papi, Shibboleth
- XML Standards zu Provisioning und Workflow
  - SAML, XACL, SPML, WfMC, WS-CDL

4.) Schemata im Hochschulbereich

- Einführung in Schema
- X.500/LDAP Schemadefinition
- X.500-Standards
  - Person, organizationalPerson, organization, organizationalUnit
- LDAP-Standards
  - inetOrgPerson, eduPerson, pkiUser, x509PKC, naturalPerson
- Schema-Definitionen in europäischen Forschungsnetzen
- Schema Registry

DAASI International

Directory Applications for Advanced Security and Information Management

5.) Produktübersicht Identity Management

- Schritte vor der Produktwahl
- Kurze Marktübersicht, woher kommen die Player
- Marktstrategien (Entwicklen, Aufkaufen, Partnerschaften)
- Die wichtigsten Produkte:
  - Calendra
  - Computer Associates
  - IBM Tivoli
  - MaxWare
  - Microsoft
  - Novell
  - Siemens
  - Sun

DAASI International

Directory Applications for Advanced Security and Information Management

6.) Identity Management an deutschen Hochschulen

- Organisatorische Probleme
- Kostenfaktoren
- Projektbeispiele
- Projektidee Metadirectory Kompetenzzentrum

DAASI International

Directory Applications
for Advanced Security
and Information Management

DAASI International und deutsche Hochschulen

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

DFN Projekte als Keimzelle von DAASI International

- 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

Projektergebnisse

- AMBIX: Datenschutzkonformes Emailverzeichnis für die Forschung in Deutschland mit Webfrontend
  - Relaunch als EVA-Wiss ab 1. Juli 2004 www.evawiss.de
- IDEV: Index von Personenverzeichnissen an deutschen Hochschulen
- Vergleich verschiedener LDAP-Implementierungen
- Arbeiten zu Verzeichnissen für PGP-Schlüssel und X.509-Zertifikate
- Arbeiten zu zentraler Authentifizierung
  - Zwei Unified Login Lösungen
- Vertretung des DFN in nationalen und internationalen Gremien

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 5 feste und 2 freie Mitarbeiter
- Kooperation mit anderen Firmen und Freelancern für größere Projekte

DAASI International

Directory Applications for Advanced Security and Information Management

Juni 2004 (c) DAASI International

Wofür wir stehen

- Leistungen: Consulting, Implementierung, Hosting, Datenmanagement und –konvertierung, Schulung
- Vorlieben: Offene Standards, Open Source, Datenschutz, Forschung
- Kundenzielgruppen: v.a. Forschungseinrichtungen, Bibliotheken, Behörden, KMUs
- Projekte: TERENA, deutsche Universitäten, DL-Forum, etc.
- Expertise:
  - Verzeichnisdienste, Authentifizierung, PKI, Identity Management, Informationsmanagement, Digital Libraries, XML, Semantic Web, Grid Computing
- Standardisierungsaktivitäten und Verbände:
  - IETF, Internet2, GGF, TERENA, Teletrust AG7 „PKI“, bwconn:boss

DAASI International

Directory Applications for Advanced Security and Information Management

Einführung in Identity Management

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

1.) Einführung in Identity Management

- Begriffsdefinitionen zu Identity Management
- Problemstellung
- Organisatorische Workflows
- Abbildung in EDV-Prozessen
- Rollen, Gruppen, Berechtigungen, Policy

DAASI International

Directory Applications
for Advanced Security
and Information Management

Begriffsdefinitionen zu Identity Management (IdM)

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

Definitionen zu Identity

- www.webster-dictionary.org:
  - *The state or quality of being identical, or the same; sameness.*
  - *„Identity is a relation between our cognitions of a thing, not between things themselves.“ (Sir W. Hamilton)*
- Dictionary.com:
  - *The collective aspect of the set of characteristics by which a thing is definitively recognizable or known.*
  - *The set of behavioral or personal characteristics by which an individual is recognizable as a member of a group.*
- *www.hyperdictionary.com:*
  - *The distinct personality of an individual regarded as a persisting entity*

DAASI International

Directory Applications for Advanced Security and Information Management

Weitere Definition zu Identity

- **www.webopedia.com: Identity in EDV:**
  - ***In computer technology, the unique name of a person, device, or the combination of both that is recognized by a system.***
- **www.atis.org: Identity Authentication:**
  - ***The performance of tests to enable a data processing system to recognize entities.***
- **searchsecurity.techtarget.com: Identity Theft**
  - ***Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials.***

Definition von Identity Management

- **Spencer C. Lee:**
  - ***Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities,attributes, and credentials.***

DAASI International

Directory Applications for Advanced Security and Information Management

Identität in Identity Management

- Wahrgenommene Gleichheit
- Im Zusammenhang mit einer Person, einem Ding oder einem Ort stehende, diese charakterisierenden Attribute: Name, Organisationszugehörigkeit, Email-Adresse, ...
- Eindeutige Kennung, die eine Person gegenüber einem Computersystem identifiziert
  - Z.B. Login-Id, die einen Zusammenhang mit einer Person bedeutet
- Aber auch: Rechte und Berechtigungen, die eine Person hat
- Eine Person kann in verschiedenen Zusammenhängen verschiedene Identitäten haben
  - Unterschiedliche Computersysteme
  - Unterschiedliche Rollen bei einem Computersystem
- Auch andere Entitäten als Personen können in diesem Sinn Identitäten sein, z.B. Computerprogramme, Computer, etc.
- Identitäten können gestohlen werden!

DAASI International

Directory Applications for Advanced Security and Information Management

Was soll Identity Management?

- Personen wollen:
  - Informationen über sich veröffentlichen, um z.B. kontaktiert werden zu können
  - Informationen über andere Personen erhalten
  - Sich authentifizieren, also ihre Identität beweisen, um Ressourcen und Dienste in Anspruch nehmen zu können
  - Im Netz bezahlen
- Organisationen wollen
  - Identitätsinformationen über Mitarbeiter oder Mitglieder verwalten
  - Benutzer ihrer Ressourcen verwalten
  - Konsistenz der Identitäten in verschiedenen Informationsspeicher erreichen
  - Vortäuschung falscher Identitäten verhindern
- Mobilität erhöht die Anforderungen an Identity Management

Definitionen von Provisioning?

- **www.webster-dictionary.org:**
  - ***The act of providing, or making previous preparation.***
  - ***To supply with food***
  - ***That which is stipulated in advance; a condition; a previous agreement;***
- ***www.atis.org:***
  - ***In telecommunications, the setting in place and configuring of the hardware and software required to activate a telecommunications service for a customer; in many cases the hardware and software may already be in place and provisioning entails only configuration tasks such as creating (or modifying) a customer record in a database and associating it with the service(s) and service level for which the customer has subscribed.***
- ***www.webopadiea.com:***
  - ***The process of providing users with access to data and technology resources.***

DAASI International

Directory Applications for Advanced Security and Information Management

Was ist Provisioning also?

- Der Prozess durch den ein Benutzer Zugang zu einer Ressource bekommt
  - Beteiligt an diesem Prozess in der Regel: HR und IT
  - Benutzer wird über eine Identität spezifiziert
  - Ressourcen sind z.B.: Datenbanken, Anwendungen, Rechner, Telefonapparate
  - Der Prozess impliziert, dass Zugriffsrechte und Privilegien überwacht werden
- Der Prozess durch den ein Benutzer einen Account bekommt, auf diesen zugreifen kann und alle Rechte dieses Accounts genießt

Was ist eine Rolle?

- **Dictionary.com:**
  - *1.) A character or part played by a performer.*
  - *2.) The characteristic and expected social behavior of an individual.*
  - *3.) A function or position.*
- **WordNet:**
  - *the actions and activities assigned to or required or expected of a person or group*

DAASI International

Directory Applications for Advanced Security and Information Management

Was ist eine Gruppe?

- **www.webster-dictionary.org:**
  - ***A cluster, crowd, or throng; an assemblage, either of persons or things, collected without any regular form or arrangement;***
- **WordNet:**
  - ***1.) any number of entities (members) considered as a unit***
  - ***2.) a set that is closed, associative, has an identity element and every element has an inverse***

Rolle vs. Gruppe

- Rolle
  - ist eine Eigenschaft, die bestimmte Verhaltensregeln und –weisen bestimmt, sowie mit bestimmten Rechten und Pflichten zusammenhängt. Beispiel: „Professor“
  - Kann hierarchisch strukturiert sein, z.B. Mitarbeiter -> Professor
- Gruppe
  - ist viel allgemeiner gefasst. Die Übereinstimmung nur eines beliebigen Merkmals reicht aus um eine Gruppe zu definieren. Beispiel: „Interessent an Mailingliste X“
  - Gruppe kann auch durch Ausschluss gebildet werden, z.B. alle nichtpromovierten Dozenten.

Problemstellung

Prozesse

- Personen
  - Werden in Organisationen aufgenommen
  - Erhalten Rollen und Berechtigungen
  - Agieren in ihrer Rolle
  - Wechseln Rollen und Berechtigungen
  - Verlassen die Organisation
- Organisationen bzw. Organisationseinheiten
  - Werden gegründet
  - Agieren in Arbeitsprozessen
  - Werden zusammengefügt (merge)
  - Werden aufgeteilt (split)
  - Werden aufgelöst
- Außenstehende wollen Kontaktinformationen

Ausgangsposition vor Identity Management

- Isolierte, voneinander unabhängige Verzeichnisse/Datenbanken mit den gleichen Identitätsdaten, die nicht miteinander interagieren und zwischen denen kein Vertrauen bezüglich der Richtigkeit der Daten besteht
- Jede dieser Datensammlungen hat eigene Administratoren, Benutzerverwaltungen und Zugriffskontrollmechanismen
- Redundanz der Daten und der Datenpflege, Mehrfacharbeit
- Historisch gewachsene Infrastrukturen und Prozesse
- Zunehmender Erwartungsdruck der Mitarbeiter und Kunden (Studierende)

DAASI International

Directory Applications for Advanced Security and Information Management

Probleme bei nicht vorhandem IdM

- Benutzer brauchen Login-Accounts für jeden Computer und jede Anwendung und müssen sich viele Passwörter merken
- Administratoren verwenden verschiedene Tools, haben verschiedene Regeln und Prozesse für die Daten
- verschiedene Authentifizierungsmechanismen
- Jede neue Anwendung vergrößert den Leidensdruck
- Prozesse sind langsam
- Identitätsinformationen sind in verschiedenen Datensammlungen unterschiedlich (Meyer vs. Meier)
- Unterschiedliche Identitätsinformationen werden gesammelt (unterschiedliche Datenschemata)

DAASI International

Directory Applications for Advanced Security and Information Management

Noch mehr Probleme

- Benutzer bekommen zu spät Zugriff auf Ressourcen
- Helpdesk wird überlastet durch das „Passwort-Vergessen-Syndrom“
- Zugriffskontrollen werden falsch gesetzt. Das Berichtigen ist wegen Kommunikation mit anderen Administratoren aufwendig
- Nach Weggang des Mitarbeiters werden nicht alle Accounts und Berechtigungen gelöscht
- Sicherheit ist oft nicht gegeben

Ein Paar Zahlen der META Group*1

- Bei Unternehmen mit über $500 Millionen Umsatz*2:
  - Sind 45% der Help-Desk-Aktivitäten besteht aus dem Rücksetzen von Passwörtern
  - Haben 11% der Mitarbeiter mindestens ein Zugriffsrechte-Problem pro Monat
  - Dauern Provisioning-Vorgänge zwischen 6 und 29 Stunden
  - Wird interne Benutzerinformation an 22 verschiedenen Orten gespeichert

*1: Meta Group: The Value of Identity Management
*2: entspricht in der Benutzerzahl einer größeren Universität

Noch mehr Zahlen der Meta Group

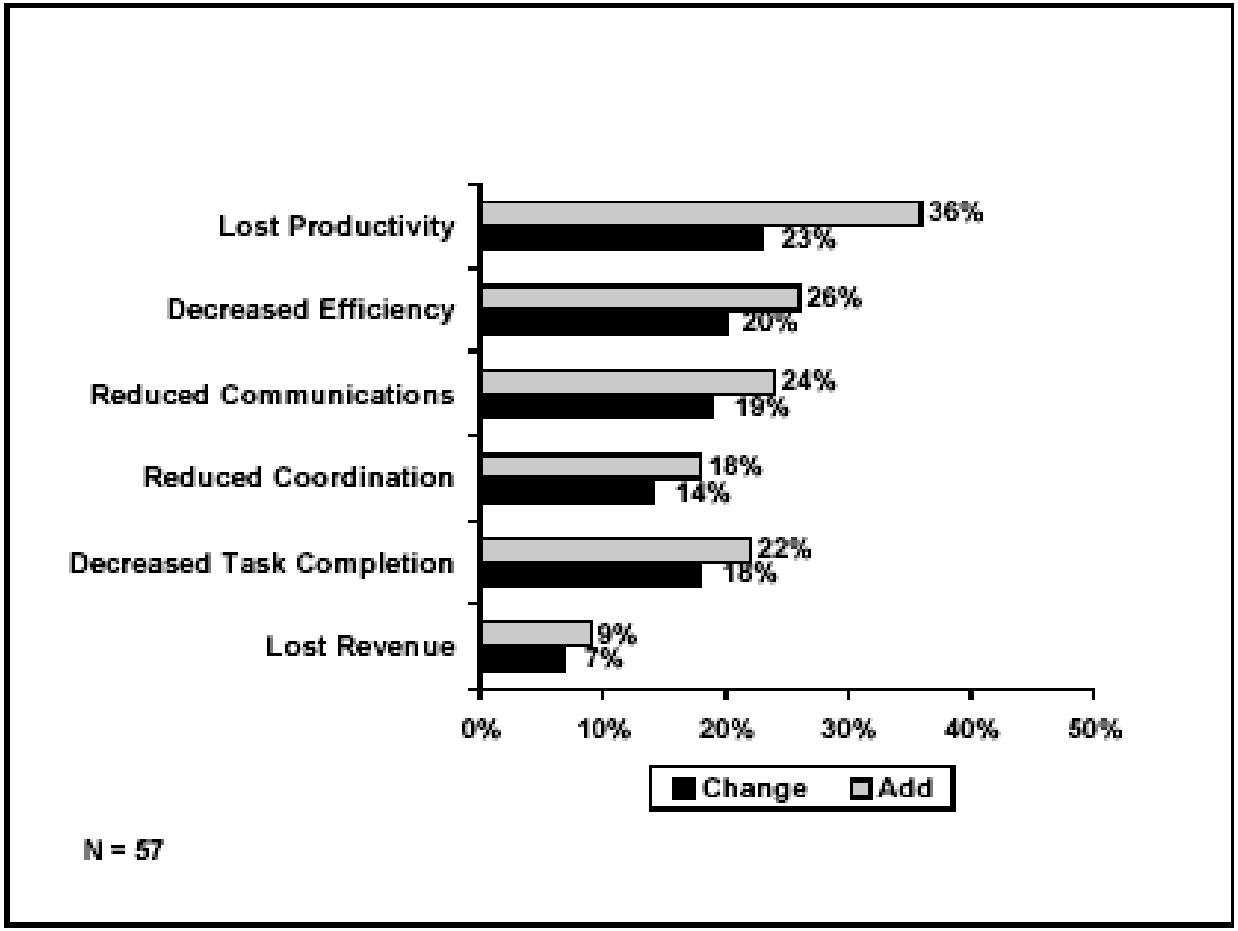


Figure 3 – Impacts of a non-optimized user provisioning process

DAASI International

Directory Applications
for Advanced Security
and Information Management

Organisatorische Workflows

DAASI International
Directory Applications
for Advanced Security
and Information Management

Typische Beteiligte am Workflow in Universitäten

- HR bzw. Studentenverwaltung ist meist erste Anlaufstelle
- RZ (Systemverwaltung, Email-Account, Printing, etc.)
- UB (Benutzer-account)
- Technisches Betriebsamt (Telefonverwaltung)
- Pressestelle (Mitarbeiterverzeichnis, Vorlesungsverzeichnis)
- Postversandstelle (Adressenverwaltung)
- Verein der Freunde der Universität (Alumni-Verwaltung)
- ...

DAASI International

Directory Applications for Advanced Security and Information Management

Was geschieht bei der Neueinstellung genau?

- Arbeitsvertrag und Eingangsformular geht an HR
- Mitarbeiter füllt für verschiedene Dienste am RZ (Email, Rechneraccount, ...) verschiedene Formulare aus
- Mitarbeiter füllt ein weiteres Formular in der UB aus
- Mitarbeiter beantragt ein Telefon
- Mitarbeiter wird in verschiedenen Verzeichnissen aufgenommen
- ...
- Weitere Prozesse werden beim Wechsel des Namens, Wohnorts, Arbeitsplatzes, Arbeitsvertrag, sowie bei der Beendigung des Arbeitsverhältnisses

DAASI International

Directory Applications for Advanced Security and Information Management

Datenverwaltung an Hochschulen

- von der Personalverwaltung in einer Mitarbeiter-Datenbank, für z.B. Lohnbuchhaltung und Abrechnung der Urlaubstage
- von der Systemadministration in einer Benutzerdatenbank, für z.B. Login- und Email-Accounts und für Mailinglisten
- von der Verwaltung in einer Telefondatenbank, z.B. für die Erstellung eines gedruckten und/oder elektronischen Telefonbuchs
- vom technischen Bettriebsamt, z.B. für die Verwaltung von Telefonapparaten und –anschlüssen
- vom Presseamt, z.B. für die Erstellung eines gedruckten/elektronischen Vorlesungsverzeichnisses und für Adressenlisten für postalischen Versand von Mitteilungen etc.

Ausgangssituation: Worst Case Scenario

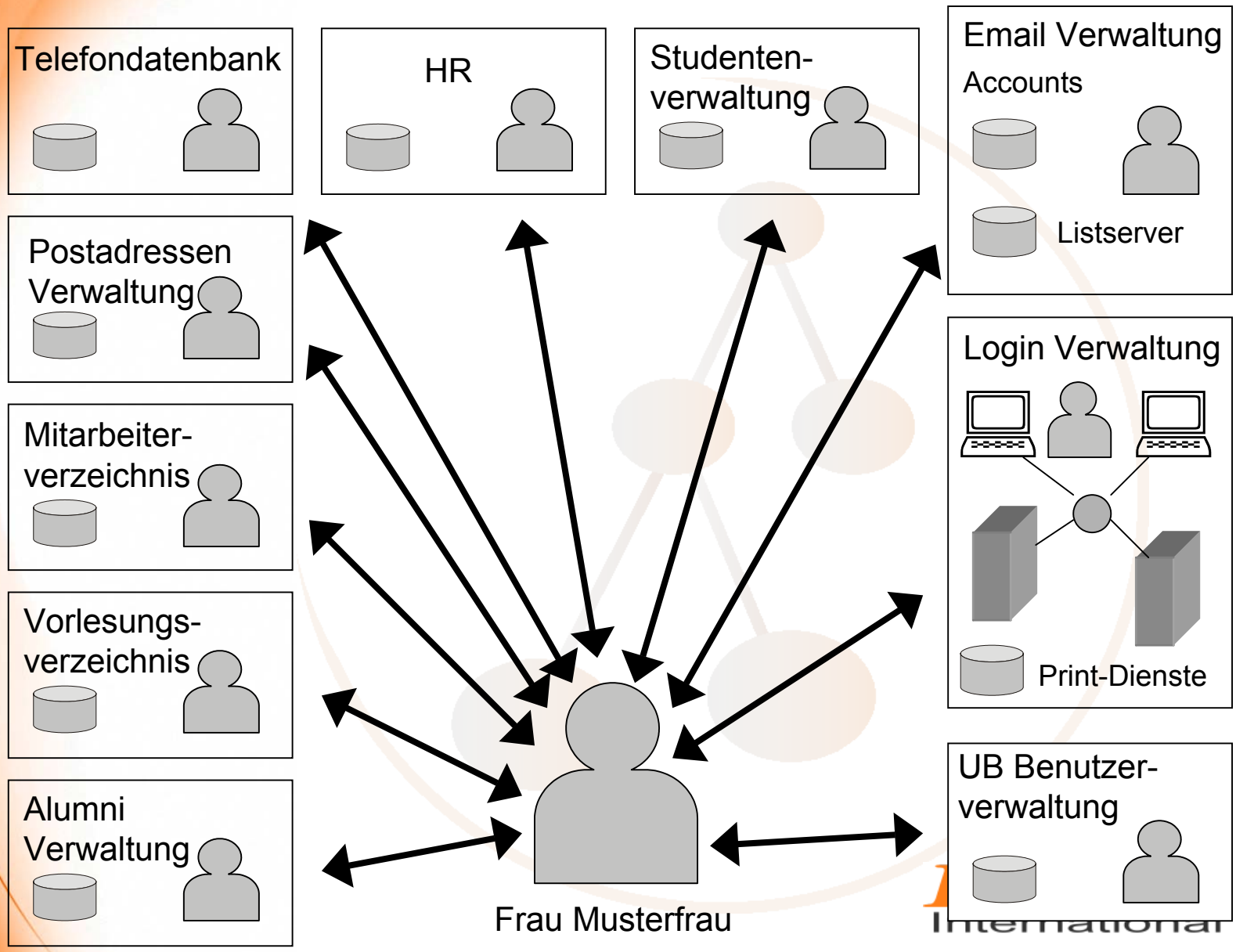


Abbildung in EDV-Prozessen

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

Abbildung der Prozesse im Identity Management

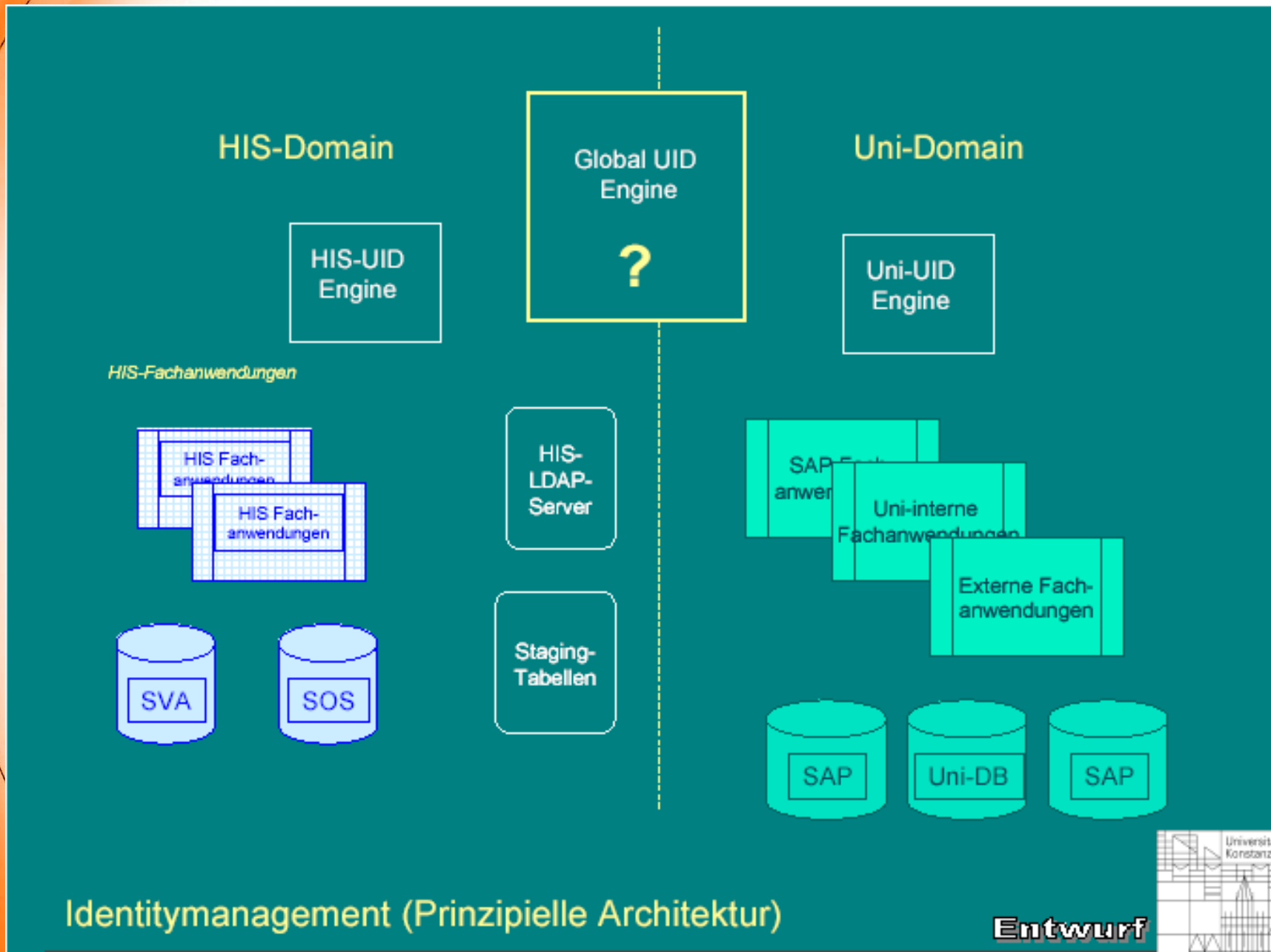
- Identitäten: erzeugen
- Identitätsinformationen aktualisieren
- Identitäten löschen
- Identitäten archivieren
- Identitätsinformation anfordern und anzeigen
- Identitäten verifizieren
- Mit Identitäten signieren (PKI)
- Zugriffskontrollregeln durchsetzen (Lese- und Schreibrechte)
- Datenbanken für Identitäten aufbauen und pflegen
- Identitätsdatenbanken synchronisieren
- Identitätsdatenbanken aufteilen und zusammenführen

Nach: The Open Group: Business Scenario: Identity Management, 15. July 2002, www.opengroup.org

Was gehört zu Identity Management?

- Passwort-Verwaltung und –Synchronisierung
- Identitätszertifizierung mit Public Key Infrastructure
- Externe Identitätsdienste (MS Passport, Liberty Alliance)
- Single Sign On Mechanismen
- Rollenkonzepte und Berechtigungen
- Verwaltung des Zugriffs auf Ressourcen
- Authentifizierung und Autorisierung
- Verzeichnisdienste können genutzt werden zur Speicherung von Identitätsinformation, Passwörtern, Zertifikaten, Rollen und Berechtigungen, Policy
- Metadirectories dienen zur Synchronisierung verschiedener Datenspeicher und Vermeidung von Inkonsistenzen
- Provisioning Systeme verwalten Berechtigungen und versorgen Anwendungen mit Identitätsinformation

Identity-DBs an Universitäten



Rollen, Gruppen, Berechtigungen, Policy

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

Vorteile eines Rollenkonzepts

- Identitäten werden Berechtigungen zugeordnet, z.B.:
  - Id1 darf Dienst 1 benutzen
  - Id2 darf Dienst 1 und 2 benutzen
  - ...
  - Id12345 darf Dienst 9 benutzen
- Berechtigungen für jede Identität zu verwalten erzeugt hohen Aufwand
- RBAC: Role Based Access Control
- Mit Rollen kann die Anzahl der Berechtigungsregeln erheblich reduziert werden:
  - Rolle1 (MitarbeiterIn) darf xxx und yyy
  - Rolle 2 (StudentIn) darf zzz
  - Id1-150 haben Rolle 1
  - Id100-12345 haben Rolle 2

DAASI International

Directory Applications for Advanced Security and Information Management

Vorteile von Gruppen

- Verschiedene Möglichkeiten Gruppen zu definieren:
  - Statische Gruppen: Ein Gruppeneintrag enthält Verweise auf die Mitglieder der Gruppe
  - Halbdynamische Gruppen: Mitgliedseinträge enthalten Verweis auf Gruppeneintrag
  - Dynamische Gruppen: Filter Definiert Gruppenzugehörigkeit
- Gruppen und Rollen lassen sich beide parallel in Verzeichnisdiensten verwenden
- Gruppen können z.B. Unixbenutzer, Windowsbenutzer, etc. sein.

DAASI International

Directory Applications for Advanced Security and Information Management

Stolpersteine bei Rollen

- Man sollte nicht zu viele verschiedene Rollen definieren
- Sonst ist der Hauptvorteil des Rollenkonzepts vertan
- Rolle und Rollenbindung sollten voneinander getrennt werden
  - Besser Entität <-> Rollenbindung <-> Rolle

DAASI International

Directory Applications for Advanced Security and Information Management

Berechtigungen

- Können einem einzelnen Eintrag vergeben werden
- Können einer Gruppe vergeben werden
- Können einer Rolle vergeben werden
- Anwendungen können, wenn sie entsprechend „LDAP-enabled“ sind, ohne Provisioning Authentifizierung und Berechtigunsprüfungen durchführen
- Provisioning-System kann auf im Verzeichnis gespeicherte Gruppen- und Rolleninformation zugreifen
- Zugriffskontrollmechanismen können zur Gruppenbildung verwendet werden

DAASI International

Directory Applications for Advanced Security and Information Management

Von Identität zu Authorisierung

Systems of record

Identify

Persons

Who have

Affiliations / Attributes

That are mapped to

Entitlements

That determine eligibility for

Services

That are offered by

Service Providers

Aus: Keith Hazelton, Univ. of Wisconsin-Madison:

Directory based Middleware Services, Internet2 Advanced CAMP, Boulder Colorado, 31-Jul-02

DAASI International

Directory Applications for Advanced Security and Information Management

Grundbausteine in Identity Management Systemen

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

2.) Grundbausteine in Identity Management Systemen

- Datenbanken vs. Verzeichnisdienste
- Metadirectory vs. Provisioning
- Policy, Passworte, Workflow, Auditing
- Identity Management Architekturen

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

Datenbanken

- Die meisten Anwendungen und Identitätsdatenspeicher bzw. Benutzerverwaltungen basieren auf relationalen Datenbanken
- Es gibt keine standardisierten Tabellenschemata
- Entitätsinformationen werden auf verschiedene Tabellen aufgeteilt
- Mehrfachwerte erzwingen eine neue Tabelle
- Begrenzte Anzahl von Datentypen
- Vergleichsregeln sind nicht Teil des Datenmodells
- Änderungen des Datenschemas schwer möglich
- Netzzugriff ursprünglich nicht vorgesehen

Verzeichnisdienste

- Mitarbeiterverzeichnisse und Authentifizierungssysteme basieren bereits meist auf LDAP
- Es gibt standardisierte Datenschemata
- Entitätsinformationen bleiben an einem Platz
- Mehrfachwerte sind unproblematisch
- Unbegrenzte Anzahl von Datentypen
- Vergleichsregeln sind Teil des Datenmodells
- Änderungen des Datenschemas einfach möglich (Lego-Prinzip)
- Netzzugriff von vorneherein vorgesehen:
  - Datenreplikation und Datenverteilung über das Netz

DAASI International

Directory Applications for Advanced Security and Information Management

Zentraler Verzeichnisdienst

- Konsolidierung durch Migration einzelner Anwendung auf Verzeichnis-Datenbasis
- Verschiedene Daten können in verschiedene Verzeichnisdienste repliziert werden

DAASI International

Directory Applications
for Advanced Security
and Information Management

Erweiterbarkeit von Verzeichnisdiensten

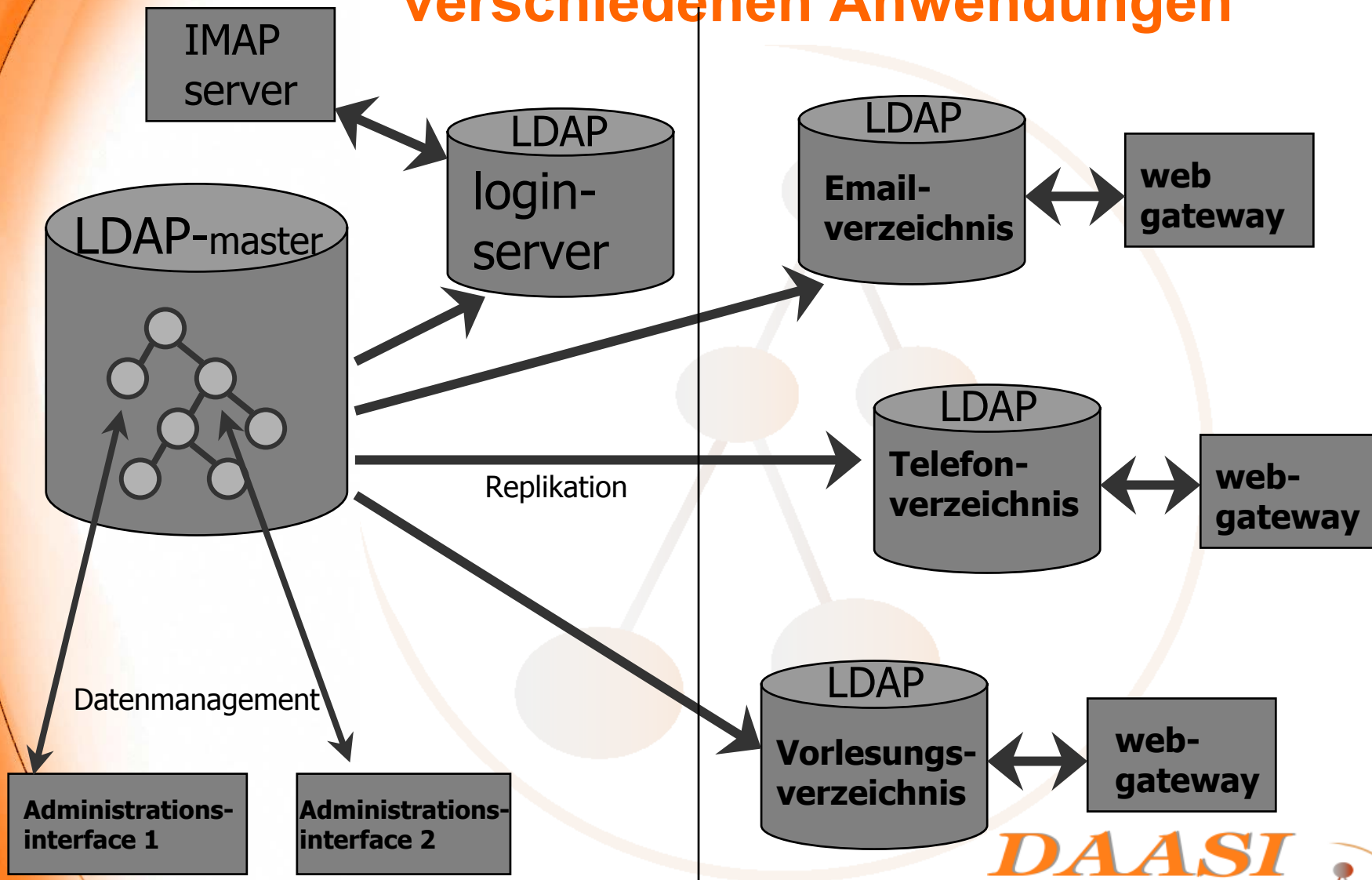
- Gleiche Daten - Verschiedene Dienste
  - Z.B.: Eine Datenstruktur, beliebig verteilt und/oder (teil)repliziert für:
    - Emailverzeichnis
    - elektronisches Telefonbuch
    - Benutzerverwaltung und Authentifizierungsdienst
    - Elektronisches Vorlesungsverzeichnis
  - Einfach weitere Objektklassenattribute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

DAASI International

Directory Applications for Advanced Security and Information Management

1. Juni 2004 (c) DAASI International

Beispiel für zentrales Verzeichnis mit verschiedenen Anwendungen



DAASI International

Directory Applications for Advanced Security and Information Management

Metadirectory – die realistischere Alternative?

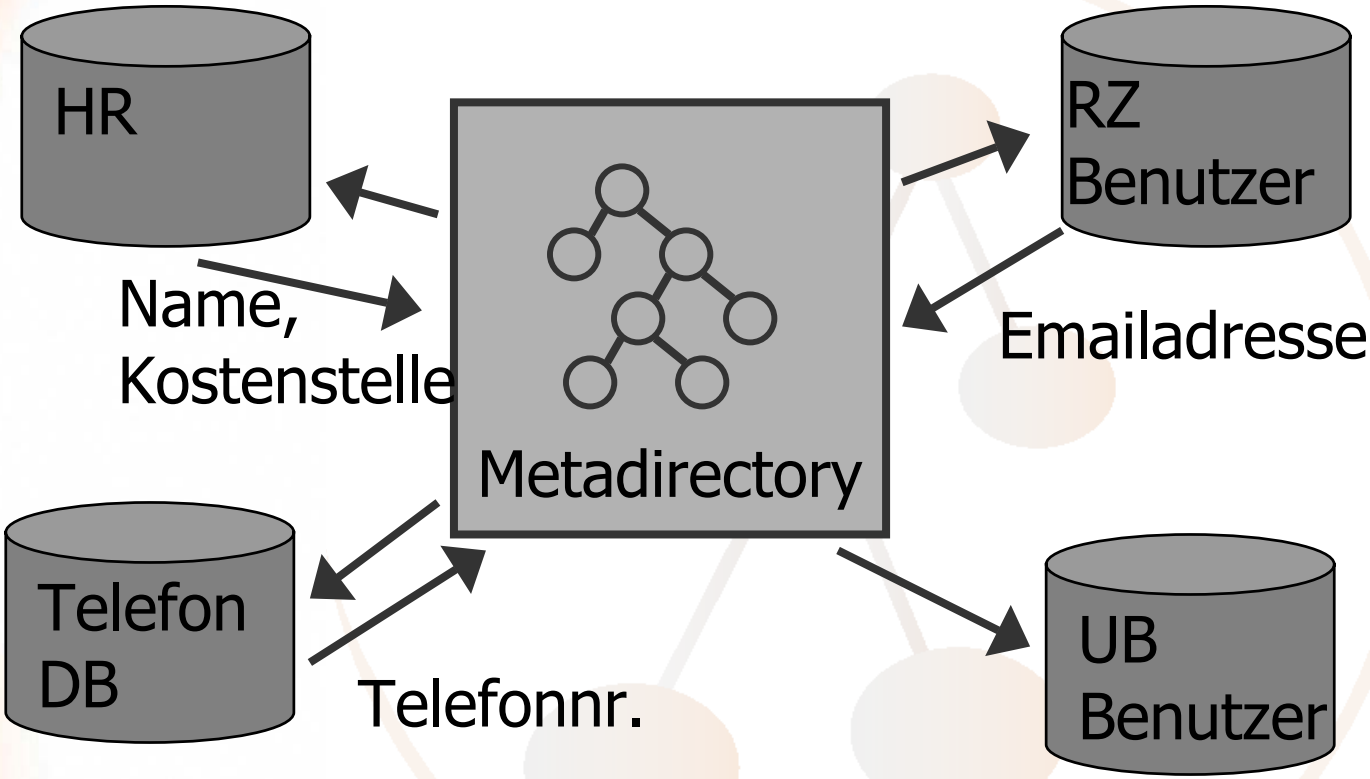
- Verknüpfung verschiedener Datenbanken, die verwandte Daten enthalten, z.B.:
  - Emailbenutzerdatenbank
  - Personaldatenbank
  - Telefondatenbank
- Die gleichen Daten müssen nur einmal eingegeben, bzw. gepflegt werden
- In den verknüpften Datenbanken werden sie automatisch angelegt bzw. geändert
-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

DAASI International

Directory Applications for Advanced Security and Information Management

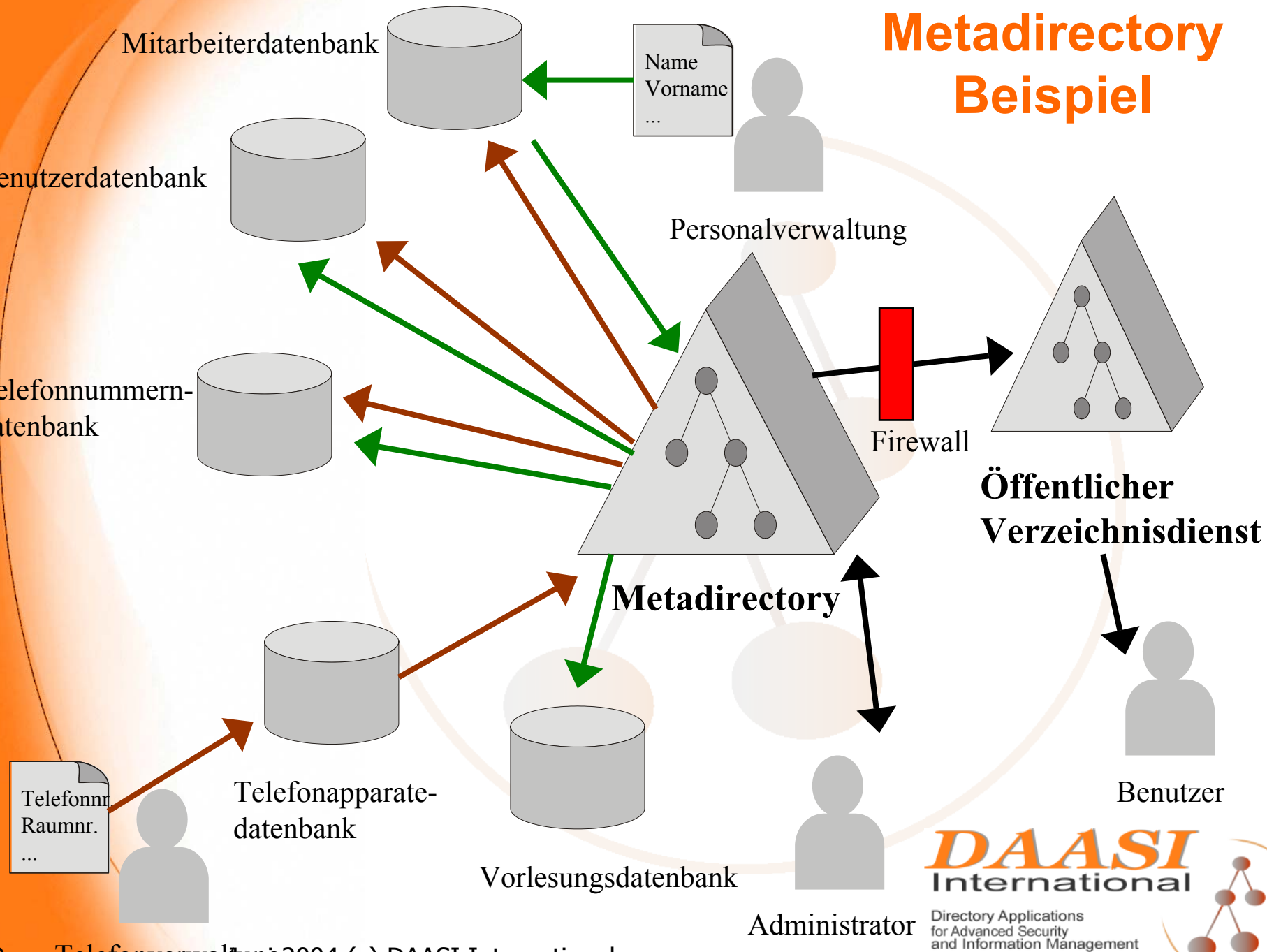
Juni 2004 (c) DAASI International

Metadirectory-Beispiel einer Universität



DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory Beispiel



DAASI International
Directory Applications for Advanced Security and Information Management

Provisioning

- Versorgt Anwendungen mit Identitäts-Informationen
- Benötigt eine zentrale authoritative Quelle für Identitätsinformation
- Beinhaltet ein Work-Flow Management
- Kann die Rechtevergabe beinhalten (Policy Management)
- Sollte eine Audit-Funktionalität haben
- Beinhaltet Passwort-Synchronisation
- Kann Alternative zu Metadirectory sein (vorausgesetzt es gibt eine andere autoritative Quelle für Identitätsinformation)

Metadirectory/Virtual Directory/Provisioning

- Metadirectory
  - Aus Datenbanken synchronisierte Daten werden redundant gespeichert
  - Konnektoren sorgen für Synchronisierung mit den Datenbanken in beide Richtungen
- Virtual Directory
  - Nur eine Sicht auf Daten der Datenbanken
  - Keine redundante Speicherung
  - Konnektoren sorgen für die Darstellung der Daten on the fly
- Provisioning
  - Letzlich nichts anderes als Konnektoren in Richtung der Datenbanken

Policy, Passworte, Workflow, Auditing

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

Policy Management

- Oberfläche zur Verwaltung von Berechtigungen
- Kann Access Control konfigurieren
- Kann unabhängig von den Daten spezifiziert werden
- Kann zusätzliche Parameter spezifizieren, die das Verhalten bei Rollen und Gruppen verändern
  - Kontexte
  - Login-Zeiten
  - Andere Voraussetzungen

Work Flow Management

- Spezifiziert die Abläufe bei Neueinstellung, Datenänderungen und Aufhebung des Beschäftigungsverhältnisses.
- Kann flexibel neue neue Anwendungen integrieren
- Spezifiziert genau welche Attribute von wo nach wo fließen sollen
- Legt per Attribut die autoritative Datenquelle fest
- Es werden mittlerweile verschiedene Workflow-Beschreibungssprachen standardisiert für Interoperabilität zwischen verschiedenen Workflow-Managementsystemen
  - Wf-XML (WfMC)
  - WS-CML (W3C)

DAASI International

Directory Applications for Advanced Security and Information Management

Passwort Management

- Auch bei gleichem Passwort müssen die Passwörter oft redundant gespeichert werden wegen verschiedenen Verschlüsselungs- bzw. Hash-Algorithmen
- Problematisch sind hierbei insbesondere Windows-Passwörter, sowie Lotus Notes

Zwei Architekturen beim Passwort Management

- Zentrales Zurücksetzen des Passworts
  - Z.B. über ein Web-Interface.
  - Die Passwörter müssen nur in eine Richtung (jeweils richtig verschlüsselt) synchronisiert werden
  - Lokale Passwortänderungen müssen verhindert werden
- Dezentrale Passwort-Synchronisierung
  - Z.B. Passwortänderungen sowohl an der Windows-Domäne, als auch im Unix-Rechner möglich.
  - Komplexer und mögliche Sicherheitslöcher, da Passwort unverschlüsselt über das Netz muss
  - Bequemer für den Benutzer

Auditing

- Loggen aller Provisioning-Transaktionen in einer getrennten Datenbank
- Lässt jede Änderung der Account-Daten und Berechtigungen verfolgen
- Lässt Einbruchsversuche verfolgen

DAASI International

Directory Applications
for Advanced Security
and Information Management

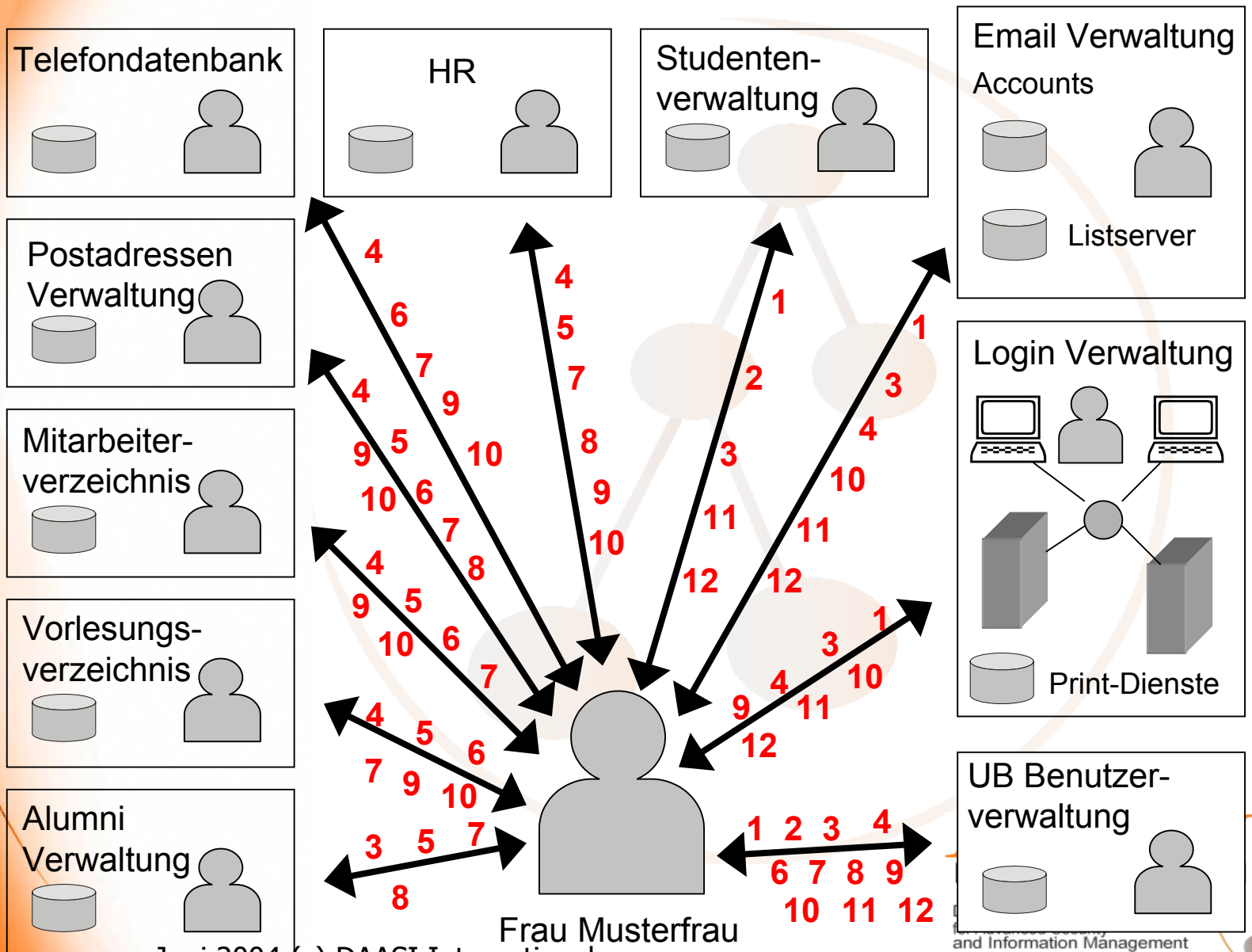
Verschiedene Architekturen

DAASI International
Directory Applications
for Advanced Security
and Information Management

Prozesse (für Worst Case Scenario)

- 1 Immatrikulation
- 2 Studienfachwechsel
- 3 Abschluss / Wechsel der Universität
- 4 Einstellung als Dozent
- 5 Promotion
- 6 Wechsel der Büroräume
- 7 Namensänderung (z. B. Heirat)
- 8 Änderung des Wohnorts
- 9 Änderung des Arbeitsvertrags
- 10 Beendigung des Arbeitsverhältnisses
- 11 Immatrikulation als Gasthörer / Seniorenstudium
- 12 Exmatrikulation

Worst Case Scenario: Interaktionen



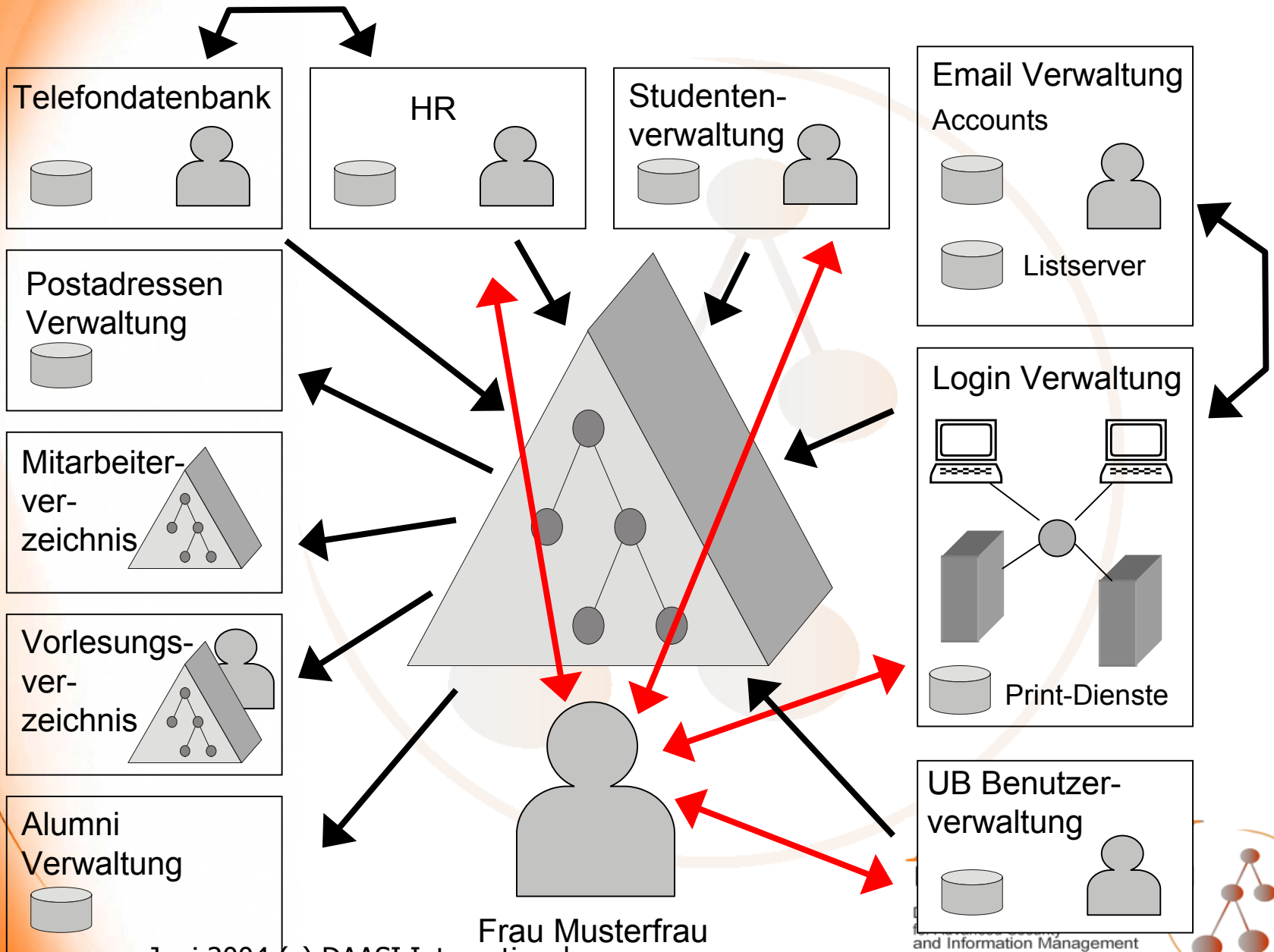
Ergebnis des Worst Case Scenario

- Frau Musterfrau hat:
  - 63 mal Formulare ausgefüllt
  - und ist mit 10 verschiedenen Verwaltungsmitarbeitern in Kontakt getreten.
  - Ihre persönlichen Daten werden in 15 verschiedenen Datenbanken vorgehalten.
- Es warten schon weitere Benutzerverwaltungen:
  - Grid Computing Services
  - Kommunikationsplattformen
  - Voice over IP
  - Portalbenutzer
  - PKI

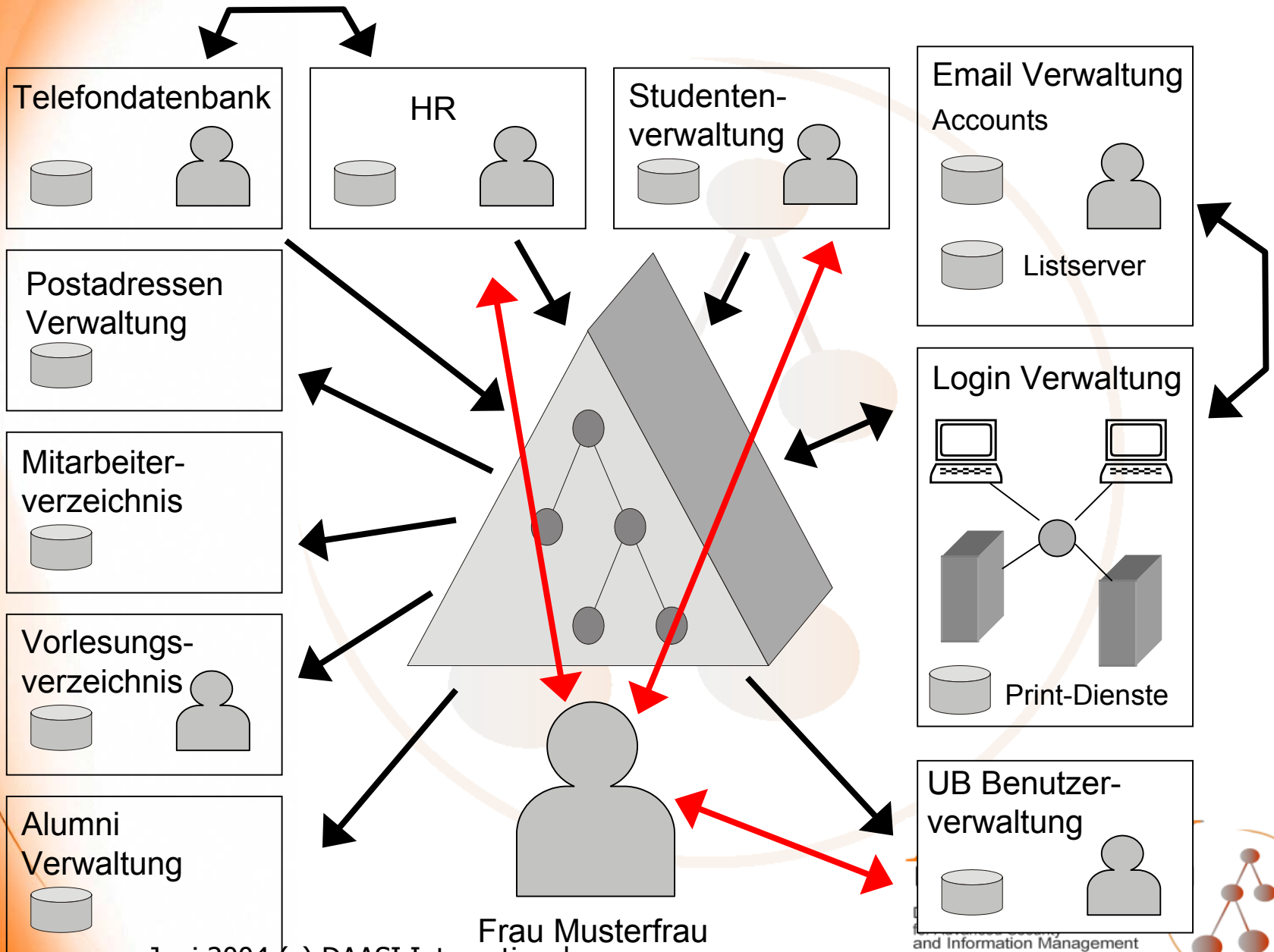
DAASI International

Directory Applications for Advanced Security and Information Management

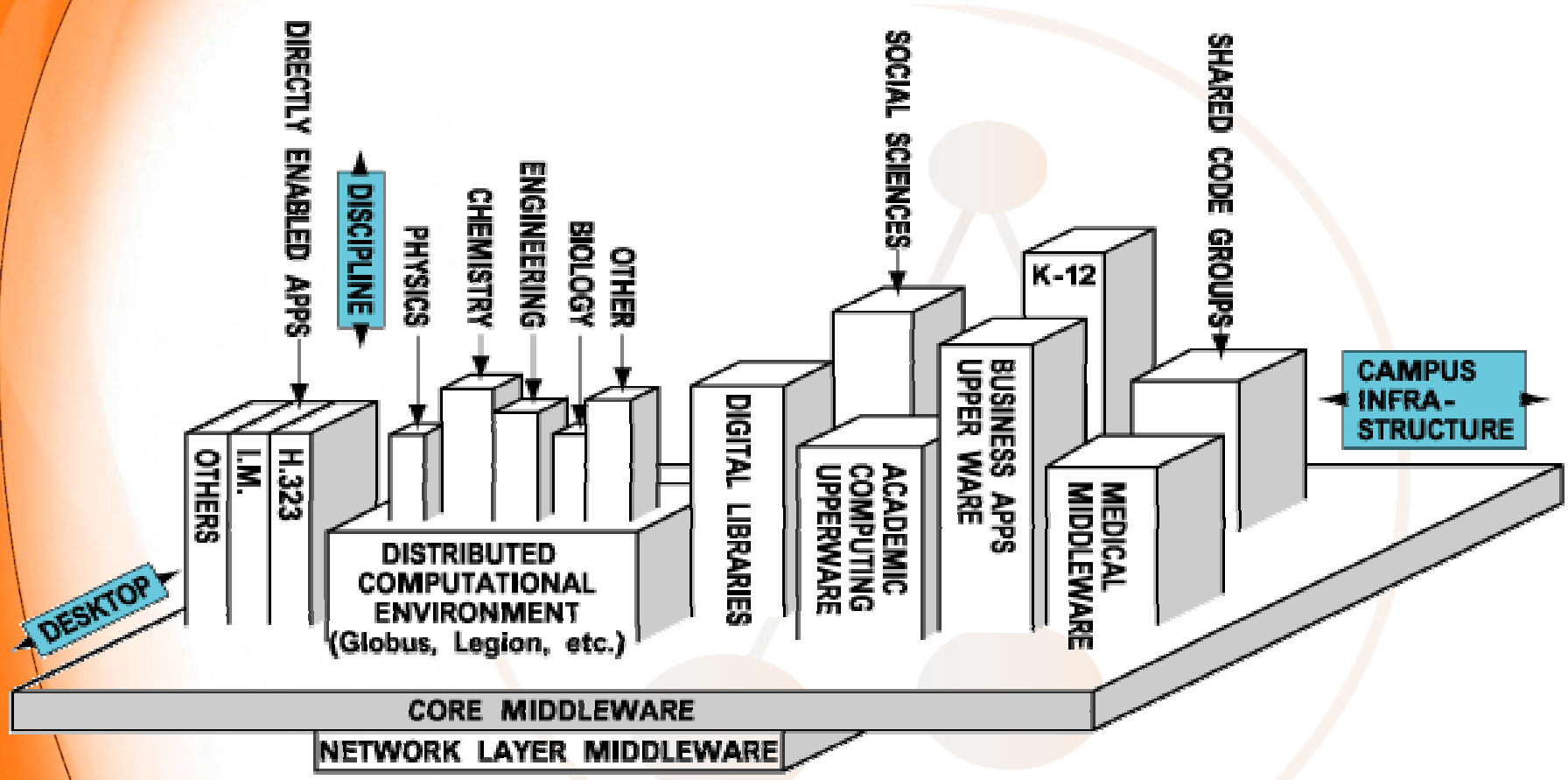
Lösung 1: zentrales Directory / Komm.db



Lösung 2: Metadirectory/Provisoning



Wie Internet2 Middleware versteht



Aus: Ken Klingenstein: Shibboleth Update, ALA May 1, 2002,
http://shibboleth.internet2.edu/shib-presentations.html

DAASI International
Directory Applications for Advanced Security and Information Management

Relevante Technologien

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

3.) Relevante Technologien

- Einführung in Verzeichnisdiensttechnologien
  - X.500, LDAP
- Technologien für zentrale Authentifizierungssysteme
  - SASL, GSSAPI, PAM, NSS, RADIUS
  - X.509 PKI
- Föderierte Identitäten und andere Unique Identifiers
  - Passport, Liberty Alliance, URN, OID
- Technologien für Authentifizierung und Autorisierung
  - LDAP, Kerberos, AAA, X.509 PMI,
- Implementierungen für Domainübergreifende AA
  - Permis, Papi, Shibboleth
- XML Standards zu Provisioning und Workflow
  - SAML, XACL, SPML, WfMC, WS-CDL

DAASI International

Directory Applications for Advanced Security and Information Management

Einführung in LDAP

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

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

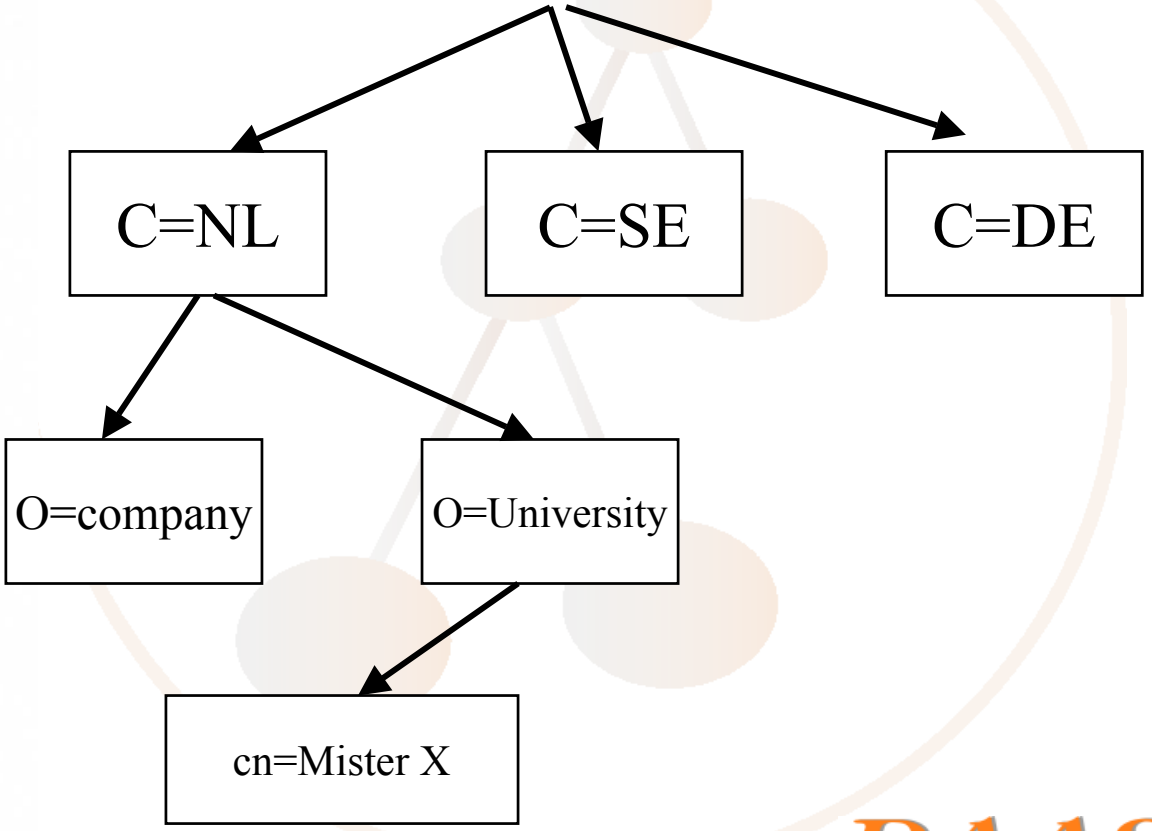
Directory Information Tree (DIT)

- 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)



DAASI International
Directory Applications for Advanced Security and Information Management

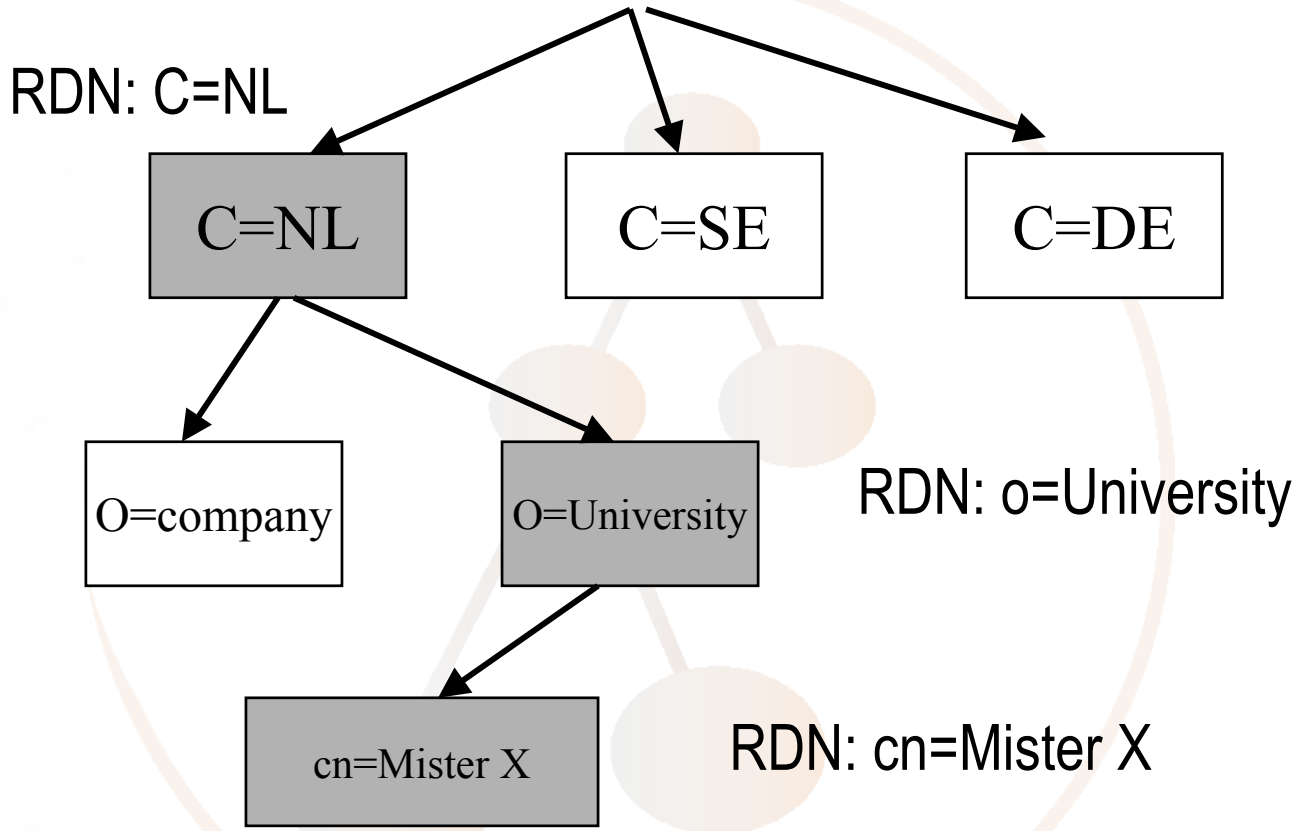
Distinguished Name (DN)

- 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 im gesamten Baum einen gleichen Namen

DAASI International

Directory Applications for Advanced Security and Information Management

Relative Distinguished Name (RDN)
Distinguished Name (DN)



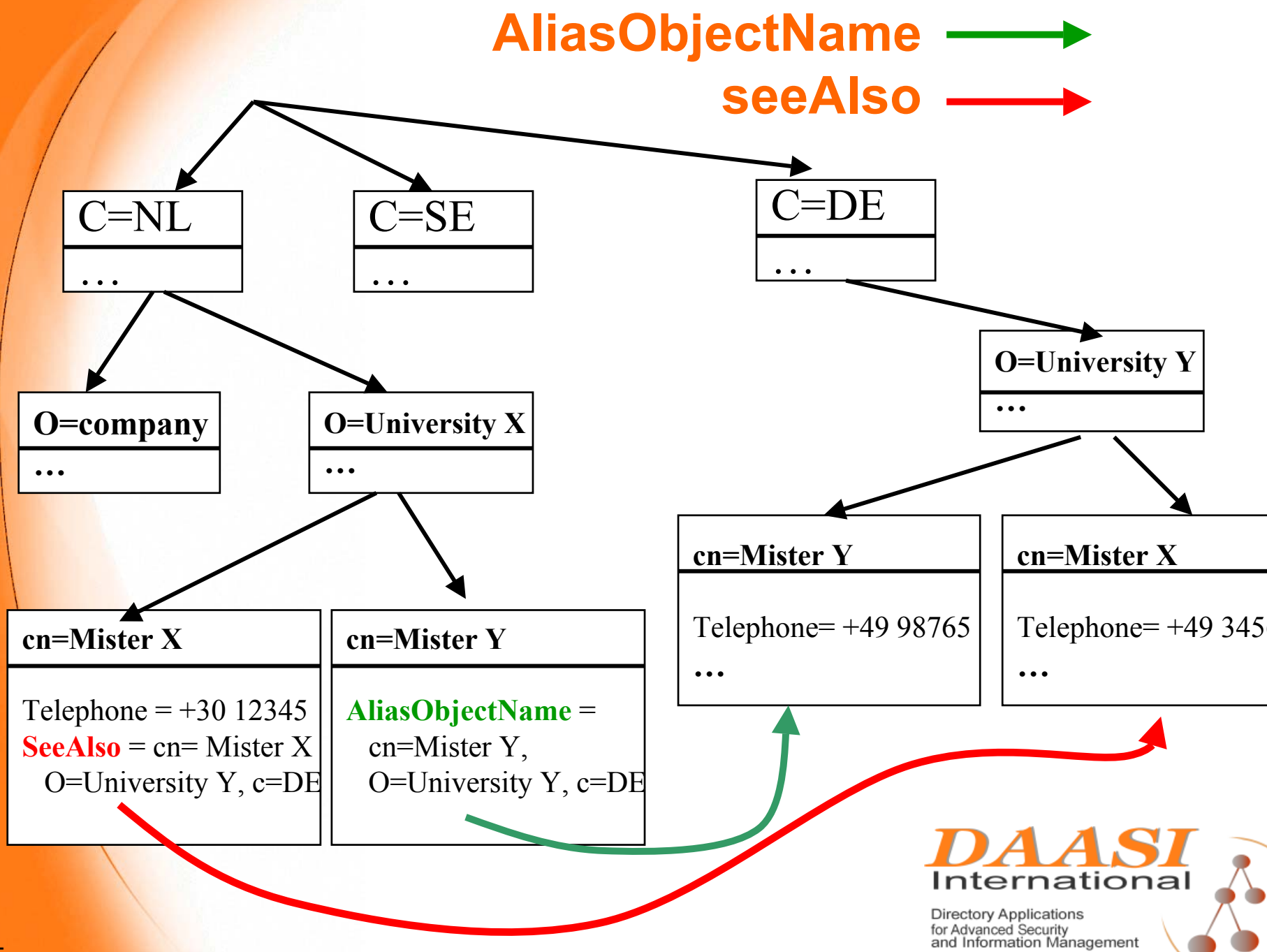
DN: c=NL;o=University;cn=Mister X

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

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

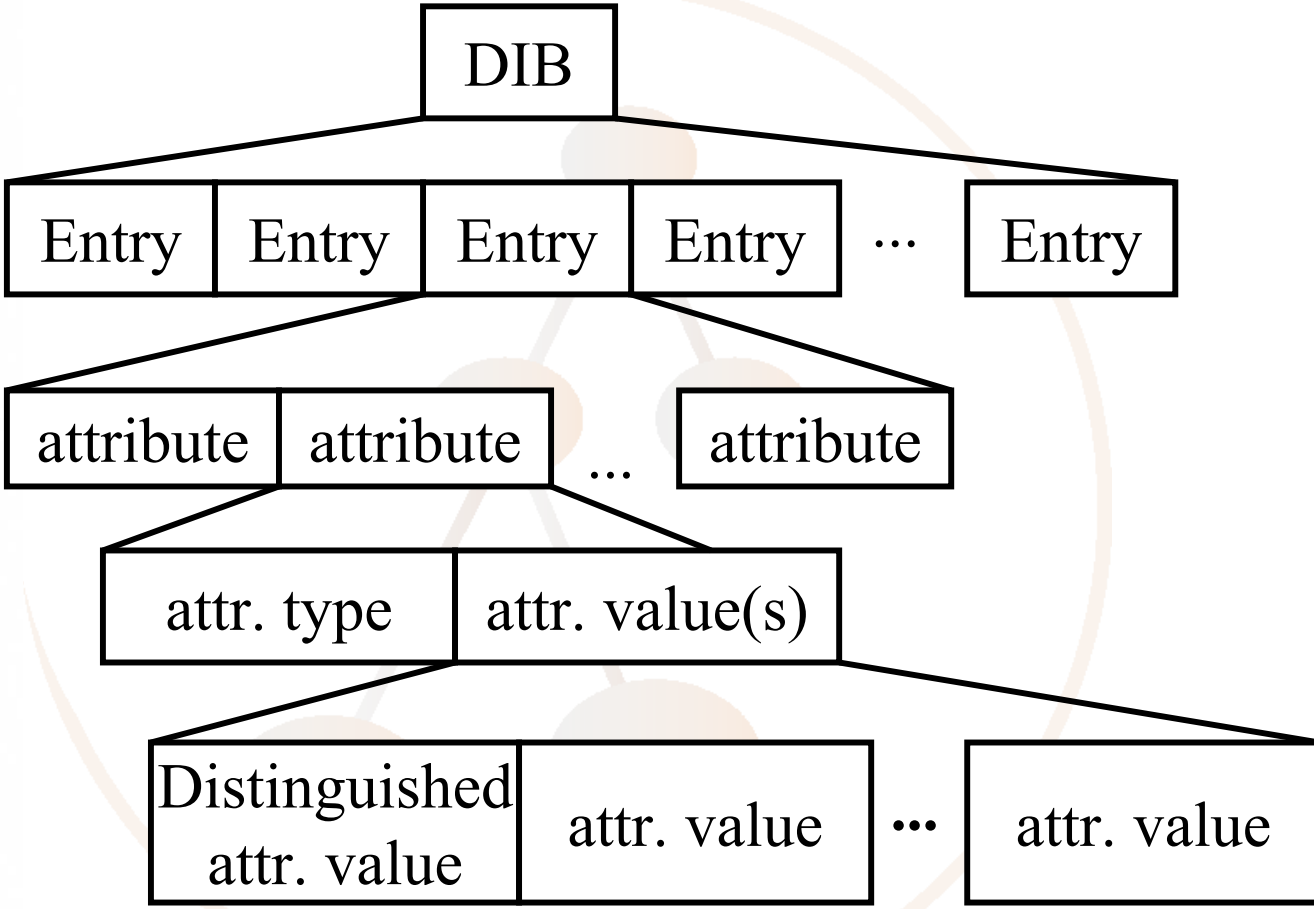
3 Objektklassen Typen

- ABSTRACT
  - Wird nur für die Vererbungshierarchie verwendet
  - Darf nicht allein instanziiert werden
  - ein Eintrag darf nicht nur von abstrakten Objektklassen modelliert werden
- STRUCTURAL
  - Definiert die Hauptcharakteristik eines Eintrags, wie z.B. Person, Organisation, etc.
  - Ein Eintrag darf nur eine Strukturelle Objektklasse, bzw. deren Vererbungshierarchie enthalten
- AUXILIARY
  - Hilfsklasse, die einem Eintrag zusätzliche Eigenschaften modelliert
  - Z.B.: PKIUser mit Attribut userCertificate

Schema

- Eine Ansammlung von Objektklassen, Attributen, Syntaxen und Matching Rules, die für einen bestimmten Zweck definiert wurden, werden *Schema* genannt
- Jedes Schemaelement (Attributtypen, Objektklassen, Syntaxen, Matchingrules, etc.) hat eine weltweit eindeutige Nummer (Object Identifier, OID) mit der es identifiziert werden kann

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, .

Beispiel

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

ABSTRACT →	**objectClass=top**
STRUCTURAL (nur eine Vererbungshierarchie) →	**objectClass=person** **objectClass=organizationalPerson** **objectClass=inetOrgPerson**
AUXILIARY →	**objectClass=pKIUser**
cn aus person →	**cn=Mister X** **cn=Xavier Xerxes**
mail aus inetOrgperson →	**mail=X@dot.com** **mail=Mister.X@dot.com**
telephoneNumber aus organizationalPerson →	**telephoneNumber=1234567**
userCertificate aus pKIUser →	**userCertificate=a1b2c3d4e5f6…**

DAASI International

Directory Applications for Advanced Security and Information Management

Offene Struktur

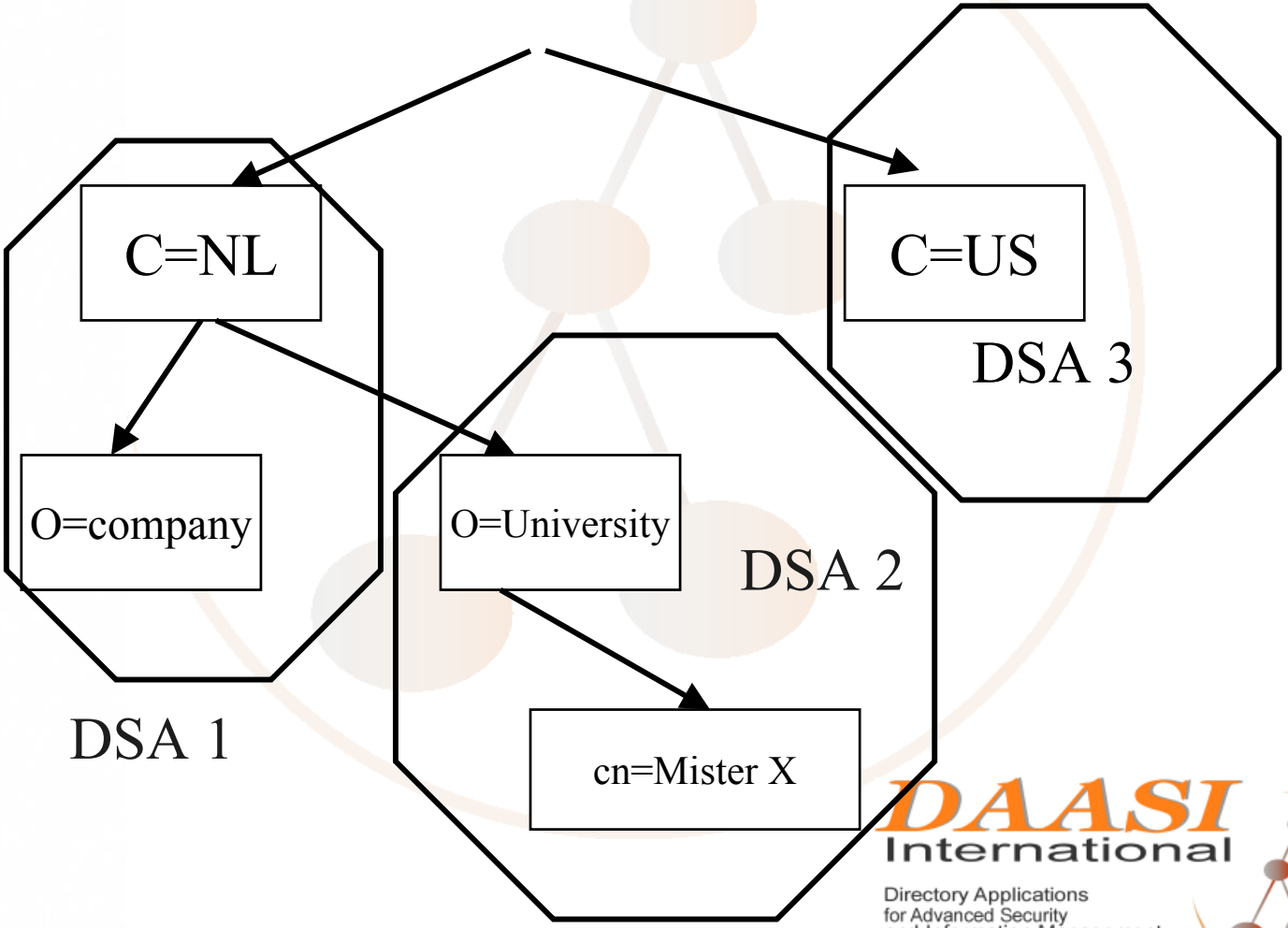
- Mann kann eigenes Schema definieren
  - Objektklassen
  - Attribute
  - [Syntaxen]
  - [Matching Rules]
- Lokal kann man selbstdefiniertes Schema einfach verwenden
- Wenn das Schema global genutzt werden soll muss man es
  - Standardisieren (IETF-RFC)
  - Oder wenigstens registrieren (s.u.)

DAASI International

Directory Applications for Advanced Security and Information Management

Verteilung der Daten

- **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

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 (RFC 2849)

- LDAP Data Interchange Format
- ASCII-Format zum Datenaustausch
  - Auch für delete und modify
- Beispiel:

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

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

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)
- Immer noch in Arbeit
  - Replikationsmodell
  - Zugriffskontrolle

DAASI International

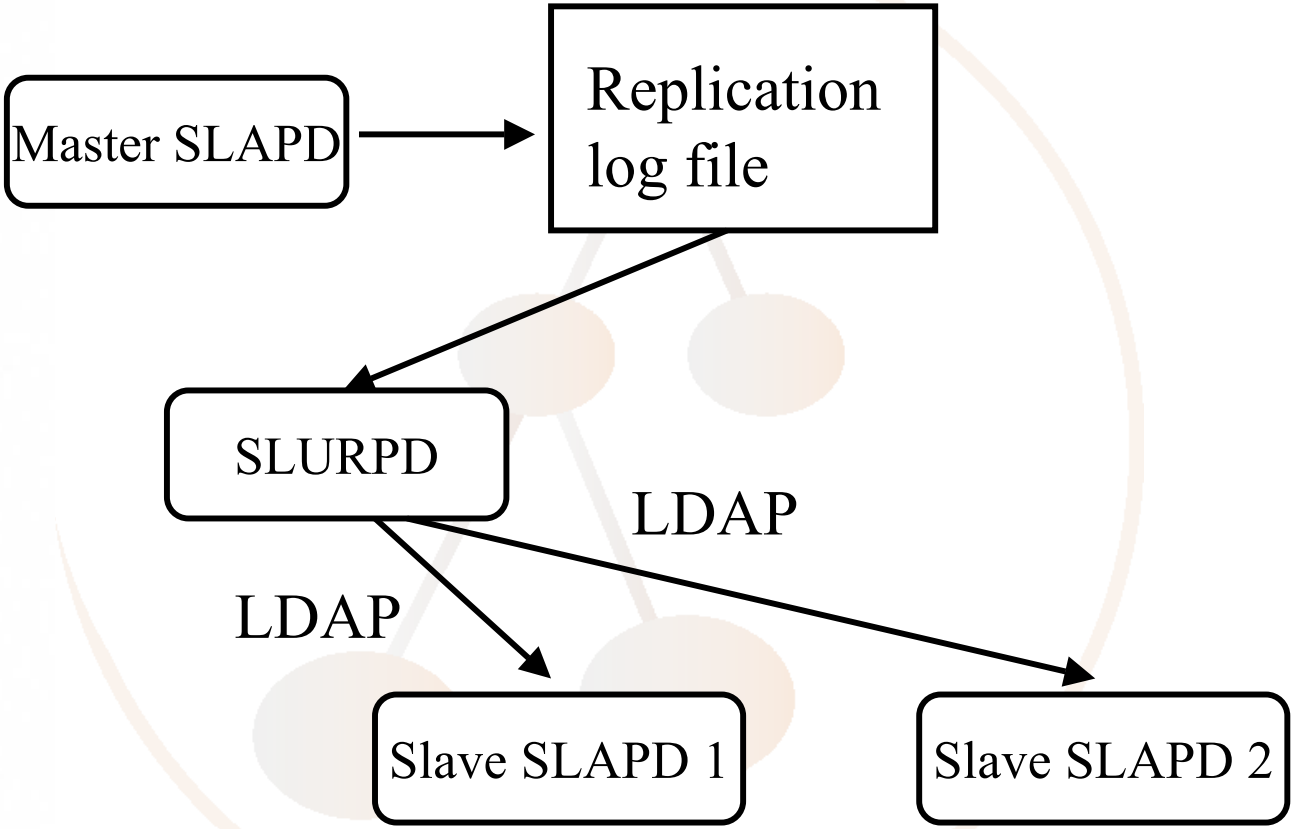
Directory Applications for Advanced Security and Information Management

Replikation

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

DAASI International
Directory Applications for Advanced Security and Information Management

Replikationslösung in Open Source Implementierung



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
```

DAASI International

Directory Applications for Advanced Security and Information Management

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 berücksichtig
  - 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

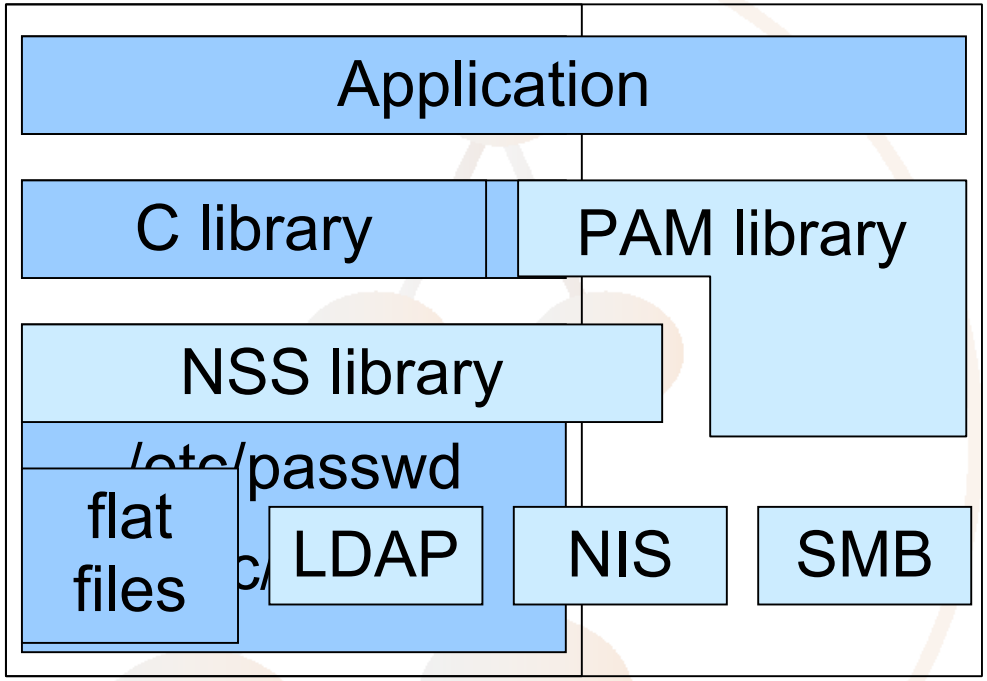
Zentrales Authentifizierungssystem

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

Unix authentifizierung



Unix-Benutzerverwaltung

- Standardisierte LDAP Objektklassen zur Abbildung von NIS (RFC 2307)
  - 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

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)

DAASI International

Directory Applications for Advanced Security and Information Management

Unified Login with Active Directory (AD)

- First project result was based on AD
  - Usefull in a primarily Windows based landscape
  - Integrated Kerberos Key Distribution Center (KDC) easily provides SSO functionality
  - AD did not fully support NIS schema,
    - Open LDAP server was additionally used for NIS data
    - AD was only used for authentication
  - PAM_LDAP as well as PAM_krb5 could be used, easily switchable
  - SSO system supports Unix and Windows login, SMTP auth, IMAP auth, SSH, CVS, FTP

DAASI International

Directory Applications for Advanced Security and Information Management

Why search for something else?

- We needed a more flexible solution
  - something in which you can integrate your own code => Open Source
- No licensing problems
- Better Unix support
- Only one directory for all applications
  - Not only integrate NIS but any directory services
  - Easier administration
    - One central administration point
    - Different admins have different access rights (on subtree and on attribute level)
    - Good old log files instead of strange error messages
- Easier replication mechanism

DAASI International

Directory Applications for Advanced Security and Information Management

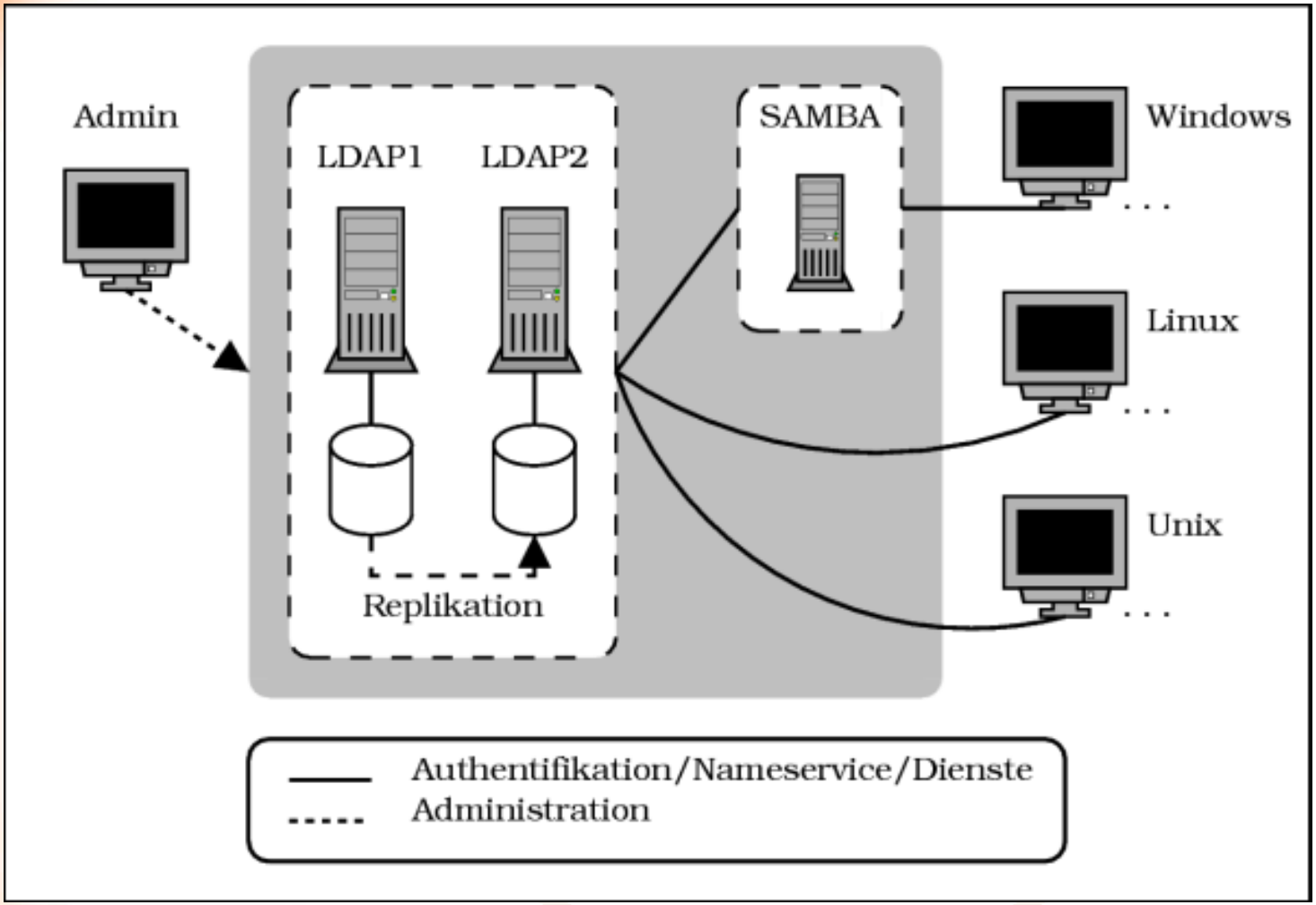
OpenLDAP/Samba recipe

- Take a linux box with minimal linux installation
- Add the following (newer versions will also do):
  - binutils-2.11.90.0.29-15.i386.rpm
  - gcc-2.95.3 136.i386.rpm
  - glibc-devel-2.2.4-40.i386.rpm
  - make-3.79.1-180.i386.rpm
  - nss_ldap-167-54.i386.rpm
  - openldap2-2.0.12-33.i386.rpm
  - openldap2-client-2.0.12-28.i386.rpm
  - openldap2-devel-2.0.12-28.i386.rpm
  - openssl-devel-0.9.6b-62.i386.rpm
  - pam-devel-0.75-78.i386.rpm pam_
  - ldap-122-77.i386.rpm
- And don‘t forget Samba, we took 2.2.8a
- Useful are the IDEALX smbldap-tools-0.7.tgz

DAASI International

Directory Applications for Advanced Security and Information Management

Architektur der OpenLDAP-Lösung



DAASI International

Directory Applications for Advanced Security and Information Management

Client platforms that work

- Unix:
  - Linux
  - FreeBSD
  - OpenBSD
  - NetBSD
  - Solaris
  - HP-UX
  - AIX
- Windows:
  - 2000
  - XP

DAASI International

Directory Applications
for Advanced Security
and Information Management

Production service

- We currently use central authentication for:
  - Linux client login
  - BSD client login
  - Win2k client login
  - Cyrus-imapd
  - Sendmail smtp auth
  - sshd
  - cyrus-sasl
  - tutos (open source project planner / CRM)
- We do cashing via Name Service Casheing Daemon (nscd)

DAASI International

Directory Applications for Advanced Security and Information Management

Problems

- Memory allocation reentrance bug in SASL made the following authentication chain crash:
  cyrus-imapd -> cyrus-sasl -> pam -> pam_ldap
- Either redesign the SASL library (☹) or use the work around patch of Rein Tollevik

DAASI International

Directory Applications
for Advanced Security
and Information Management

Zope based user/admin interface

- Easy to use interface for users and admins
- Using Zope
  - Very portable
  - Nice CMS functions
  - Has an LDAP API („LDAPUserFolder“)
- Interface uses SSL/TLS
- Manages any kind of data

DAASI International

Directory Applications
for Advanced Security
and Information Management

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://athena.directory.dfn.de:8080/authadmin/ULSadmin

ve direc... | Index of /samba/ftp | devel.samba.org | SAMBA - opening windows to ... | ULS Administrator Bereich

DAASI International

Directory Applications for Advanced Security and Information Management

Unified Login Server

ULS Administration | ULS Benutzereinstellungen | DAASI Homepage | Uni Tübingen | Verwende Rechte von Benutzer: **Anonymous User**

Zope @ DAASI

Configure | LDAP Schema | Caches | Users | Groups | Log | Undo | Ownership | Security

LDAPUserFolder at /authadmin/acl_users — Help!

Change the basic properties of your LDAPUserFolder on this form.

Title	Zentrale Authentifikation		
Login Name Attribute	uid (uid)		
RDN Attribute	uid (uid)		
Users Base DN	ou=Users,o=smb,dc=daasi,dc=de	Scope	SUBTREE
Group storage	Groups stored on LDAP server		
Groups Base DN	ou=Groups,o=smb,dc=daasi,dc=de	Scope	SUBTREE
Manager DN	cn=root,o=smb,dc=daasi,dc=de	*Password*	*******
Manager DN Usage	For login data lookup only		
User object classes	top,inetOrgPerson,posixAccount,sambaAccou		
User password encryption	SSHA		
Default User Roles	Anonymous		

Migration from AD to OpenLDAP

- IDEALX tools help to migrate passwords
- We wrote a script that migrates all infos stored in AD to the OpenLDAP server
- You can in theory also migrate the profiles since samba supports the roaming profile feature (we are still working on that)

Results

- Stable service via replicated LDAP server
- No performance problems via cashing
- Both directory implementations (AD and OpenLDAP) are fast enough for the requirements of a university

DAASI International

Directory Applications
for Advanced Security
and Information Management

Unified login vs. Single Sign On (SSO)

- Mit dem Authentifizierungsdienst lässt sich nicht nur ein „Unified Login“ realisieren
- Sondern auch eine „Unified Password“ Lösung:
  - Integration in verschiedene Netzanwendungen
  - z.B.: IMAP, POP, SMTP auth, FTP, SSH, ...
  - Viele Produkte sind bereits „LDAP-Enabeled“
  - Wo noch nicht vorhanden, lassen sich LDAP-Schnittstellen einbauen (Voraussetzung: Open Source)
- SSO-Lösung: Unified Password mit OpenLDAP mit Einbindung von Kerberos (hier basteln wir noch)

DAASI International

Directory Applications for Advanced Security and Information Management

RADIUS

- Remote Authentication Dial In User Service
- Server für Ferneinwahl-Benutzer-Authentifizierung und Accounting
- Hauptnutzer sind Internet Service Provider
- Mittlerweile wird RADIUS auch für zentrale Benutzer-Authentifizierungssysteme im Intranet verwendet,
- sowie für Accounting im Intranet
- Es werden verschiedene Authentifizierungstechnologien verwendet:
  - /etc/passwd
  - Interne Datenbank
  - SQL-Authentifizierung
  - PAM-Authentifizierung (z.B. PAM_LDAP!)

DAASI International
Directory Applications for Advanced Security and Information Management

Zusammenfassung Authentifizierungsdienst

- Vorteil: Ein Passwort für alle Rechner
  - Der User muss sich weniger merken
  - Administratoren und Help Desk werden stark entlastet
  - Passwortqualität zentral kontrollierbar
  - Vereinheitlichung der Authentifizierungsschnittstellen
  - Zwingt zu einem Gesamtkonzept
- Nachteil: Ein Passwort für alle Rechner
  - Single point of failure (wenn keine Replikation)
  - Größerer Schaden bei Kompromittierung
  - LDAP Password Policy fehlt noch in OpenLDAP
  - Root-access sollte immer lokal bleiben

DAASI International

Directory Applications for Advanced Security and Information Management

PKI

DAASI International
Directory Applications
for Advanced Security
and Information Management

Public Key Infrastructure

- Basiert auf asymmetrische Verschlüsselung:
  - Schlüsselpaar das in einem mathematischen Zusammenhang steht: privater Schlüssel und öffentlicher Schlüssel
- Mit dem öffentlichen Schlüssel kann man einen Text so verschlüsseln, dass er nur mit dem privaten Schlüssel entschlüsselt werden kann.
  - Vorteil: man muss vor der Verschlüsselung keinen Geheimnisaustausch machen
- Mit dem privatem Schlüssel kann man Texte digital signieren. Diese Signatur kann mit dem öffentlichen Schlüssel verifiziert werden
- In einem Zertifikat bezeugt eine vertrauenswürdige Stelle die Zugehörigkeit eines öffentlichen Schlüssels zu einer Person
- Perfekter Identitätsnachweis
- Mit sog. Attributzertifikaten können Attribute (z.B. Berechtigungen) einem Identitätszertifikat zugeordnet werden

Ziele einer PKI

- Authentizität
  - Gewissheit einer Entität, dass eine andere Entität auch wirklich diejenige ist, die sie vorgibt zu sein.
- Integrität
  - Gewissheit einer Entität, dass Daten nicht verändert worden sind.
- Vertraulichkeit
  - Gewissheit einer Entität, dass niemand außer dem beabsichtigten Empfänger bestimmte Daten lesen kann.
- Non-Repudiation
  - Verbindlichkeit einer Entität, eine geleistete elektronische Signatur nicht bestreiten zu können.

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

Standard LDAP-Schema für Zertifikate

- Objektklasse pkiUser mit Attributtyp userCertificate, in dem ein oder mehrere binäre Zertifikate gespeichert werden
- Objektklasse pkiCA mit Attributtypen caCertificate, CRL und crossCertifikate, in denen die entsprechenden Daten binär abgespeichert sind
- Problem die Feldinformationen in den binären Strukturen sind nicht über LDAP suchbar

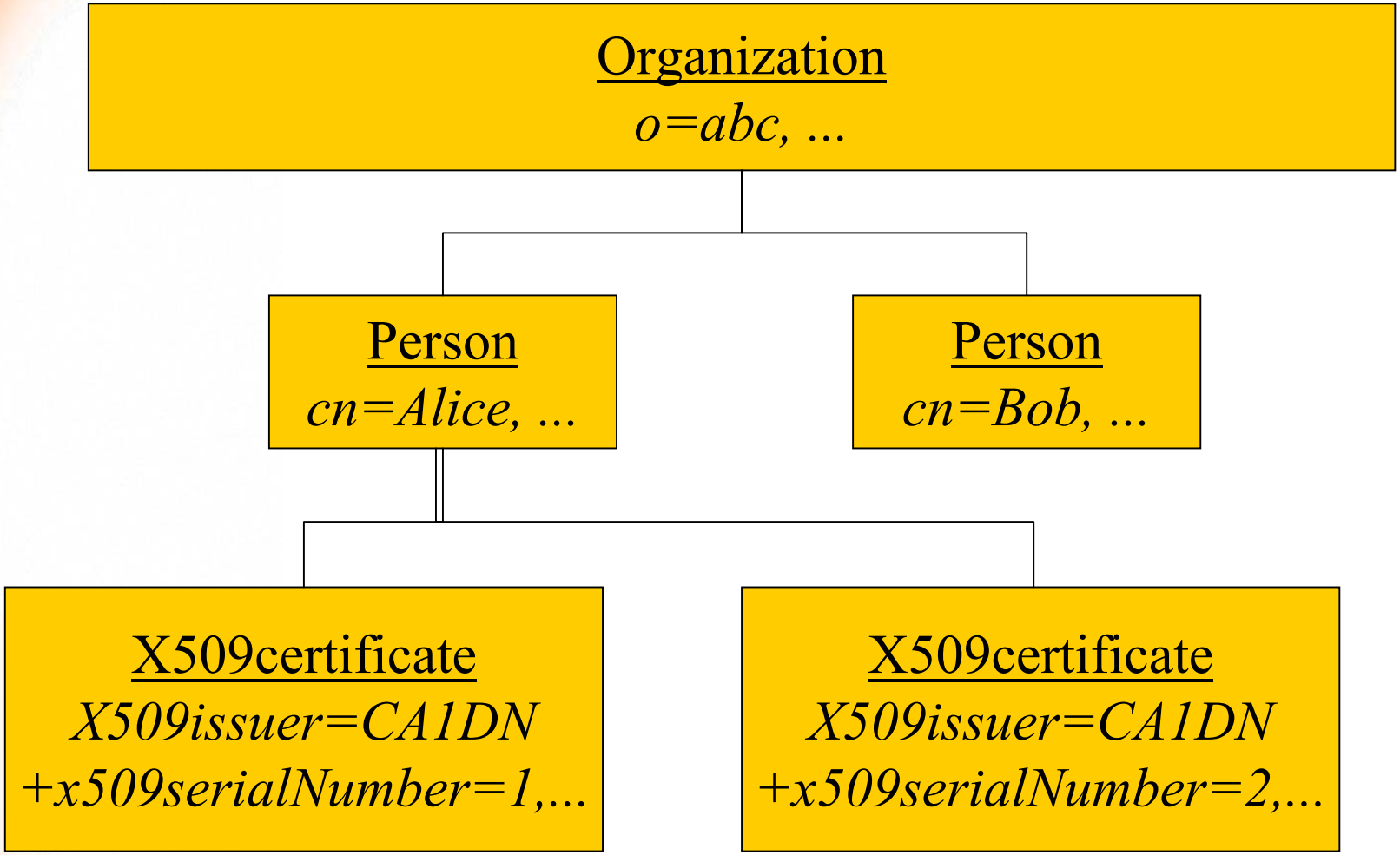
Neuer Vorschlag

- 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
  - Draft-ietf-pkix-ldap-pkc-schema-00.txt

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

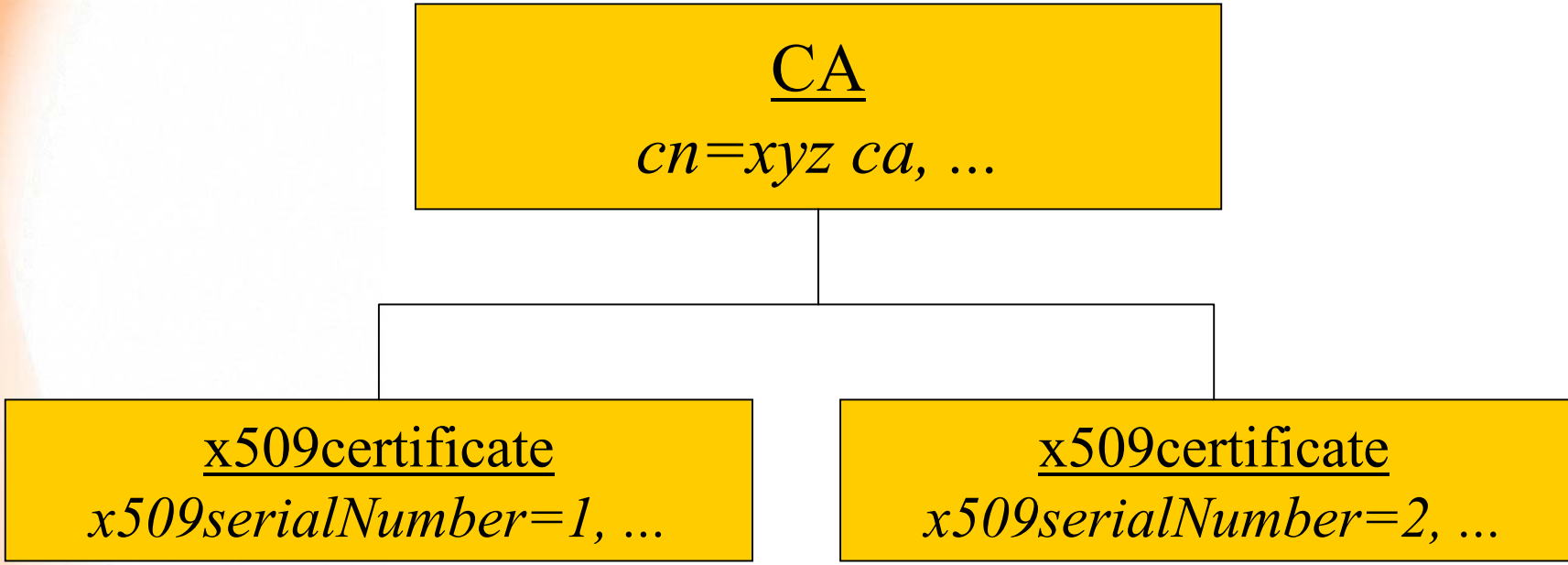
DIT-Struktur im Personenverzeichnis



DAASI International

Directory Applications
for Advanced Security
and Information Management

DIT-Struktur im Zertifikatsverzeichnis



DAASI International

Directory Applications for Advanced Security and Information Management

Globale Unique Identifiers

Microsoft Passport

- Zentrale Vergabe von globalen Identitäten von Microsoft
- Pro Person nur eine Identität
- Identität enthält Name, Land, Bundesstaat, PLZ, Zeitzone, Geschlecht, Geburtsdatum, Beruf und Kreditkartendaten
- Kinderpass für Jugendschutz
- Integration in Bezahlsysteme
- Sicherheitsprobleme und Angst vor Big Brother Bill Gates hat Akzeptanz verhindert

Liberty Alliance

- Als Reaktion auf Passport entstanden
- Offener Standard definiert von einem Industriekonsortium
- Föderales Modell: nicht nur ein Aussteller
- Pro Person nur eine Identität aber mehrere sog. Profile
- Vertrauensmodell „circles of trust“
- Verteilte Datenbank
- Unterscheidung von Authentifikation und Autorisierung
- Benutzer hat Kontrolle darüber, wer die Zugriff auf die eigenen Daten hat
- Aktueller Standard: Liberty Alliance Phase 2 for Federated Identity

DAASI International

Directory Applications for Advanced Security and Information Management

Object Identifiers (OID)

- Aus Nummern bestehende Zeichenfolgen:
  - 1.2.345.678.1.2345678.2
- Hierarchischer Nummern-Raum mit Delegation der Verantwortung über Teilbäume.
  - Der für den Teilbaum 1.2.345.6 Verantwortliche kann jemand Anderem die Verantwortung für 1.2.345.6.1 delegieren, usw.
  - Verantwortung besteht in Vermeidung von Doppel-Verwendung einer Nummer
- System stammt aus der ITU-OSI-Welt
- OIDS können verschiedenste Dinge bezeichnen:
  - Schemaelemente, Policies, etc. etc.

DAASI International

Directory Applications for Advanced Security and Information Management

OID-Tree

- Z.B.: Teilbaum der DAASI International:
  - Daasi = 1.3.6.1.4.1.10126
  - On 1.3.6.1.4.1. Siehe auch http://www.iana.org/assignments/enterprise-numbers
  - Ca. 14.000 Enterprise-numbers wurden bereits von der IANA vergeben
  - Weitere Infos zu OIDs siehe http://www.alvestrand.no/objectid/

DAASI International

Directory Applications for Advanced Security and Information Management

Uniform Resource Names (URN)

- Name, durch den eine Ressource oder Informationseinheit unabhängig vom Speicherort (URI) bezeichnet wird.
- Langlebigere Bezeichnung, ein persistenter Name:
- Eine URL identifiziert den Ort oder das Behältnis einer Instanz einer Ressource, die durch eine URN bezeichnet wird.
- Hierarchischer Namensraum mit Delegation der Verantwortung für die URN-Vergabe (wiebei OIDs)
- Es gibt einen URN-Namensraum für OIDS (RFC 3001)
- Wurde ursprünglich für Texte im weitesten Sinn verwendet
- Könnte aber zu beliebig Anderem verwendet werden

DAASI International
Directory Applications for Advanced Security and Information Management

Technologien für Authentifizierung und Autorisierung

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

LDAP-Alternative zu Provisioning Systeme

- LDAP setzt sich als offener Standard durch
- Hersteller haben aber proprietäre Provisioningsysteme, die sie integrieren wollen
- Alternative: LDAP anstelle von Provisioning
  - Modell mod_auth_ldap des Apache-Servers
  - Anwendungen machen Autorisierungsentscheidungen aufgrund LDAP-Authentifikation und LDAP-Filter
  - Voraussetzung:
    - Rollen- und Gruppenkonzepte müssen im Verzeichnisdienst abgebildet werden
    - Anwendungen müssen LDAP-enabled werden
  - Vorteile:
    - wirkliche Herstellerunabhängigkeit und damit Flexibilität in der Softwarewahl
    - Flexibilität bei den Ausnahmen
    - Kostenersparnis durch Realisierbarkeit mit Open-Source-Software

Generischer Prozess für Authentifizierung in Anwendungen

1. [Anwendung authentifiziert sich selbst einmalig mit einer Bind-Operation an einem dedizierten LDAP-Eintrag]
2. Anwendung erfragt vom Benutzer eine LoginId (anstelle eines LDAP-DNs) und Passwort.
3. Anwendung sucht anhand der LoginID den relevanten LDAP-Eintrag suchen.
4. Anwendung führt Bind-Operation an ermittelten Eintrag mit dem vom Benutzer mitgegebenen Passwort durch. Nach dem Erfolg dieser Bind-Operation kann der Benutzer als authentifiziert gelten.
5. [Anwendung beendet die Session mit unbind]
6. [Nach Beendigung aller Abfragen kann sich die Anwendung mit einem unbind abmelden]

DAASI International

Directory Applications for Advanced Security and Information Management

Beispiel Apache: Konfigparameter für LDAP Authentifizierung

- AuthLDAPURL
  - LDAP-URL mit LDAP-Servernamen und -Port sowie BaseDN und Suchtiefe ("sub" für den gesamten Teilbaum, "one" für nur eine Hierarchieebene unter dem BaseDN)
  - An der Stelle der URL, an der normalerweise die zurückzugebenden Attribute angegeben werden, das LDAP-Attribut, in dem der vom Benutzer angegebene Username/LoginId gesucht werden soll
  - [LDAP-Filter, der mit dem automatisch von mod_auth_ldap gebildeten Filter „ (<attr=username>)“ mit logischem UND kombiniert wird.
- AuthLDAPBindDN
  - optionaler DN, an dem sich mod_auth_ldap vor der Such-Operation authentifizieren kann.
- AuthLDAPBindPassword
  - das zu diesem BindDN gehörige Passwort.

DAASI International

Directory Applications for Advanced Security and Information Management

Beispiel Apache: Konfigparameter für LDAP Autorisierung

- **Erweiterung des Parameters require:**
  - **require valid-user: Zugriff für alle, die sich erfolgreich am LDAP-Server authentifiziert hat.**
  - **require user <Benutzername>: Jeder einzelne berechtigte Benutzer wird angegeben**
  - **require dn: Einzelne Benutzer bezeichnet mit ihrem DN, anstelle des Werts des Attributs <attr>**
  - **require group <Gruppenname>: Zugriff für alle, die in einer mit einem DN bezeichneten Gruppe Mitglied sind**
    - **AuthLDAPGroupAttributeIsDN on|off:**
      - DN des Gruppenmitglieds oder
      - der durch das Attribut <attr> bezeichnete Benutzer in den Werten der Attribute member und uniquemember gesucht.
    - **AuthLDAPGroupAttribute: Hiermit kann man andere Attribute als member oder uniquemember angeben, in denen dann anstelle dieser nach Gruppenmitgliedern gesucht wird.**

DAASI International

Directory Applications for Advanced Security and Information Management

Das Interdomanen-Problem

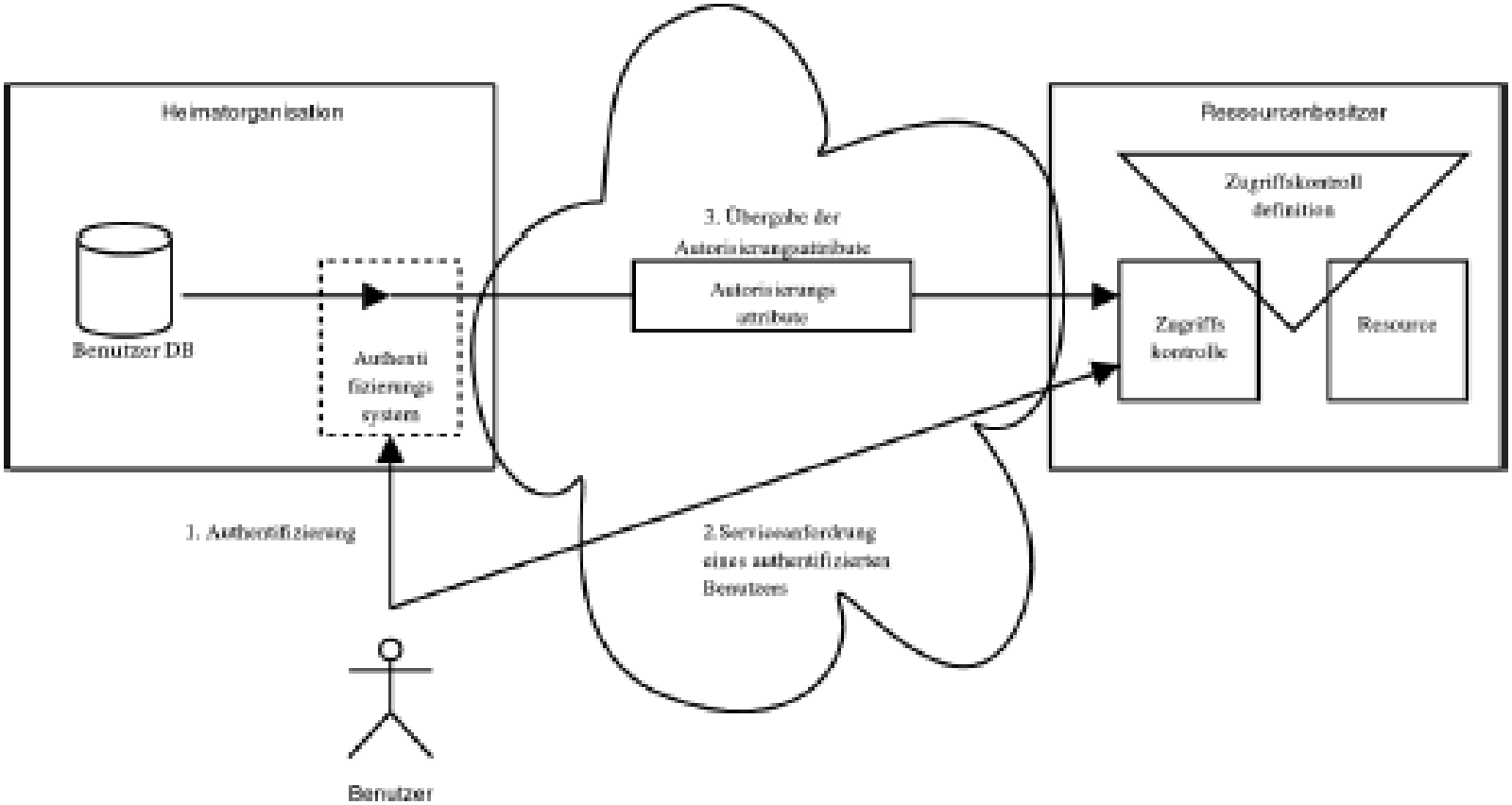


Abbildung 1: Modell eines Systems zur Authentifizierung und Autorisierung (nach [45])

Aus Strattmann: Authentifizierung und Autorisierung in verteilten Systemen, DA Tübingen 2004
nach TERENA TF-AACE: Deliverable B.1.

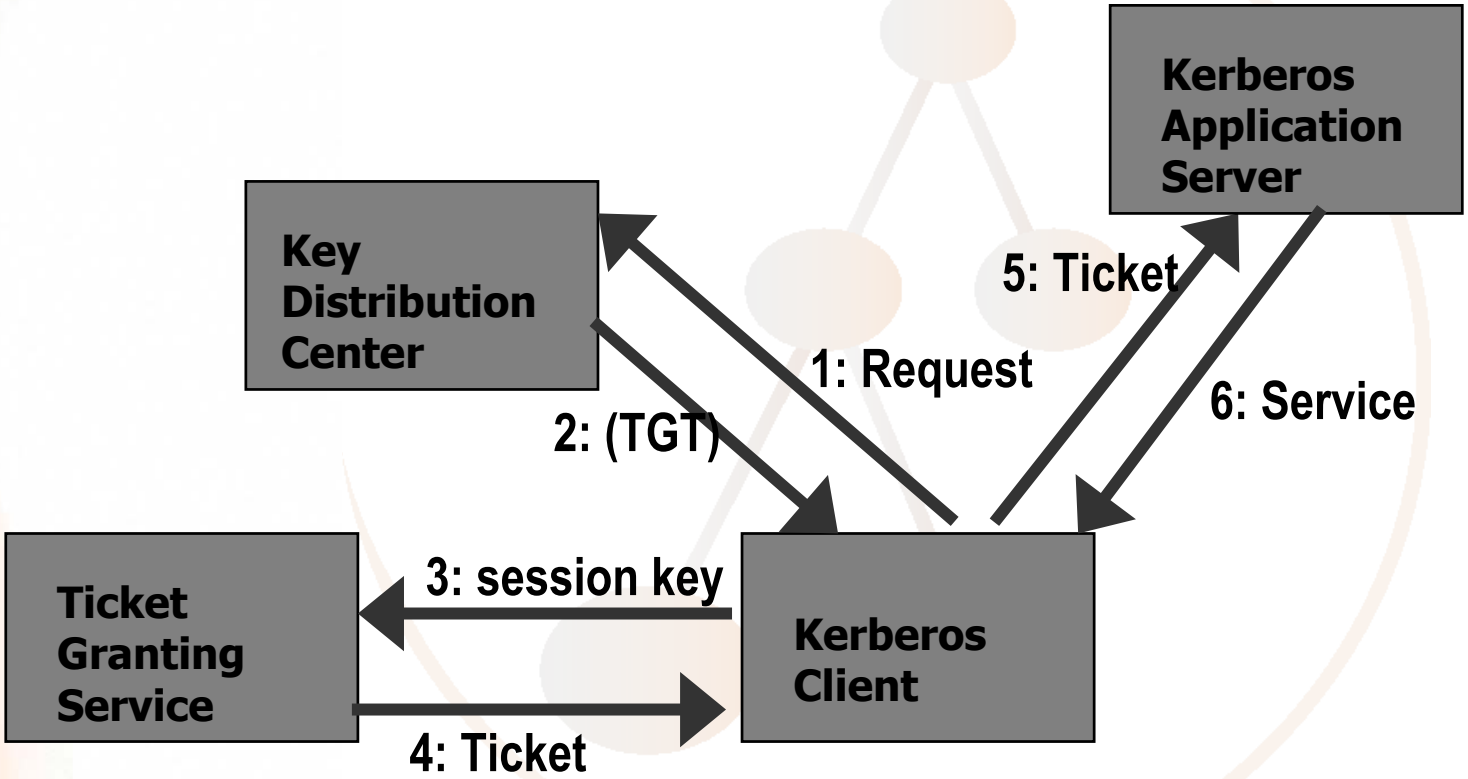
Kerberos

- Speichert Benutzername (=Kerberos Principle) und Passwort
- Passwörter, ob verschlüsselt oder nicht,werden nicht über das Netz geschickt
- Server verschlüsselt Schlüssel mit dem Benutzerpasswort
- Nach der Authentifizierung erhält der Benutzer ein Ticket
  - Hat eine definierte Lebenszeit (z.B. 8 Stunden)
  - Tickets werden von Kerberos Application Servern akzeptiert
- Kerberos bewirkt nur Authentifizierung. Authorisierungsentscheidung liegt beim Dienst

DAASI International
Directory Applications for Advanced Security and Information Management

Juni 2004 (c) DAASI International

Kerberos Architektur



DAASI International
Directory Applications for Advanced Security and Information Management

Kerberos-Daten in LDAP

- Man kann die LDAP-Infrastruktur auch nutzen, um dort zusätzlich Kerberosdaten vorzuhalten
- Heimdal Kerberos kann als Backend LDAP verwenden.
  - Heimdal, configured mit --with-openldap=/usr/local (Installationsort von OpenLDAP).
  - OpenLDAP 2.0.x., configured mit --enable-local um lokale LDAP-Kommunikation zu ermöglichen.
  - OpenLDAP 2.1.x und höher benötigt patch um SASL EXTERNAL authentication zu unterstützen
  - KDC LDAP schema (krb5-kdc.schema)
- LDAP ACL: access to * by sockurl="^ldapi:///$" write

DAASI International

Directory Applications for Advanced Security and Information Management

Beispiel von www.padl.com

- krb5.conf:
  - [kdc] database = { dbname = ldap:ou=KerberosPrincpals,dc=padl,dc=com mkey_file = /path/to/mkey }

```
kdc# kadmin -l
kadmin> init PADL.COM
Realm max ticket life [unlimited]:
Realm max renewable ticket life [unlimited]:
kadmin> ank lukeh
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
lukeh@PADL.COM's Password:
Verifying password - lukeh@PADL.COM's Password:
kadmin> exit
```

Beispiel von www.padl.com

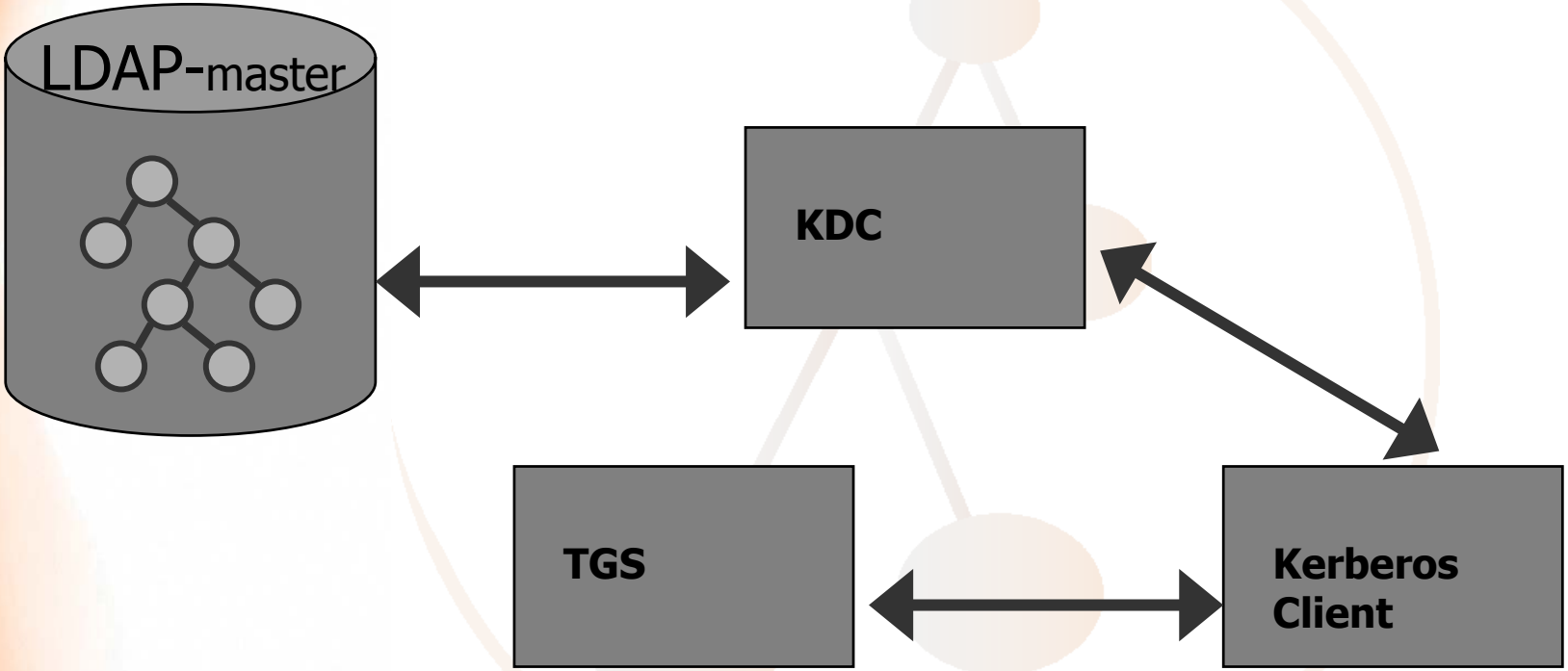
Zum Überprüfen, ob die KDC Principles korrekt im LDAP gespeichert sind:

```
kdc# ldapsearch -L -h localhost -D cn=manager \
 -w secret -b ou=KerberosPrincipals,dc=padl,dc=com \
 'objectclass=krb5KDCEntry'
```

DAASI International

Directory Applications for Advanced Security and Information Management

LDAP als Kerberos backend



DAASI International

Directory Applications for Advanced Security and Information Management

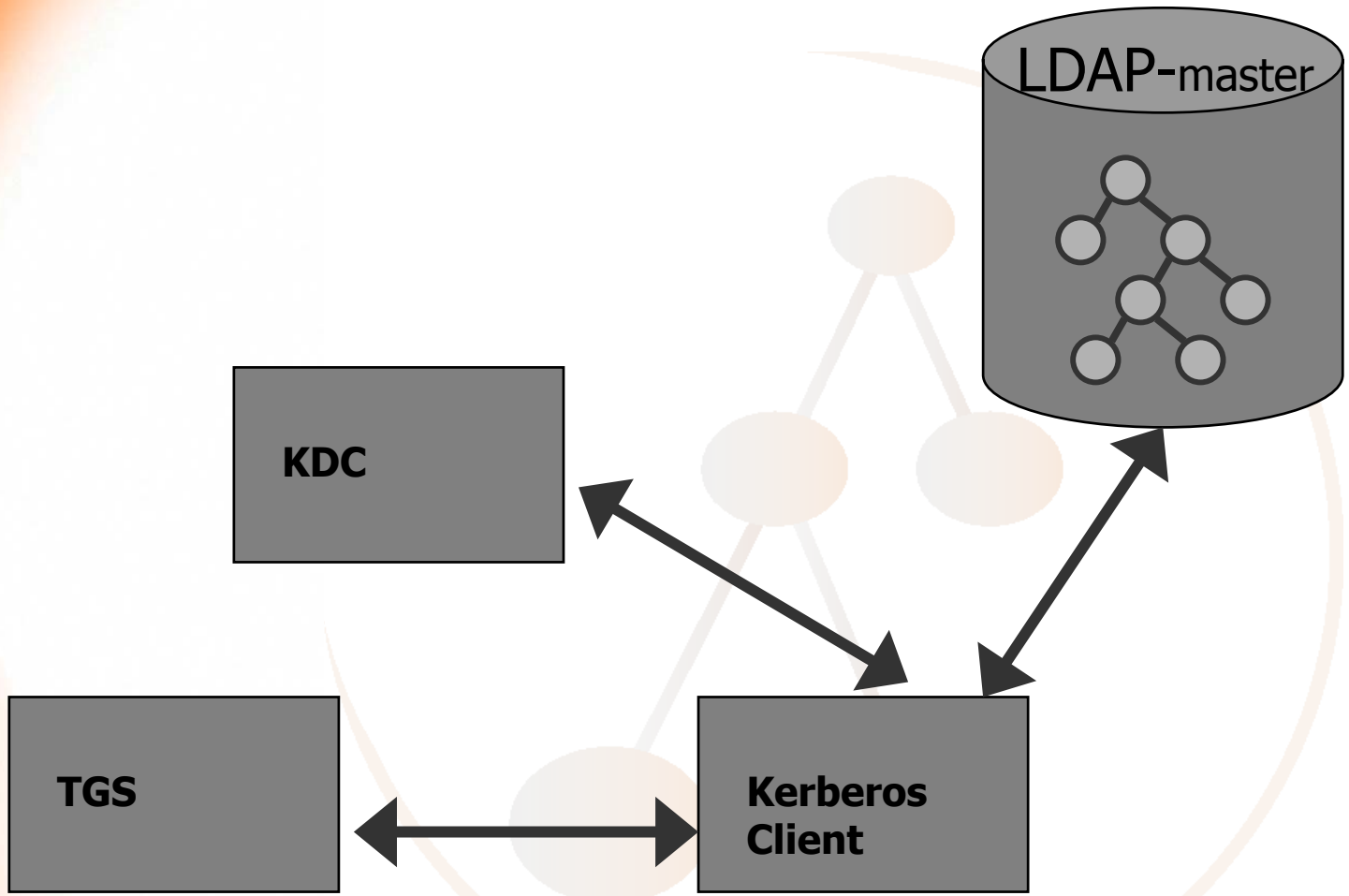
LDAP mit Kerberos Authentifizierung

- Über SASL – GSS-API – KERBEROS5 möglich
- Ausgetestet und funktioniert
- Heimdal oder MIT Kerberos
- Cyrus SASL
- OpenLDAP configured mit:
  - --with-cyrus-sasl

DAASI International

Directory Applications
for Advanced Security
and Information Management

LDAP mit Kerberos-Authentifizierung



DAASI International

Directory Applications
for Advanced Security
and Information Management

Kerberos Authentifizierung

- Über PAM-Modul pam_krb vielfältig einsetzbar
- Noch sicherer als LDAP?
- Stellt echtes Single Sign On bereit

DAASI International

Directory Applications
for Advanced Security
and Information Management

AAARCH

- Authorization, Authentication and Accounting ARCHitecture research group (AAARCH)
- Forschungsgruppe der IRTF
- Ziel:
  - Kapselung der AAA-Prozesse
  - ein generisches Modell für eine Gruppe von untereinander verbundenen AAA-Servern zu definieren
  - und eine Schnittstelle, die es Anwendungen erlaubt, AAA-Funktionen abzurufen.
  - Verschiedene Architekturmodelle mit folgenden Entitäten:

    Benutzer, Heimatorganisation, Service-Provider

DAASI International

Directory Applications for Advanced Security and Information Management

AAAArch Architekturen 1

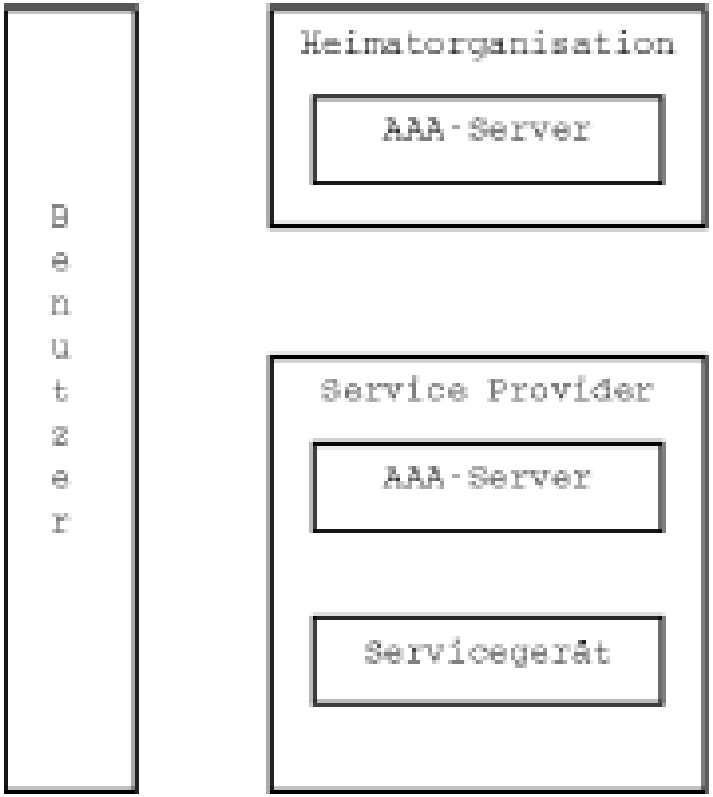


Abbildung 2: Instanzen des Autorisierungsprozess

Aus Strattmann: Authentifizierung und Autorisierung in verteilten Systemen, DA Tübingen 2004

DAASI International
Directory Applications for Advanced Security and Information Management

AAAArch Architekturen 2

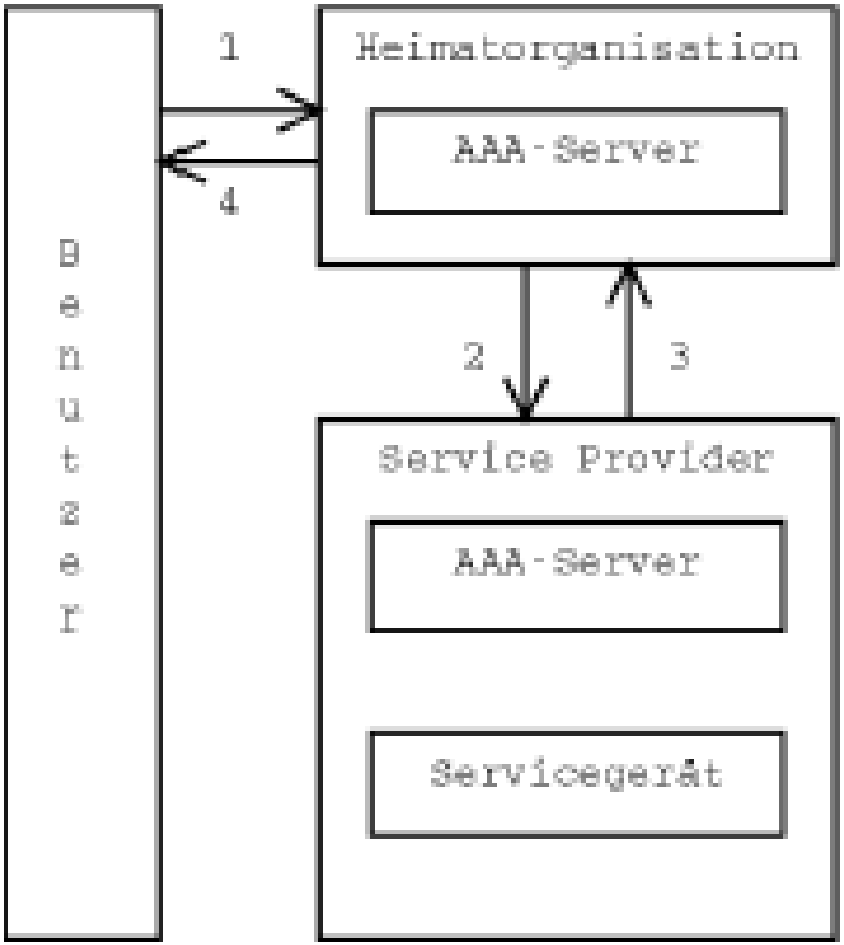


Abbildung 3: Die Agent-Abfolge

Aus Strattmann: Authentifizierung und Autorisierung in verteilten Systemen, DA, Tübingen 2004

DAASI International
Directory Applications for Advanced Security and Information Management

AAAArch Architekturen 3

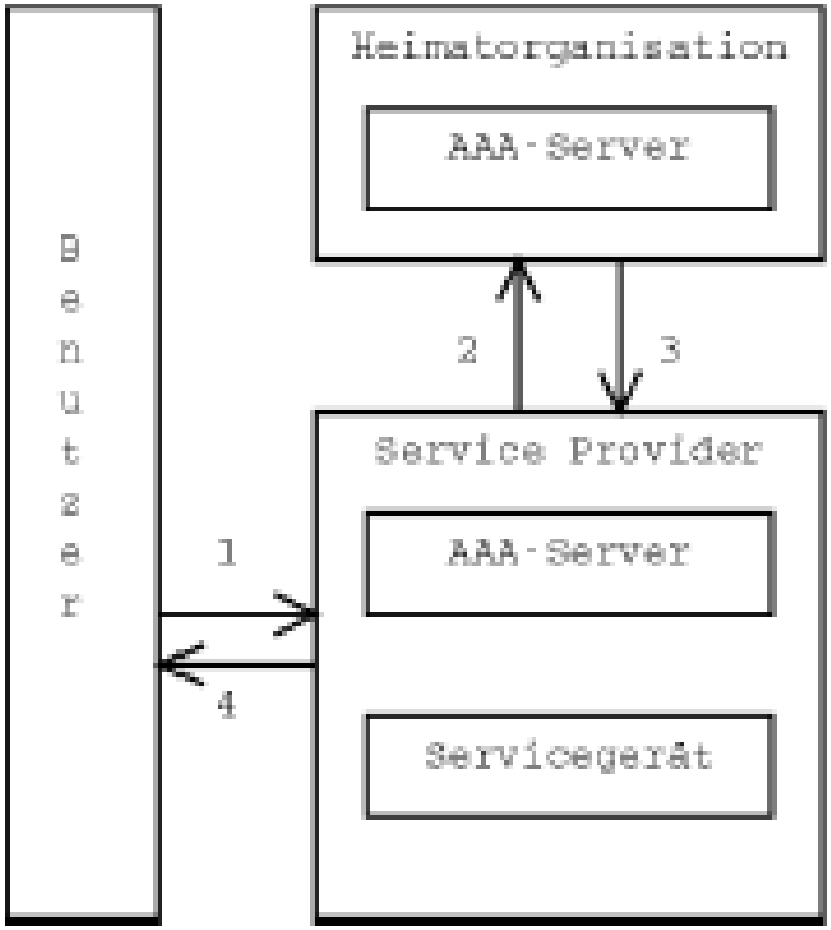


Abbildung 4: Die Pull-Abfolge

Aus Strattmann: Authentifizierung und Autorisierung in verteilten Systemen, DA, Tübingen 2004

DAASI International
Directory Applications for Advanced Security and Information Management

AAAArch Architekturen 4

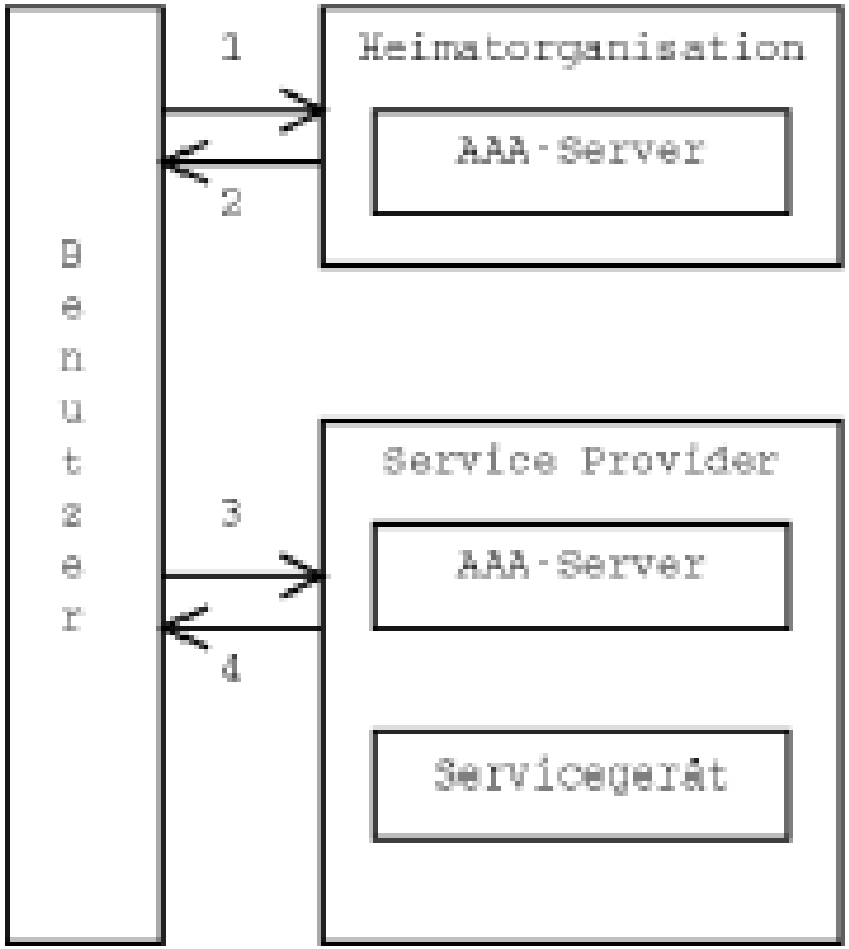


Abbildung 5: Die Push-Abfolge

Aus Strattmann: Authentifizierung und Autorisierung in verteilten Systemen, DA, Tübingen 2004

Juni 2004 (c) DAASI International

DAASI International
Directory Applications for Advanced Security and Information Management

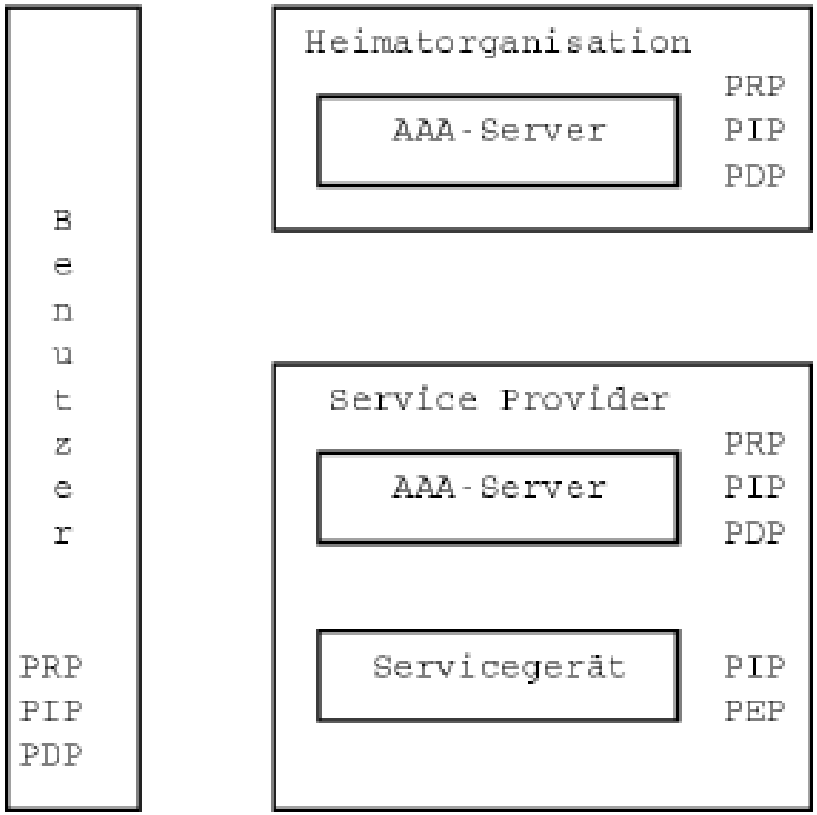
Policy in AAAArch

- PRP
  - Eine Policy wird an einem Policy Retrieval Point (PRP) abgefragt
- PDP
  - an einem Policy Decision Point (PDP) ausgewertet
- PEP
  - an einem Policy Enforcement Point(PEP) durchgesetzt.
- AAA-Server
  - kann eine Policy abfragen und auswerten
- Servicegerät
  - kann eine Policy durchsetzen
- Policy-Repositories
  - können bei AAA-Servern angelegt werden oder sich anderswo im Netzwerk befinden.
- PIP
  - Informationen darüber, welche Policybedingungen ausgewertet werden, sind an sogenannten Policy Information Points (PIP) erhältlich.

DAASI International

Directory Applications for Advanced Security and Information Management

AAAArch Architekturen 5



PRP = Policy Retrieval Point
PIP = Policy Information Point
PDP = Policy Decision Point
PEP = Policy Enforcement Point

Abbildung 7: Wo sich Policyelemente befinden können

Aus Strattmann: Authentifizierung und Autorisierung in verteilten Systemen, DA, Tübingen 2004

DAASI International
Directory Applications for Advanced Security and Information Management

X.509 PMI

- Priviledge Infrastrukture
- Auf X.509-Attributzertifikaten aufbauende Authorisierungsinfrastruktur
- Attributzertifikat bezieht sich auf ein PKI-Identitätszertifikat
- Die Attribute Authority, die Attribute vergibt ist unabhängig von der Certification Authority, die die PKI-Zertifikate erstellt.

Attributzertifikate / PMI

- Durch PKI werden Identitäten zertifiziert
- Unter Nutzung dieser Identitätszertifikaten wird eine unabhängige Priviledge Management Infrastructure aufgebaut
- Attributzertifikate, die bestimmten Identitäten bestimmte Attribute zuweist
  - Z.B. Das Subjekt des PKI-Zertifikats 123 ist bei der Rechtsanwaltskammer eingetragen und darf eine RA-Praxis aufmachen.
- Attribute Authorities (AA) stellen Attributzertifikate aus
  - Pendant zu CA

DAASI International

Directory Applications for Advanced Security and Information Management

XML-Technologien

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

Formate für Identitätsinformation

- X.500/LDAP enthält verschiedene Objektklassen die Personen abbilden (siehe weiter unten)
- Es gibt aber auch viele andere Formate die verschiedene Anwendungen benötigen, z.B.:
  - *Lightweight Internet Person Schema* von NAC
  - *vCard* electronic business card format von IMC
- Verschiedene Anforderungen -> verschiedene Formate
- Deshalb wird ein Rahmenwerk benötigt, in dem verschiedene Formate existieren können, die aber automatisch ineinander konvertiert werden können
- Hier ist XML die Technologie der Wahl:
  - DSML, SAML, XACML (oder XACL) und SPML.
  - Einsetzbar in Webservices

DAASI International

Directory Applications for Advanced Security and Information Management

XML

- XML bietet sich als Sprache zur Beschreibung von Metadaten an.
  - Beliebige Metadatenformate lassen sich mit XML abbilden.
- Linksprache Xlink
- Sprache für Stylesheets XSL
  - XSLT für Transformierungen von XML-Dokumenten
  - XPath , einer Ausdruckssprache, die von XSLT benutzt wird, um Teile eines XML-Dokuments zu referenzieren zu können.

XML-Schema

- Das XML Schema ist eine Metasprache, um XML-Tag-Gruppen zu spezifizieren
  - bietet also eine ähnliche Funktionalität wie die DTD
- zusätzliche Möglichkeiten:
  - Zuweisung von Datentypen zu Elementen und Attributen
  - explizite Unterstützung von Namensräumen
  - ein wesentlich mächtigeres content-Modell.
- XML Schema verwendet zur Definition der XML-Tags wiederum XML.

XML / XML-S

- XML ist die Oberflächensyntax ohne semantische Spezifizierung
  - Aus SGML entstanden
  - Syntax durch HTML bekannt:
    - <tag>xxx</tag>
    - <tag name=xxx>
- XML-S ist eine Sprache zur Einschränkung der Struktur eines XML-Dokuments und kann neue Datentypen in XML einführen
- Die meisten neueren Standards basieren auf XML-Technologien

DAASI International

Directory Applications for Advanced Security and Information Management

Apropos Web Services

- SOAP
  - Simple Object Access Protocol
  - XML basierende Remote Procedure Calls
- WSDL
  - Web Services Description Language
  - XML basierte Schnittstellenbeschreibung für Web Services
- UDDI
  - Universal Description, Discovery and Integration
  - Datenspeicher für WSDL Beschreibungen
  - Kann mit LDAP implementiert werden

DAASI International
Directory Applications for Advanced Security and Information Management

SOAP

- Mit SOAP definiert man
  - XML codierte Interaktionen zwischen Clients und Web Services
  - sowie zwischen verschiedenen Web Services
- Das Ziel sind also interoperable Web-basierte verteilte Anwendungen
- Unter Web Services versteht man in sich geschlossene, modulare Anwendungen, die über ein Netzwerk, in der Regel das Web, beschrieben, veröffentlicht und aufgerufen werden können.
  Web Services:
  - können lokal, verteilt oder webbasiert sein
  - können miteinander interagieren und sich gegenseitig aufrufen, um spezifische Teile von komplexen Work-Flows durchzuführen.
  - SOAP fungiert als Kommunikationsschicht zwischen solchen Anwendungen.

WSDL / UDDI

- WSDL
  - Ist eine XML-Beschreibungssprache für Web Services, womit neue Anwendungen beschrieben werden können
  - So können Services auch von Programmenentdeckt werden
- UDDI
  - Ist ein plattformübergreifendes Rahmenwerk zur Registrierung, Beschreibung, Integration und zum Auffinden von Diensten im Internet.

LDAP und XML

- DSML: Directory Service Markup Language
  - Bildet das komplette Informationsmodell ab
  - Kann also beliebige LDAP-Daten in einem XML-Format darstellen
  - In Version 2.0. Können auch alle LDAP-Operationen abgebildet werden
- XED: XML enhanced Directory
  - Neue Arbeitsgruppe in der IETF
  - XML Daten können vollständig in LDAP Server abgebildet werden
- Grundsätzlich sind die Datenmodelle von LDAP und XML kompatibel

DAASI International
Directory Applications for Advanced Security and Information Management

Juni 2004 (c) DAASI International

DSMLv1 Struktur

```
<dsml:dsml xmlns:dsml="http://www.dsml.org/DSML">
  <!-- a document with both -->
  <dsml:directory-schema>
    <dsml:class id="..." ...>...</dsml:class>
    <dsml:attribute-type id="..." ...>...</dsml:attribute-type>
  </dsml:directory-schema>
  <dsml:directory-entries>
    <dsml:entry dn="...">...</dsml:entry>
   <dsml:entry dn="...">...</dsml:entry>
   <dsml:entry dn="...">...</dsml:entry>
   ...
  </dsml:directory-entries>
 <dsml:dsml>
```

DAASI International

Directory Applications for Advanced Security and Information Management

DSMLv1 Eintrag

```
<dsml:entry dn="uid=prabbit,ou=development,o=bowstreet,c=us">
  <dsml:objectclass>
    <dsml:oc-value>top</dsml:oc-value>
    <dsml:oc-value>person</dsml:oc-value>
    <dsml:oc-value>organizationalPerson</dsml:oc-value>
    <dsml:oc-value>inetOrgPerson</dsml:oc-value>
  </dsml:objectclass>
  <dsml:attr name="cn"><dsml:value>Peter Rabbit</dsml:value>
  <dsml:attr name="sn"><dsml:value>Rabbit</dsml:value></dsml:attr>
  <dsml:attr name="uid"><dsml:value>prabbit</dsml:value></dsml:attr>
  ....
</dsml:entry>
```

DAASI International

Directory Applications for Advanced Security and Information Management

DSMLv2 Struktur

- Anfrage:

```
<batchRequest xmlns="urn:oasis:names:tc:DSML:2:0:core">
  <modifyRequest>…</modifyRequest>
  <addRequest>…</addRequest>
  <delRequest>…</delRequest>
  <addRequest>…</addRequest>
</batchRequest>
```

- Antwort:

```
<batchResponse xmlns="urn:oasis:names:tc:DSML:2:0:core"
  <modifyResponse>…</modifyResponse>
  <addResponse>…</addResponse>
  <delResponse>…</delResponse>
  <addResponse>…</addResponse>
</batchResponse>
```

DAASI International

Directory Applications for Advanced Security and Information Management

DSMLv2 Modify-Beispiel

- Anfrage:

```
<modifyRequest dn="CN=Bob Rush,OU=Dev,DC=Example,DC=COM">
  <modification name="telephoneNumber" operation="replace">
    <value>536 354 2343</value>
    <value>234 212 4534</value>
  </modification>
  <modification name="sn" operation="replace">
    <value>Rush</value>
  </modification>
</modifyRequest>
```

- Antwort:

```
<modifyResponse>
  <resultCode code="53" descr="unwillingToPerform"/>
  <errorMessage>System Attribute may not be modified</errorMessage>
</modifyResponse>
```

DAASI International

Directory Applications for Advanced Security and Information Management

SAML

- Die Security Assertion Markup Language (SAML) definiert einen Standard, sicherheitskritische Informationen in XML zu beschreiben und auszutauschen.
- Insbesondere zum Austausch von Authentifizierungs- und Autorisierungsinformation
- SAML v.1.1. Herausgegeben von OASIS (www.oasis.org)
- Unterstützt Passwörter, Kerberos, Zertifikate (X.509, SPKI, XKMS, SSL/TLS) und XML digitale Signaturen
- Wird z.B. verwendet in Liberty Aliance, Shibboleth, PAPI
- Aber auch in Provisioning-Produkten von:
  - IBM Tivoli, Netegrity, Novell, Oblix, RSA Security, Sun
  - Geplant in Novell nSure und CA eTrust, .Net
  - Achtung: SAML-Kommunikation ist eher Komplex (mind. 6 Kommunikationsschrite)
- Opensource Implementierung:
  - http://www.opensaml.org/

DAASI International

Directory Applications for Advanced Security and Information Management

SAML

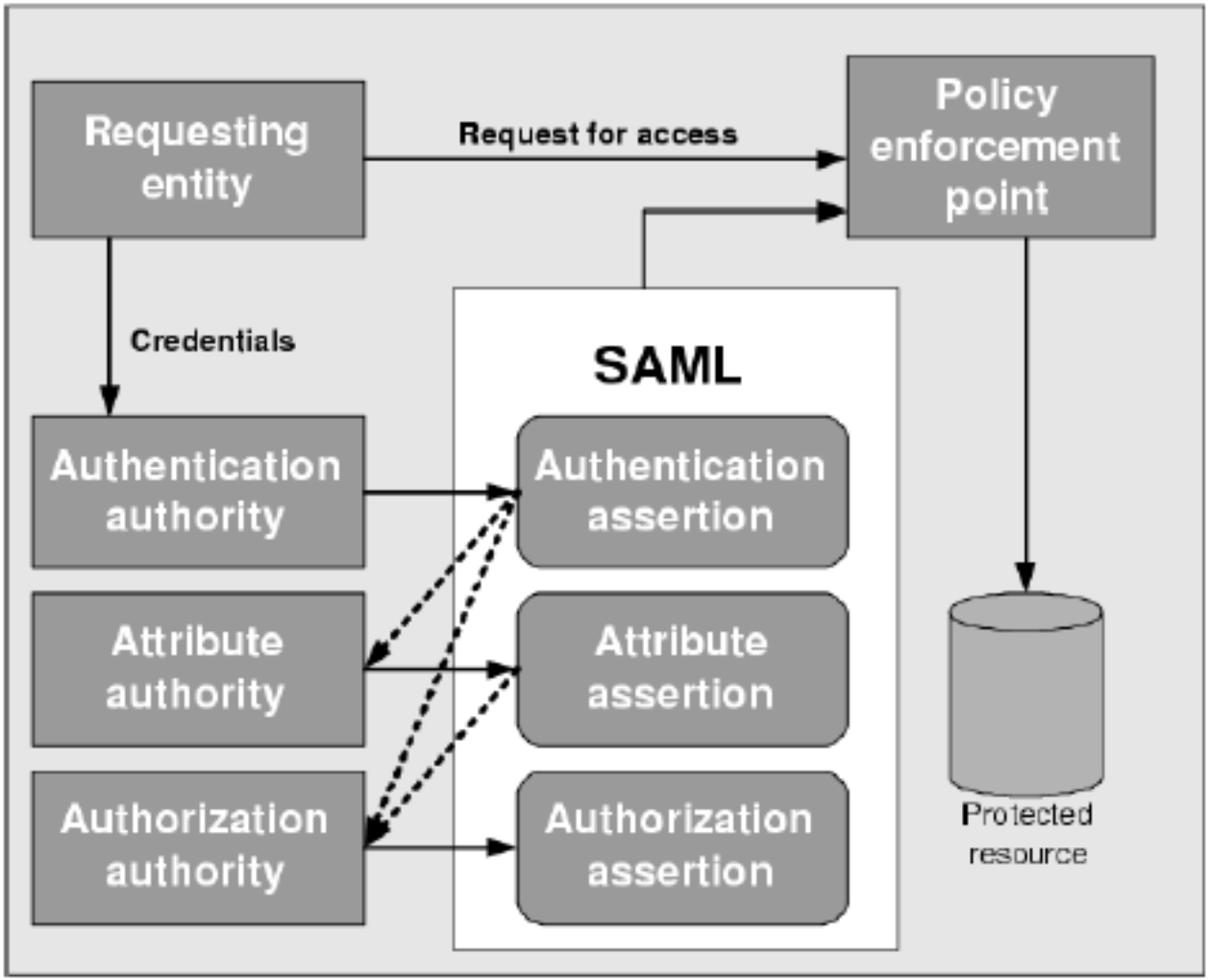
- SAML definiert Protokolle, durch Clients sog. Assertions von SAML-Autoritäten anfordern und deren Antworten empfangen können.
- Die SAML-Autoritäten können diverse Informationsquellen, beispielsweise externe Policy-Repositories oder in der Anfrage bereits enthaltene Assertions, benutzen, um ihre Antworten zu generieren
- Assertions werden dann zu einem SAML-Ausweis gebündelt, der zusammen mit der Anforderung an den PEP der angeforderten Ressource geschickt wird.
- Dieser entscheidet dann über den Zugriff
- Der SAML-Ausweis wird digital unterschrieben, um Modifikationen zu verhindern.
- Deswegen können SAML-Ausweise wiederverwendet werden, ohne eine erneute Authentifizierung erforderlich zu machen.
- SAML ermöglicht damit single sign-on (SSO)

Bestandteile von SAML

- 1.) Assertion:
  - Aussagen einer Identitäts-Authorität (IA) über einen Benutzer oder einer sonstigen Identität
  - IA ist eine vertrauenswürdige Quelle für Authentifizierung und Autorisierung
  - Es gibt drei Arten der Assertion:
    - Authentifizierung
    - Autorisierung
    - Attributierung

DAASI International
Directory Applications for Advanced Security and Information Management

SAML Architektur



Nach: RUBENKING, NEIL J.: Securing web services.
PC Magazine, 2002.

DAASI International
Directory Applications for Advanced Security and Information Management

Bestandteile von SAML 2

- 2.) Protokolle
  - Jeder Assertion-Typ hat ein eigenes Protokoll (Request/Response)
  - Zusätzlich: Artefacts: Zeiger auf Assertions
- 3.) Bindings
  - Transportmechanismus für die SAML-Protokolle
  - SOAP über HTTP
  - Direktes HTTP in Planung
- 4.) Profiles
  - Beschreibt wo im Transportmechismus die SAML-Statements zu finden sind. Bisher definiert für
    - SOAP
    - Web Browser (HTML-Formulare, SSO)

DAASI International

Directory Applications for Advanced Security and Information Management

XACML

- Extended Access Control Markup Language
- OASIS-Standard
- Generisch: Zugriffsregeln (Policy) können Anwendungsunabhängig spezifiziert werden
- Verteilt: Eine Policy kann sich auf eine andere an einem anderen Ort gespeicherte Policy beziehen
- Es gibt XACML-Profile für SAML und LDAP/DSML

XACML-Elemente

- PolicySet: Container für Policies bzw. weitere PolicySets
- Policies und policySets können mit Algorithmen kombiniert werden
- Bedingungen setzen sich zusammen aus Subjekt, Ressource und Aktion
- Environment
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)
- Target: Sammlung vereinfachter Bedingungen
- Rule: Access Control Regeln
- Attribute

DAASI International
Directory Applications for Advanced Security and Information Management

XACML-Beispiel

```
<Policy PolicyId="SamplePolicy„
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:
        rule-combining-algorithm:permit-overrides">
  <Target>
      <Subjects> <AnySubject/>  </Subjects>
      <Resources>
        <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">SampleServer
          </AttributeValue>
          <ResourceAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-
id"/>
        </ResourceMatch>
      </Resources>
      <Actions>
        <AnyAction/>
      </Actions>
  </Target>
```

DAASI International

Directory Applications for Advanced Security and Information Management

XACML-Beispiel

```
<Target>
        <Subjects>
          <AnySubject/>
        </Subjects>
        <Resources>
          <AnyResource/>
        </Resources>
        <Actions>
          <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">login</Attri
buteValue>
            <ActionAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="ServerAction"/>
          </ActionMatch>
        </Actions>
      </Target>
```

DAASI International
Directory Applications
for Advanced Security
and Information Management

SPML Service Provisioning Markup Language

- XML-Schemabasierendes Protokoll zum Austausch von Provisioning-Information zwischen
  - Requesting Authority (RA) und einem Provisioning Service Point (PSP)
  - PSP und einem Provisioning Service Target (PST)
- Abfragemodel mit dem eine RA Details über Provisioning-Elemente erfragen kann
- Bindings für SOAP und direktem HTTP
- Provisioning Service Object Identifier (PSO-ID)
- Provisioning Service Target Data Identifier (PSTD-ID)

DAASI International

Directory Applications for Advanced Security and Information Management

SPML Entitäten

- RA:
  - Software-Komponente welche SPML-Requests an einen SPML Service Point schickt
- PSP:
  - Software-Komponente welche SPML Requests erhält und verarbeitet, also das eigentliche Provisionierungssystem
- PST:
  - Software-Komponente welche das Ziel einer Provisioning-Aktion darstellt

SPML Operationen

- Request/Response Modell für
  - Add
  - Delete
  - Modify
  - Search
  - Extended operation
- Kompatibel mit DSMLv2

DAASI International

Directory Applications
for Advanced Security
and Information Management

SPML Beispiel

```
<addRequest>
  <attributes>
    <attr name="objectclass">
      <value>emailUser</value>
    </attr>
    <attr name="cn">
      <value>Jane Doe</value>
    </attr>
    <attr name="gn">
      <value>Jane</value>
    </attr>
    <attr name="sn">
      <value>Doe</value>
    </attr>
  </attributes>
</addRequest>
```


DAASI International
Directory Applications for Advanced Security and Information Management

SPML Beispiel

```
<addResponse result =
        “urn:oasis:names:tc:SPML:1:0#success">
  <identifier type =
"urn:oasis:names:tc:SPML:1:0#EMailAddress">
        <spml:id>Jane.Doe@acme.com</id>
  </identifier>
  <attributes>
    <attr name="mailBoxLimit">
      <value>50MB</value>
    </attr>
  </attributes>
</addResponse>
```

DAASI International

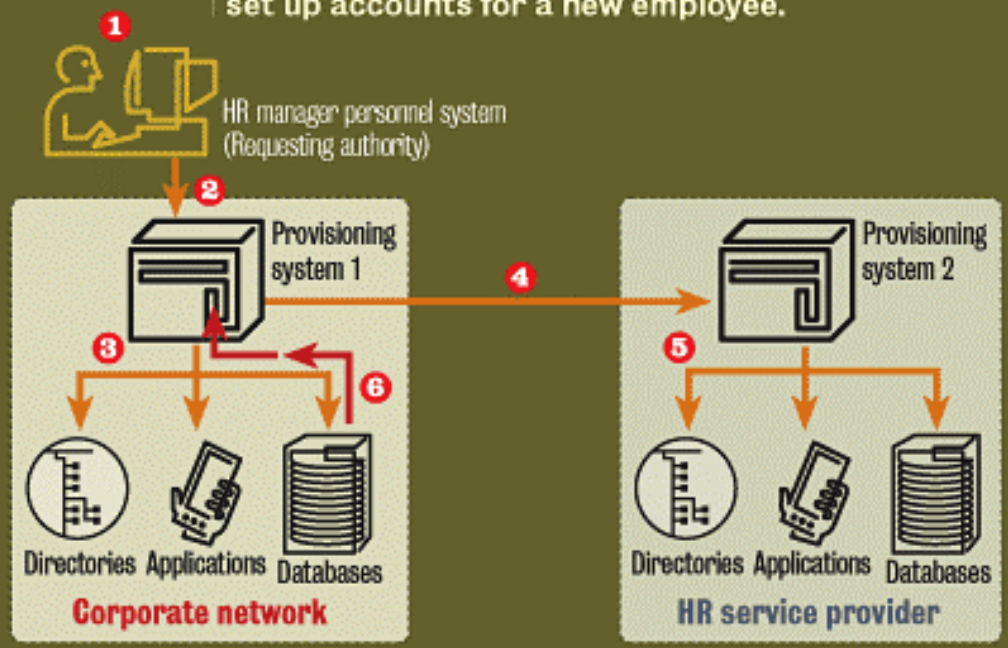
Directory Applications
for Advanced Security
and Information Management

SPML-Beispiel

HOW IT WORKS

SPML

SPML documents specify a set of operations for network services to execute. In this example, SPML is used to set up accounts for a new employee.



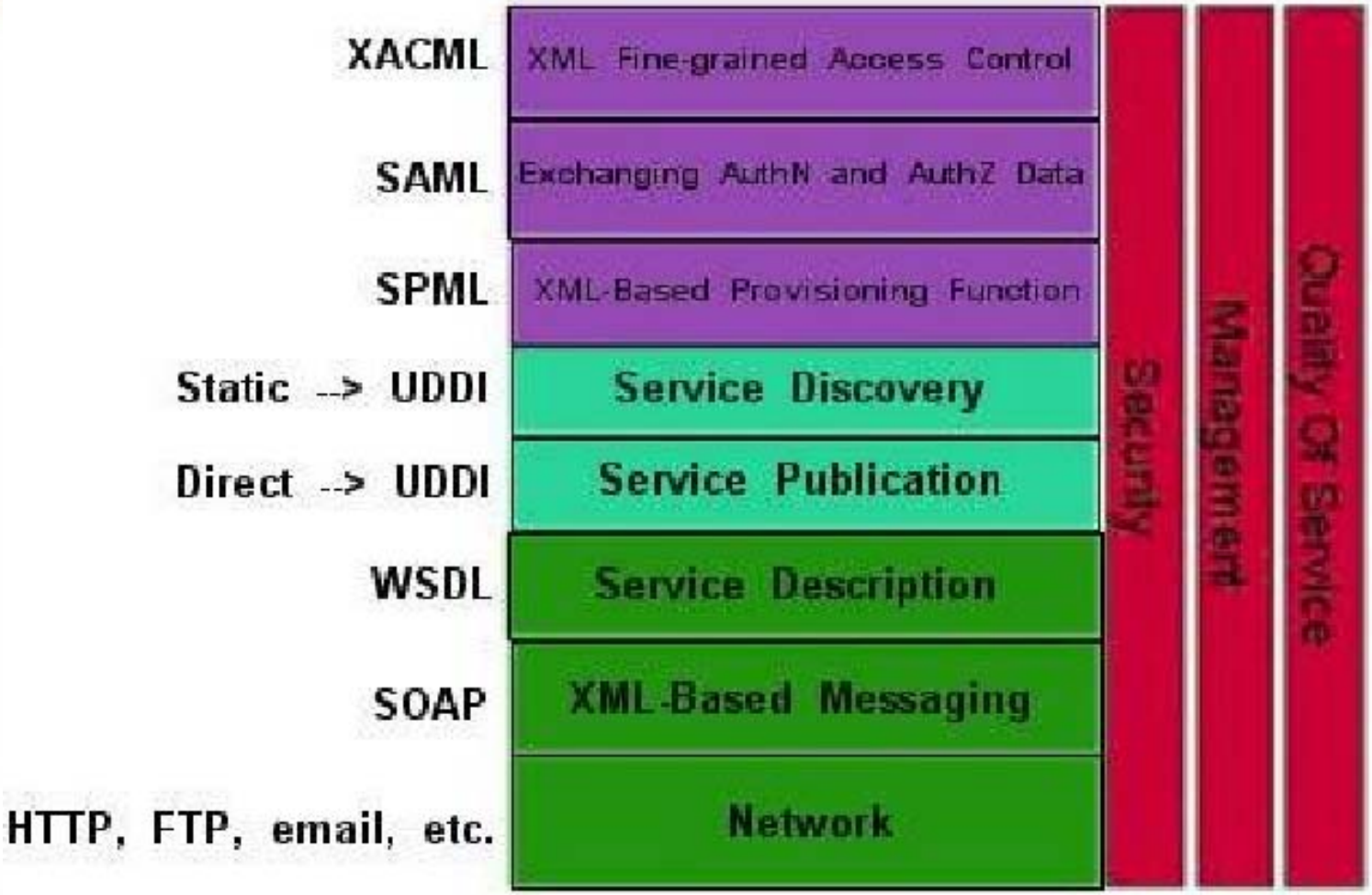
1. A manager makes a change in a personnel system to add an employee.
2. The personnel system, or requesting authority, constructs an SPML document and requests creation of the new employee's accounts across the company.
3. Provisioning system 1 takes the data passed in the SPML document, constructs its own SPML document and executes commands on a set of internal resources to create the employee's accounts in applications, databases, e-mail systems and the like.
4. Provisioning system 1 also forwards an SPML request to provisioning system 2 to add the employee to a 401 (k) system running at a third-party HR service provider.
5. Provisioning system 2 executes commands on a set of internal resources to create the employee's 401 (k) account.
6. Each internal resource reports back success/failure status to the provisioning systems for potential further action, such as notification and retry on a failure.

Aus: Darran Rolls:
SPML eases information exchange
Network World, 06/30/03

DAASI International

Directory Applications
for Advanced Security
and Information Management

Wie passen die Standards zusammen?



Aus: Gavenraj Sodhi: SPML and the importance of it within the Security Infrastructure Framework of eBusiness, Orlando Interoperability Summitt 2002
http://www.omg.org/interop/presentations/2002/Gavenraj_Sodhi.pdf

WfCM

- Spezifikationen der Workflow Management Coalition, einem Standardisierungsgremium, .a.:
  - Workflow Process Definition Interface
  - XML Process Definition Language (XPDL)
    - Datenaustauschformat für Prozessdefinitionen sollte mittels XSLT aus proprietären Definition konvertierbar sein
    - Objekte und Attribute
    - Enthäölt Erweiterungsmöglichkeiten

WfMC Konzept

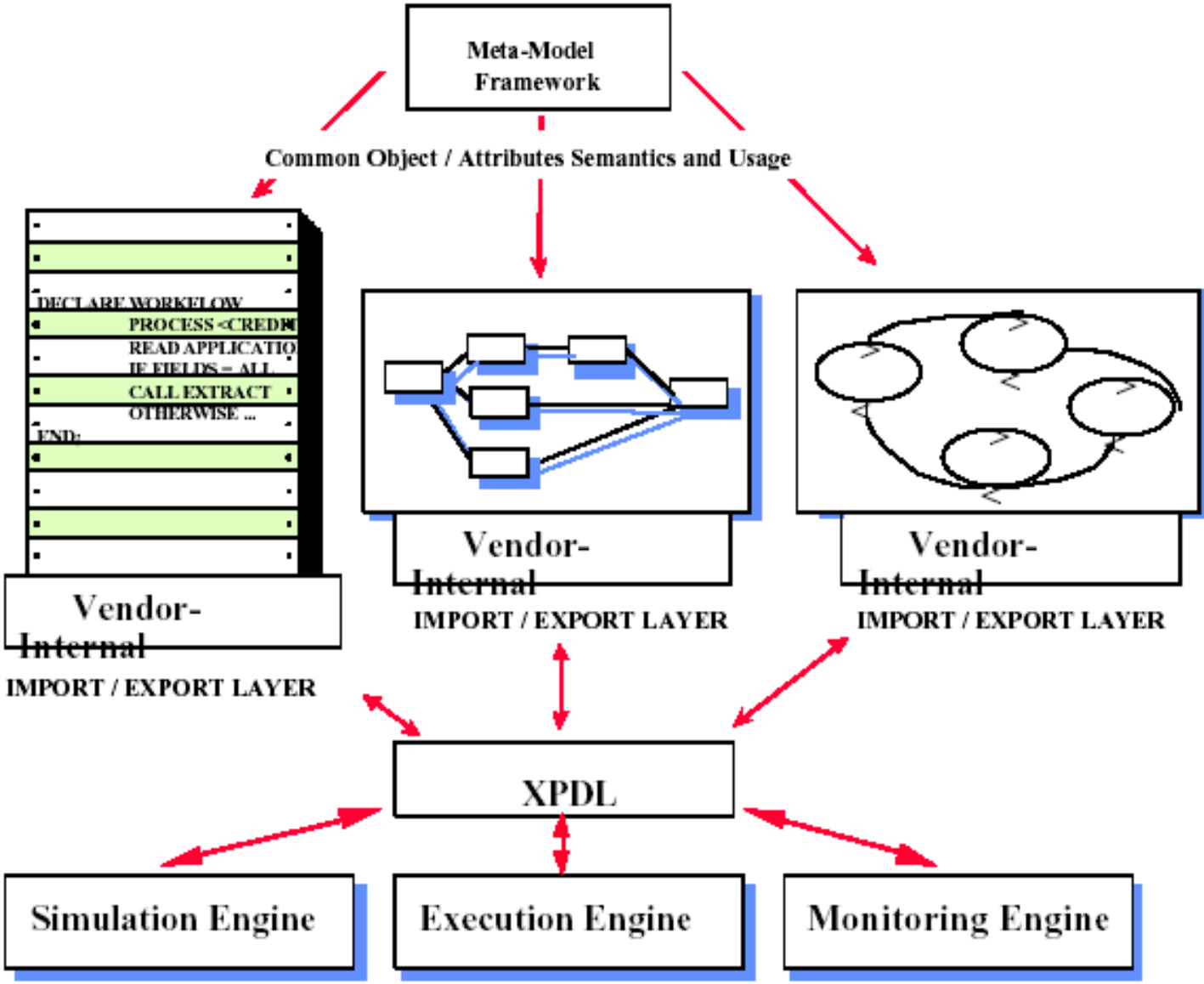


Figure 5-1: The Concept of the Process Definition Interchange

Implementierungen für domainübergreifende AA

Permis

- **PrivilEge and Role Management Infrastructure Standards Validation**
  - Ursprünglich ein EU-Projekt
  - Weiterentwicklungen in England
  - Implementierung einer AA-Software unter Verwendung der X.509 PMI
  - Basiert auf X.509 Attributzertifikaten
  - www.permis.org

DAASI International

Directory Applications for Advanced Security and Information Management

PERMIS PMI

- Rollen basierte Zugriffskontroll-Infrastruktur
- Zugriffskontrolle wird durch eine Autorisierungs-Policy geregelt, die
  - selbst in einem Attributzertifikat gespeichert ist, also von einer AA zertifiziert wurde
  - In XML verfasst ist
- Attributzertifikate werden in einem LDAP-Verzeichnis veröffentlicht

DAASI International

Directory Applications for Advanced Security and Information Management

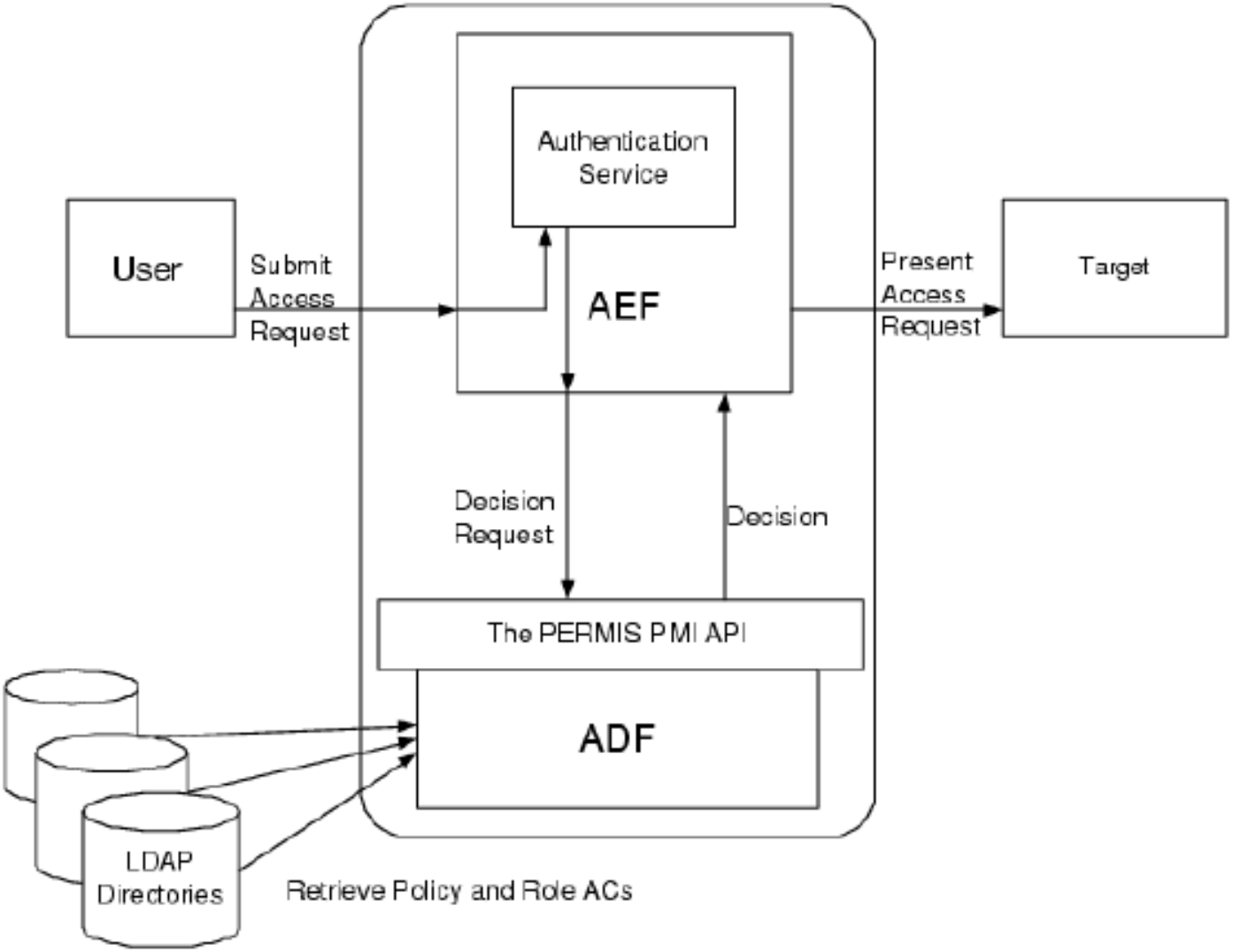
PERMIS Architektur

- Privilege Allocation Subsystem (PAS)
  - ist für die Zuordnung von Rechten zu Benutzern verantwortlich
  - Privilege Allocator (PA)
    - Hiermit werden X.509 Attributzertifikate, die die Zuordnung zu einer Rolle bescheinigen, an Benutzer vergeben
    - und zur Benutzung vom PV-Subsystem in einem LDAP-Verzeichnis gespeichert.
- Privilege Verification Subsystem (PVS).
  - ist für Authentifizierung und Autorisierung des Benutzers zuständig.
  - Die Authentifizierung kann dabei über eine PKI oder eine andere Methode (bespielsweise Login-ID/Passwort) realisiert werden.
  - Access Control Enforcement Function (AEF) für die Authentifizierung
  - Access Control Decision Function (ADF) für die Autorisierung

DAASI International

Directory Applications for Advanced Security and Information Management

Permis Architektur



DAASI International
Directory Applications for Advanced Security and Information Management

Papi

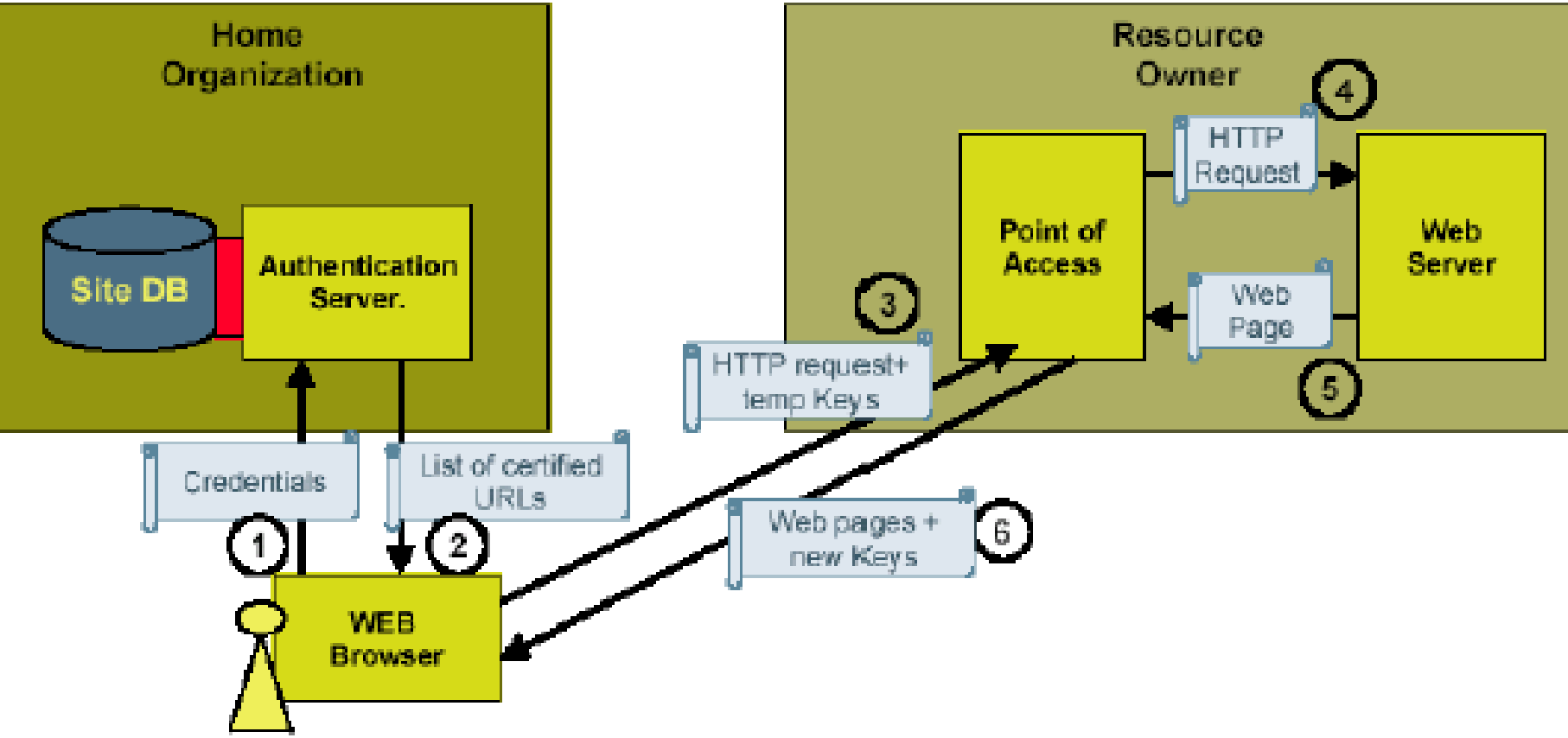
- PAPI: Punto de Acceso a Proveedores de Información
- Ein System welches domänenübergreifend Zugriffskontrolle zu geschützten Ressourcen über das Internet bietet
- Flexible Authentifizierungsmechanismen
  - Jede beteiligte Organisation kann eigenes Authentifizierungsschema verwenden
- Autorisierungsmechanismen für den Benutzer transparent
- Authentifizierung geschieht lokal in Heimatorganisation, Autorisierung geschieht bei der Ressource
- Baut auf Standard-HTTP-Befehlen auf.
- http://papi.rediris.es

DAASI International
Directory Applications for Advanced Security and Information Management

PAPI

- Der Benutzer bekommt, nachdem er sich gegenüber dem Authentication Server (AS) seiner HO authentifiziert hat, eine Liste mit Links zu den Angeboten, die er nutzen darf.
- Diese Links enthalten verschlüsselt Autorisierungsinformationen, die den Ressourcebesitzern an deren Point of Access (PoA) übermittelt werden.
- Nach der Überprüfung der Autorisierungsinformationen dient der PoA als Stellvertreter, der die Anfragen des Benutzers weiterleitet und die folgende Antwort des Webservers an den Benutzer übergibt.

PAPI



DAASI International

Directory Applications for Advanced Security and Information Management

Shibboleth

- Internet2/MACE-Projekt
  - über Architekturen, Regelwerken, und praktischen Technologien zu AA
  - OpenSource Implementierung einer domainübergreifenden AA-Lösung
- Ziel: gemeinsame AA-Infrastruktur für Universitäten in USA

Shibboleth Architekturbestandteile

- Ursprungs Domaine des Benutzers
  - Handle Server
    - Triggert das lokale Campus-Authentifizierungssystem
    - Erzeugt handles und merkt sich Mapping handle/User
  - Attribute Authority
    - Sammelt Attribute von Benutzern
    - Gibt nur notwendige Attribute nach außen
- Domaine die Resource zur Verfügung stellt
  - SHIRE
    - Shibboleth Indexical Reference Establisher
  - SHAR
    - Shibboleth Attribute Requestor
  - WAYF
    - Where are you from
  - Resource Manager

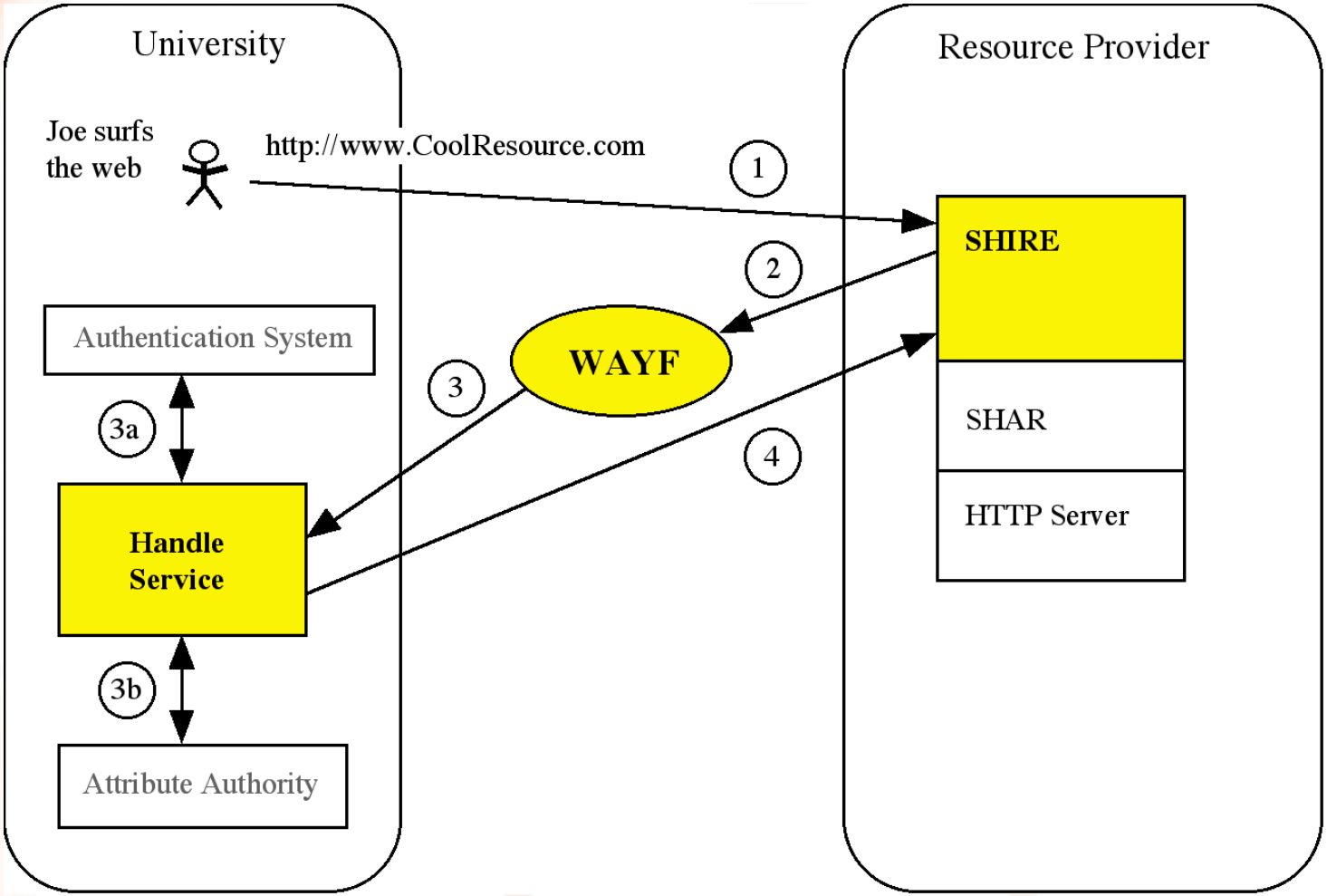
DAASI International

Directory Applications for Advanced Security and Information Management

Shibboleth Architektur

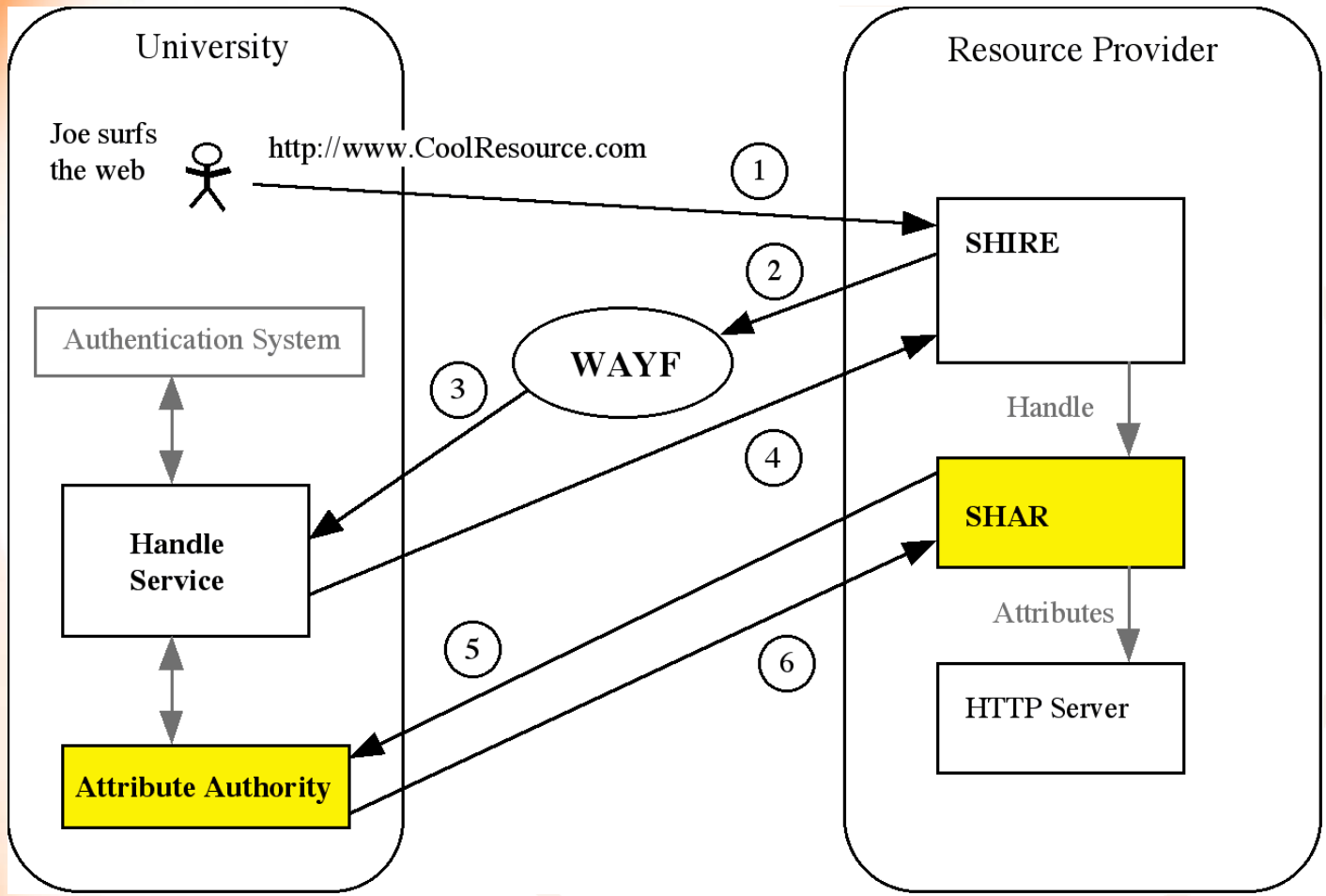
- WAYF (Where Are You From Server)
  - Leitet den Benutzer zurück zu seiner Heimorganisation
- HS (Handle Server)
  - Authentifiziert den Benutzer mit Hilfe der lokalen Authentifizierungsmechanismen.
- AA Attribute Authority
  - Übermittelt auf Verlangen die Informationen, die ein Benutzer freigegeben hat, an den SHAR der Ressource
- SHIRE Shibboleth Indexical Reference Establisher
  - Besorgt einen Handle zu dem Benutzer, ohne weitere Informationen über den Benutzer zu benötigen.
  - Ohne diesen Handle wird der Benutzer zum WAYF-Server umgeleitet, um einen Handle zu besorgen.
- SHAR Shibboleth Attribute Requester
  - Besorgt mit Hilfe des Handles die vom Benutzer freigegebenen Informationen von der AA.
- RM Resource Manager
  - Entscheidet über den Zugriff
  - basierend auf den erhaltenen Informationen.

Shibboleth Authentifizierung



Aus: Ken Klingenstein: Shibboleth Update, ALA May 1, 2002,
http://shibboleth.internet2.edu/shib-presentations.html

Shibboleth Autorisierung



Aus: Ken Klingenstein: Shibboleth Update, ALA May 1, 2002,
http://shibboleth.internet2.edu/shib-presentations.html

DAASI International
Directory Applications for Advanced Security and Information Management

Schemata im Hochschulbereich

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

4.) Schemata im Hochschulbereich

- Einführung in Schema
- X.500/LDAP Schemadefinition
- X.500-Standards
  - Person, organizationalPerson, organization, organizationalUnit
- LDAP-Standards
  - inetOrgPerson, eduPerson, pkiUser, x509PKC, naturalPerson
- Schema-Definitionen in europäischen Forschungsnetzen
- Schema Registry

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)

DAASI International

Directory Applications for Advanced Security and Information Management

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))

DAASI International
Directory Applications for Advanced Security and Information Management

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

DAASI International

Directory Applications for Advanced Security and Information Management

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

USA: Internet2

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

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 )
```

DAASI International
Directory Applications for Advanced Security and Information Management

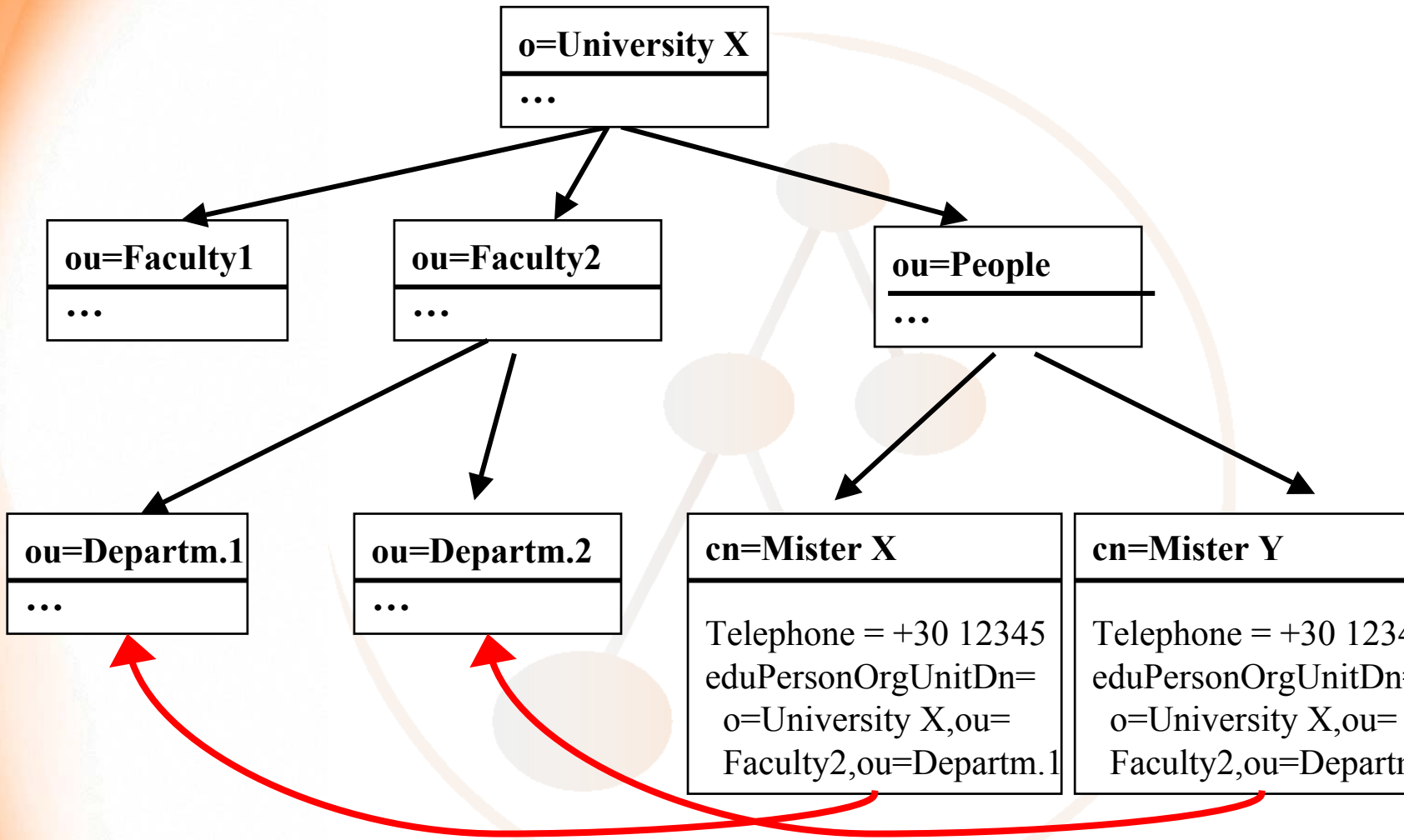
Diskussion über eduPerson

- 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

DAASI International

Directory Applications for Advanced Security and Information Management

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

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

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

DAASI International

Directory Applications for Advanced Security and Information Management

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 manage-ment (65%) and User login management (53%)

DAASI International

Directory Applications for Advanced Security and Information Management

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

DAASI International

Directory Applications for Advanced Security and Information Management

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
- Neue Internet2-Arbeitsgruppe wurde gebildet für Internationalisierung von Hochschulschemata: Intl.Schema

TERENA Projekt Directory Schema Registry (DSR)

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

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

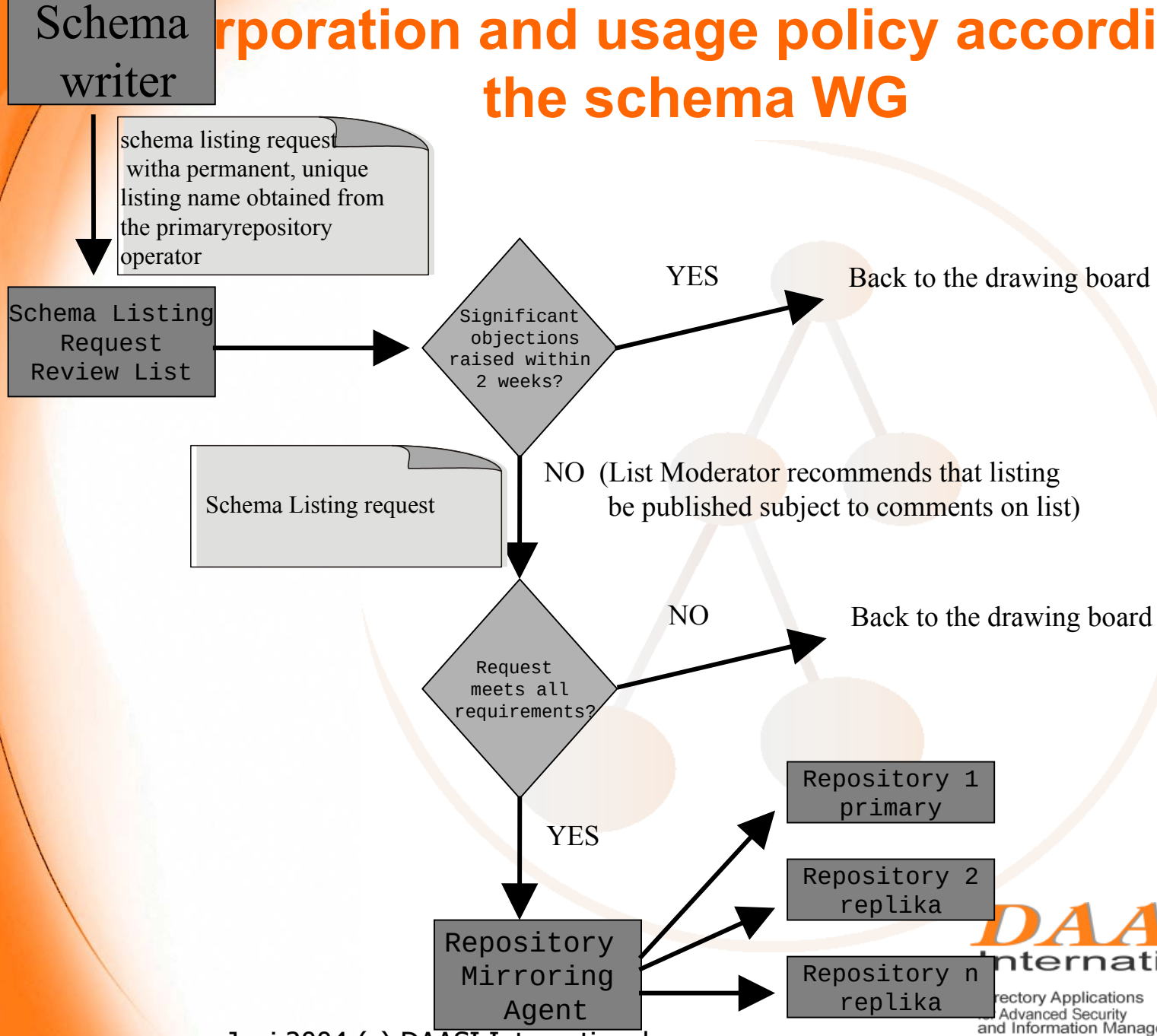
Project Documentation

- 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

DAASI International

Directory Applications for Advanced Security and Information Management

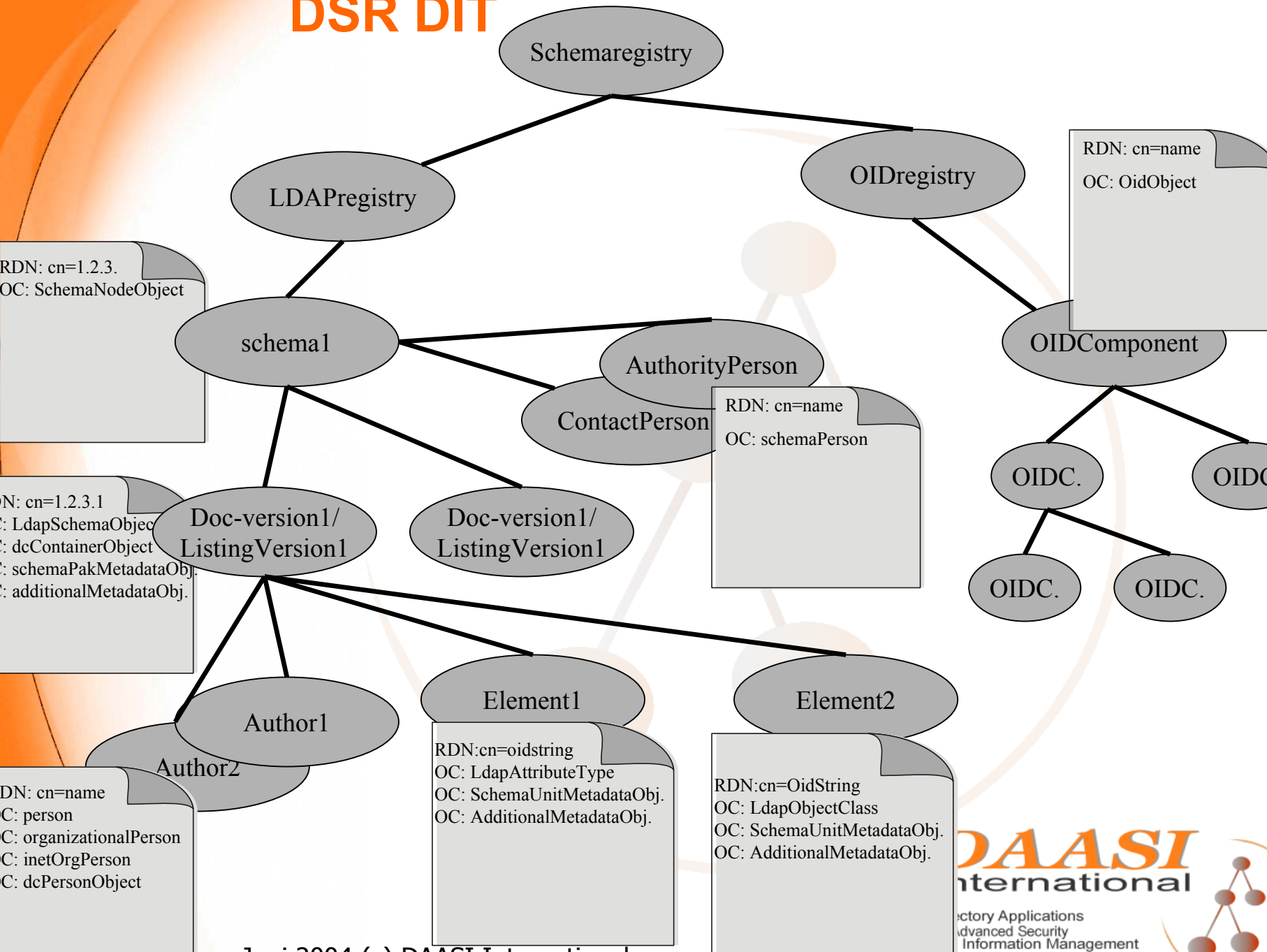
rporation and usage policy according to the schema WG



What info will be stored

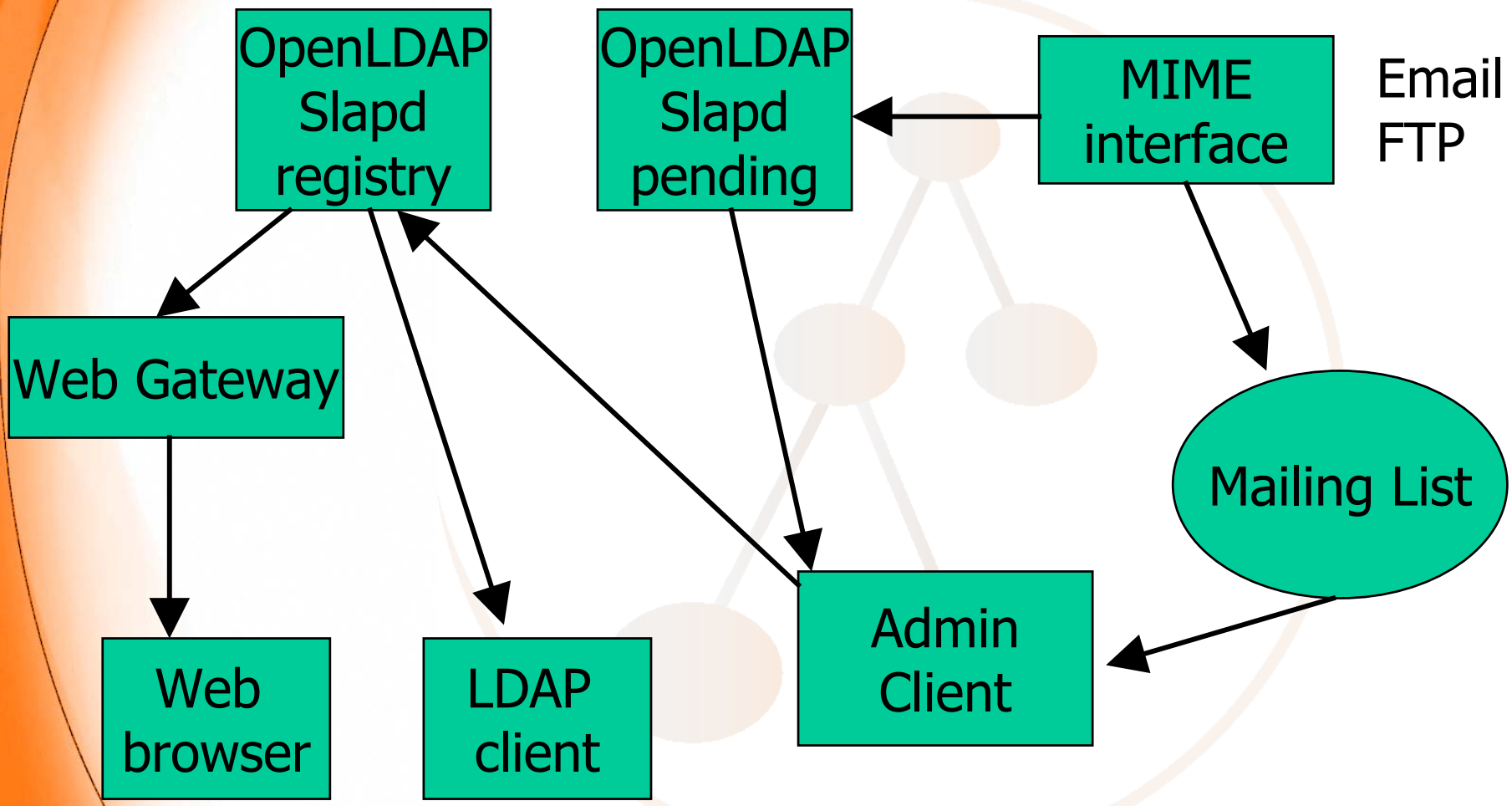
- Metadata on specification document
- LDAP compliant definitions of the schema elements
- Single parts of schema element definitions, e.g., MUST attributes in Object Classes
- Metadata as specified by the IETF WG schema
- Separate OID tree
- Additional metadata

DSR DIT



DAASI
nternational
ctory Applications
dvanced Security
Information Management

DSR Workflow



DAASI International

Directory Applications for Advanced Security and Information Management

Produktübersicht Identity Management

DAASI International

Directory Applications
for Advanced Security
and Information Management

i 2004 (c) DAASI International

Was ist bei einem LDAP-Projekt zu beachten

- Wie üblich: zuerst Anforderungen analysieren
- Schema Design
  - Zuerst schauen, was für Schema es schon gibt (Standards verwenden!)
    - In Zukunft einfach bei www.schemareg.org vorbeischauen
  - Sorgfalt bei eigenen Objektklassen und Attributtypen
- Workarounds vermeiden wie
  - Schemacheck off
  - Extensible object
- DIT-Struktur Design
- Spezifizierung der Client-Anwendungen

DAASI International

Directory Applications for Advanced Security and Information Management

Anforderungen

- Nach der Analyse können Anforderungen spezifiziert werden
  - Implementierbarkeit der Datenflüsse
  - Schnittstellen zu Datenbanken spezifizieren
  - Anforderungen an Daten-Management-Funktionalität
  - Anforderung an Datenmengen
  - Anforderungen an Performance

Erst dann kommt die Produktwahl

- Kriterien:
  - Plattformunterstützung
  - Standardkonformität
  - Leistungsumfang
  - Anpassbarkeit
  - Performance
  - Vorlieben in der eigenen Community
  - Lizenzmodell
  - Sonderkonditionen für Hochschulen
    - Oft nur wenn mehrere Organisationen gemeinsam beschaffen

DAASI International

Directory Applications for Advanced Security and Information Management

Open Source Software

- + Herstellerunabhängigkeit
- + Grössere Sicherheit:
  - Keine versteckten „Hintertüren“
  - Sicherheitspatches oft schneller entdeckt und behoben
- + Größere Flexibilität
  - Man kann benötigte Features selbst implementieren (lassen)
- + Keine Lizenskosten
- - Roadmaps mancher OpenSource-Projekte werden nicht eingehalten
  - Zur Risiko-Verminderung sollte man zur Not selber am Code arbeiten können
  - Oder Support einkaufen

DAASI International

Directory Applications for Advanced Security and Information Management

Probleme der Produktübersicht

- Grosse Anzahl von Produkten
- Grosse Fluktuation
  - Firmen werden aufgekauft
  - Allianzen geschnürt
- Test von Verzeichnisdienstprodukten sehr aufwendig
- Performancetests abhängig von Konfiguration
- Ein wirklich guten Überblick zu erstellen ist sehr Zeit- und Kostenaufwendig
- Das hier Gebotene ist also in vielerlei Hinsicht mit Vorsicht zu genießen

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP-Server-Implementierungen (Auswahl)

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

DAASI International
Directory Applications for Advanced Security and Information Management

Juni 2004 (c) DAASI International

5.) Produktübersicht Identity Management

- Kurze Marktübersicht, woher kommen die Player
- Marktstrategien (Entwickeln, Aufkaufen, Partnerschaften)
- Die wichtigsten Produkte:
  - Calendra
  - Computer Associates
  - IBM Tivoli
  - MaxWare
  - Microsoft
  - Novell
  - Siemens
  - Sun
- LDAP eine Provisioning-Alternative?

DAASI International

Directory Applications for Advanced Security and Information Management

Klassifikation der Player

- Heutige Provisioning-Produkte-Hersteller kommen aus verschiedenen Bereichen:
  - Sicherheits Management
  - Passwort Management
  - Verzeichnisdienste
  - Reine Provisioning-Hersteller
  - Identity Management Suites
  - Netzwerk-Betriebssysteme
  - Web Zugriffs Management

DAASI International
Directory Applications for Advanced Security and Information Management

Marktstrategien

- Nachdem Provisioning-Systeme im Markt Erfolg haben, mußten Hersteller reagieren
  - Kleine Start-Up-Firmen die sich auf Provisioning spezialisiert haben:
    - Waveset, Access360, Metamerge, Business Layers, Thor Technologies, TruLogica
  - Große Firmen kaufen solche kleineren spezialisierten Firmen auf:
    - IBM kauft Access360 und Metamerge, Sun kauft Waveset, Netegrity kauft Business Layers
  - Große Firmen gehen Partnerschaften ein:
    - Entrust mit Waveset, RSA mit Thor, Microsoft mit Netegrity/Business Layers und anderen.

Produktübersicht

- Basiert nur auf gelesenem
- Keine Tests durchgeführt
- Übersicht nur Skizzenhaft
- Nur eine Auswahl der auf dem Markt befindlichen Produkte
- Keine Preisinformationen
- Keine Produktversionen
- Stand Anfang 2004

DAASI International

Directory Applications
for Advanced Security
and Information Management

Calendra

- Französische Firma mit Hintergrund in Whitepages- und Yelowpages Anwendungen
- Provisioning-Lösung baut auf den Calendra Directory Manager einer auf Java und XML basierenden Virtual-Directory-Lösung
- Konnektoren für LDAP, RDBM und XML-Datenspeicher
- Statische und dynamische Rollen
- Workflow Ad-On
- Auditing und Report-Generator
- Eigene Konnektorenentwicklung mit Calendra Design Studio

DAASI International

Directory Applications for Advanced Security and Information Management

Computer Associates

- Eine der größten Software-Firmen
- eTrust Identity and Access Management Suite
  - Access Control
  - SSO
  - Web Access Control
  - Directory
  - Web Services Management
  - Audit
  - Admin (=Provisioning)

DAASI International

Directory Applications
for Advanced Security
and Information Management

Computer Associates

- Drei Schichten:
  - Benutzer Interface zur Konfiguration und Self-Service-Funktionen mit Profile und Rollen Management
  - Provisioning Engine verarbeitet Workflows und policies, Reportgenerator
  - Data Connectors Schnittstelle zu den provisionierten Systemen. Neben spezialkonnektoren wird ein universeller SPML-Konnektor mitgeliefert

DAASI International

Directory Applications for Advanced Security and Information Management

IBM Tivoli

- Tivoli Identity Manager = Access360 enRole
- Features:
  - Policies und Roles (RBAC)
  - Workflow Management (WfMC-Kompatibel)
  - Sehr viele Konnektoren
  - Konektorentwicklung mit IBM Directory Integrator (=Metamerge)
  - Self service Passwort Reset
  - Auditing (auch dezentral gemachter Änderungen) und Reportgenerator
- Netzwerkprotokoll DSML über HTTPS mit bidirektionaler Authentifizierung für Import und Export

DAASI International

Directory Applications for Advanced Security and Information Management

IBM Tivoli

- Drei Schichten:
  - IBM Websphere als Frontend mit Servlets
  - Enterprise JavaBeans Schicht mit Provisioning-Logik
  - Datenbank (DB2) oder Directory (Tivoli Directory Server oder Fremdprodukt) als Datenbackend
- Gesamtintegration in Tivoli-Suite noch nicht realisiert

MaxWare

- Norwegische Firma und ursprünglich Directory-Hersteller
  - MaxWare MetaCenter Virtual Directory
  - DirectoryExplorer: LDAP-Client der sich in den MS Explorer integriert
- Directory Synchronization Engine mit Provisioning-Funktionalität
  - Workflow
  - Benutzer Self-Service-Schnittstelle
  - Passwort-Reset
- MaxWare möchte in Europa expandieren, auch in Deutschland

DAASI International
Directory Applications for Advanced Security and Information Management

Microsoft

- Ist in das Metadirectory-Geschäft durch Aufkauf von Zoomit eingetreten
- Das Zoomit Produkt wurde zuerst als Microsoft Metadirectory Services (MMS) vermarktet und weiterentwickelt zu Microsoft Identity Integration Server (MIIS)
- Nur in Verbindung mit den Produkten der Partnerfirmen vollständiges Provisioning-Produkt

Novell

- Marktführer im Metadirectory-Bereich durch sehr frühen Einsatz von XML
- eDirectory und DirXML
- Nsure Identity Manager heißt das neue IdM- und Provisioning-Produkt auf Basis dieser Technologien
  - eGuide als Selfservice-Komponente
  - iManager als Administrator-Interface
  - Audit-Funktion mit realtime monitoring
  - Passwort-Management, Pw-Policy und Synchronisierung!
  - Programmlogik mit XSLT modellierbar
  - Viele Konnektoren
  - Rollen (statisch und dynamisch), Policy und Workflow

DAASI International

Directory Applications for Advanced Security and Information Management

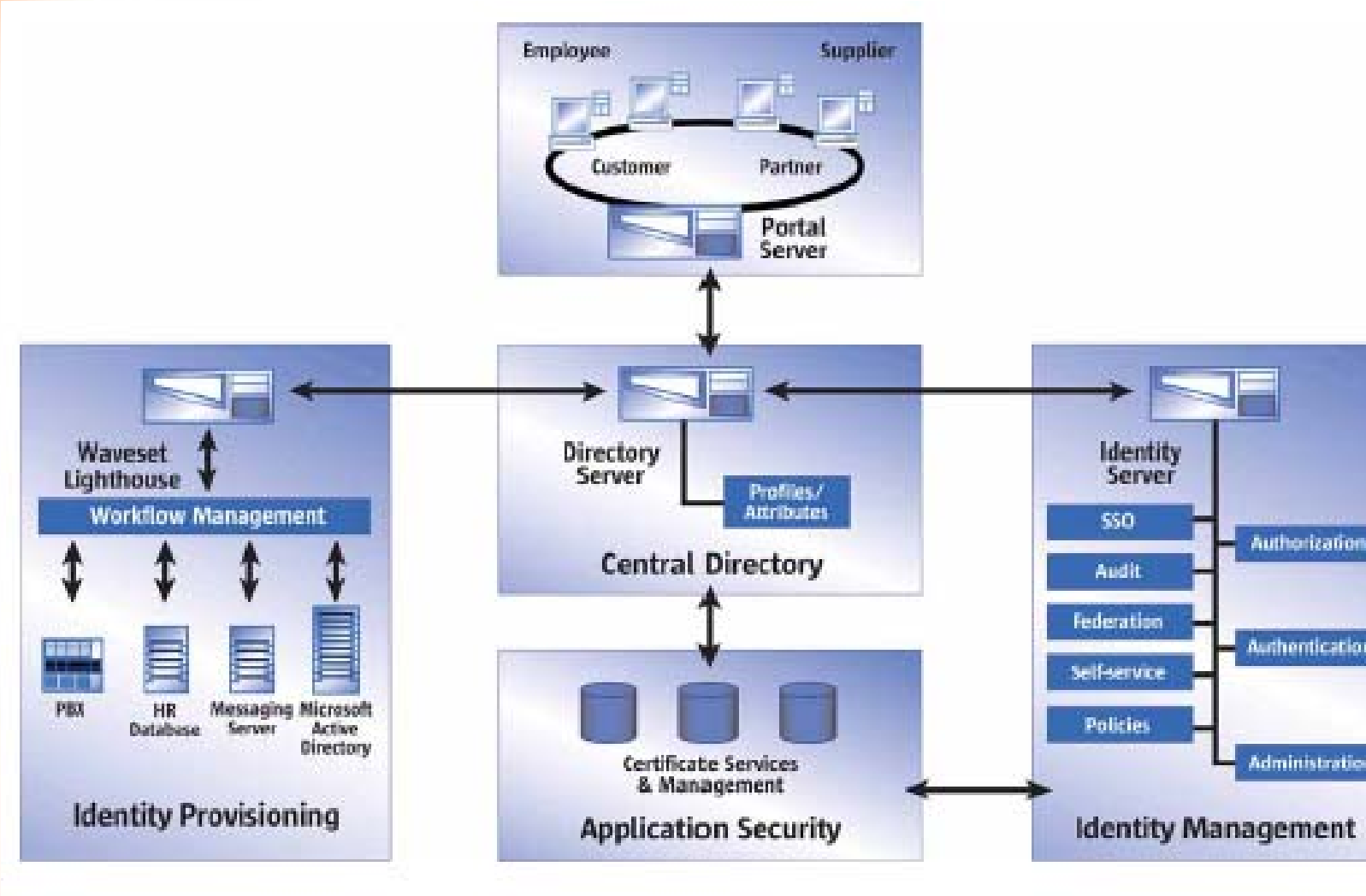
Siemens

- Hat sehr lange Directory-Erfahrung (DirX seit 1991)
- Metadirectory DirXMetahub und DirXmetaRole für RBAC bilden zusammen das IdM
  - Policy basiertes Provisioning
  - Passwort-Verschlüsselung
  - Webfrontend
  - Workflow Management
  - Konnektoren für RDBMs, LDAP und XML
- Unterstützt DSMLv2, SOAP, XSLT, SPML und XML

Sun/Waveset

- Mit dem Aufkauf von Waveset (Produkt Lighthouse) und dem eigenen Directory-Produkt kann Sun eine vollständige IdM-Lösung anbieten
  - Datenbackend ist ein Virtual Directory mit LDAP und XML Interface
  - RBAC, Policy Management, SSO
  - Workflow Management WfMC-kompatibel
  - Unterstützt J2EE und SOAP, Liberty Aliance, SAML und SPML
  - Sehr schnelle Provisionierung
  - Wiederherstellungsfunktionen
  - Eigene Skript-Sprache XPRESS

Sun Architektur



Aus: Data Sheet Sun Infrastructure Solution for Identity Management

6.) Identity Management an deutschen Hochschulen

- Organisatorische Probleme
- Kostenfaktoren
- Projektbeispiele
- Projektidee Metadirectory Kompetenzzentrum

DAASI International

Directory Applications
for Advanced Security
and Information Management

Organisatorische Probleme

- Ein Universität ist ein sehr heterogenes Gebilde
  - Zentrale Verwaltung mit verschiedenen Dezernaten
  - Zentrale Einrichtungen
  - Lehrstühle
- Viele haben viel zu sagen, niemand hat alles zu sagen
- Zuständigkeitsgerangel
- Arbeitsdelegierung
- Ein IdM-Projekt kann nur erfolgreich sein, wenn alle mitmachen, insbesondere:
  - Rektorat
  - HR in der zentralen Verwaltung
  - RZ und UB

DAASI International

Directory Applications for Advanced Security and Information Management

Kostenfaktoren

- Ist-Kosten
  - Redundante Datenpflege kostet sehr viel
- IdM-Kosten
  - Die Einführung eines IdM-Systems ist nicht billig:
    - Beratungskosten
    - Entwicklungskosten
    - Implementierungskosten
    - Lizenzkosten
  - Nach Abschluss der Einführung sollten Kosten eingespart werden können
    - Vorausgesetzt sie geben nicht zuviel für Software-Lizenzen aus

DAASI International
Directory Applications for Advanced Security and Information Management

Projektbeispiel

- Ist-Analyse und Anforderungsanalyse
- Pflichtenheft für Aufbau eines Mitarbeiterverzeichnisses
- Definition des LDAP Schemas und LDIF Datenformat unter Berücksichtigung der Standards
- Design der Software
- Implementierung auf Grundlage von OpenLDAP und einem Web-to-LDAP-Gateway
- Einpflegen der über LDIF zur Verfügung gestellten LDIF-Daten
- Installation und Konfigurierung von webformularbasierten Datenänderungsmöglichkeiten
- Dokumentation, die einen Betrieb ermöglicht

DAASI International

Directory Applications for Advanced Security and Information Management

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
- Eine ZKI-Arbeitsgruppe zu Verzeichnisdiensten kümmert sich um den gesamten Komplex Identity Management und Metadirectories
- Bitte setzen Sie sich bei Interesse mit uns in Verbindung

DAASI International

Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit!

- Noch Fragen ?

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

DAASI International

Directory Applications
for Advanced Security
and Information Management