Projektidee
Metadirectory Kompetenzentrum

ZKI AK Zentrale Verzeichnisdienste

HU-Berlin 9.12.2003

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International

Directory Applications
for Advanced Security
and Information Management

Agenda

- Verzeichnisdienste und Identity Management
- Metadirectory und Provisioning
- Projektidee Metadirectory Kompetenzzentrum

DAASI International

Directory Applications
for Advanced Security
and Information Management

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

DAASI International GmbH

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

DAASI International

Directory Applications
for Advanced Security
and Information Management

Wofür wir stehen

- Leistungen: Consulting, Implementierung, Hosting, Datenmanagement und –konvertierung, Schulung
- Vorlieben: Offene Standards, Open Source, Datenschutz, Forschung
- Kundenzielgruppen: v.a. Forschungseinrichtungen, Bibliotheken, Behörden
- Projekte: TERENA, deutsche Universitäten, DL-Forum
- Expertise: Verzeichnisdienste, Authentifizierung, PKI, Informationsmanagement, DL, XML, Grid Computing
- Standardisierungsaktivitäten: IETF, Internet2, GGF

DAASI International

Directory Applications
for Advanced Security
and Information Management

Verzeichnisdienste und Identity Management

DAASI International

Directory Applications
for Advanced Security
and Information Management

Identität in Identity Management

- Eindeutige Kennung, die eine Person gegenüber einem Computersystem identifiziert
  - Z.B. Login-Id, einen Zusammenhang mit einer Person bedeutet
- 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.

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

DAASI International

Directory Applications
for Advanced Security
and Information Management

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

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

DAASI International

Directory Applications
for Advanced Security
and Information Management

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

DAASI International
Directory Applications for Advanced Security and Information Management

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 kann 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

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.

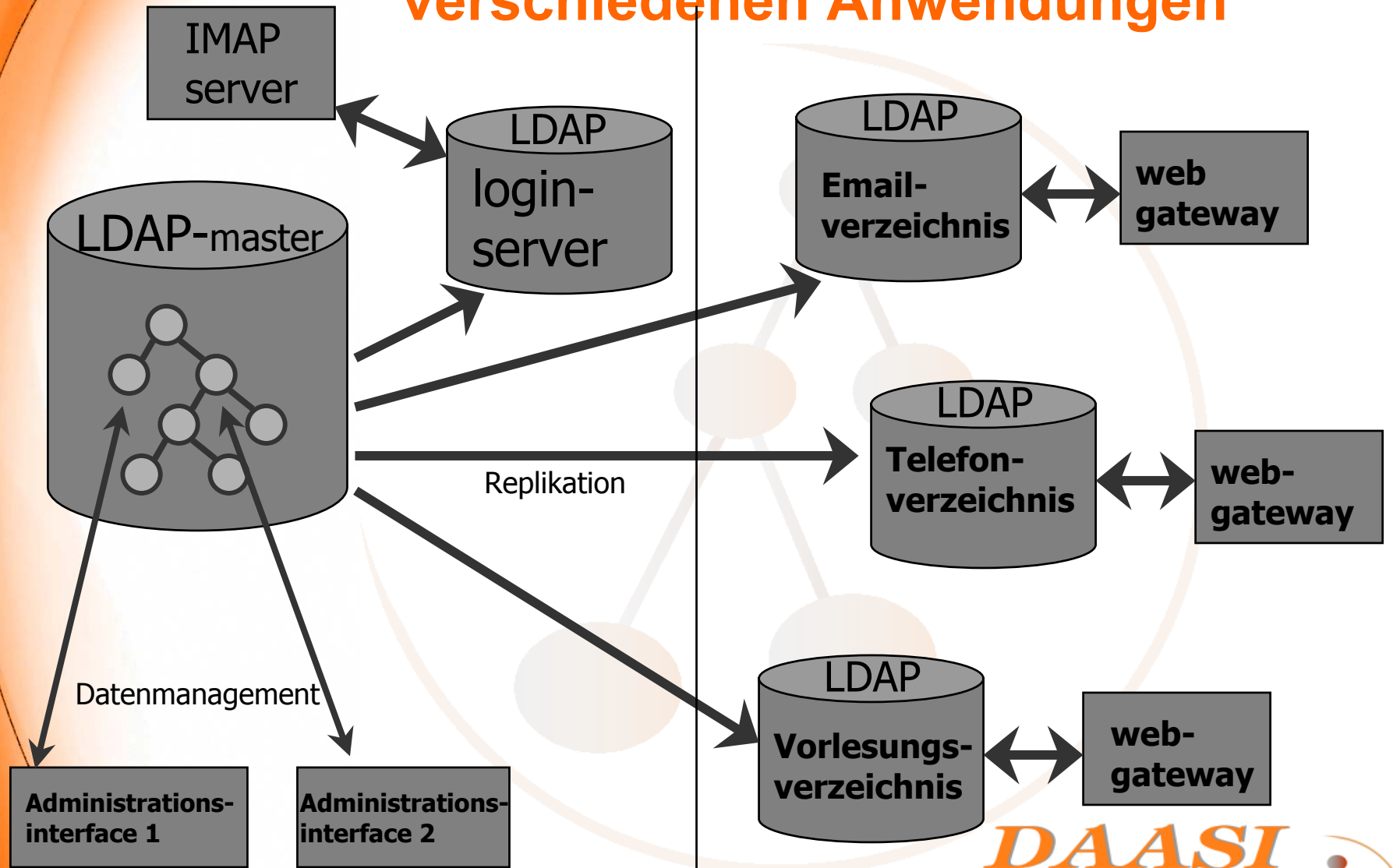
Erweiterbarkeit von Verzeichnisdiensten

- 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

Beispiel für zentrales Verzeichnis mit verschiedenen Anwendungen



DAASI International

Directory Applications for Advanced Security and Information Management

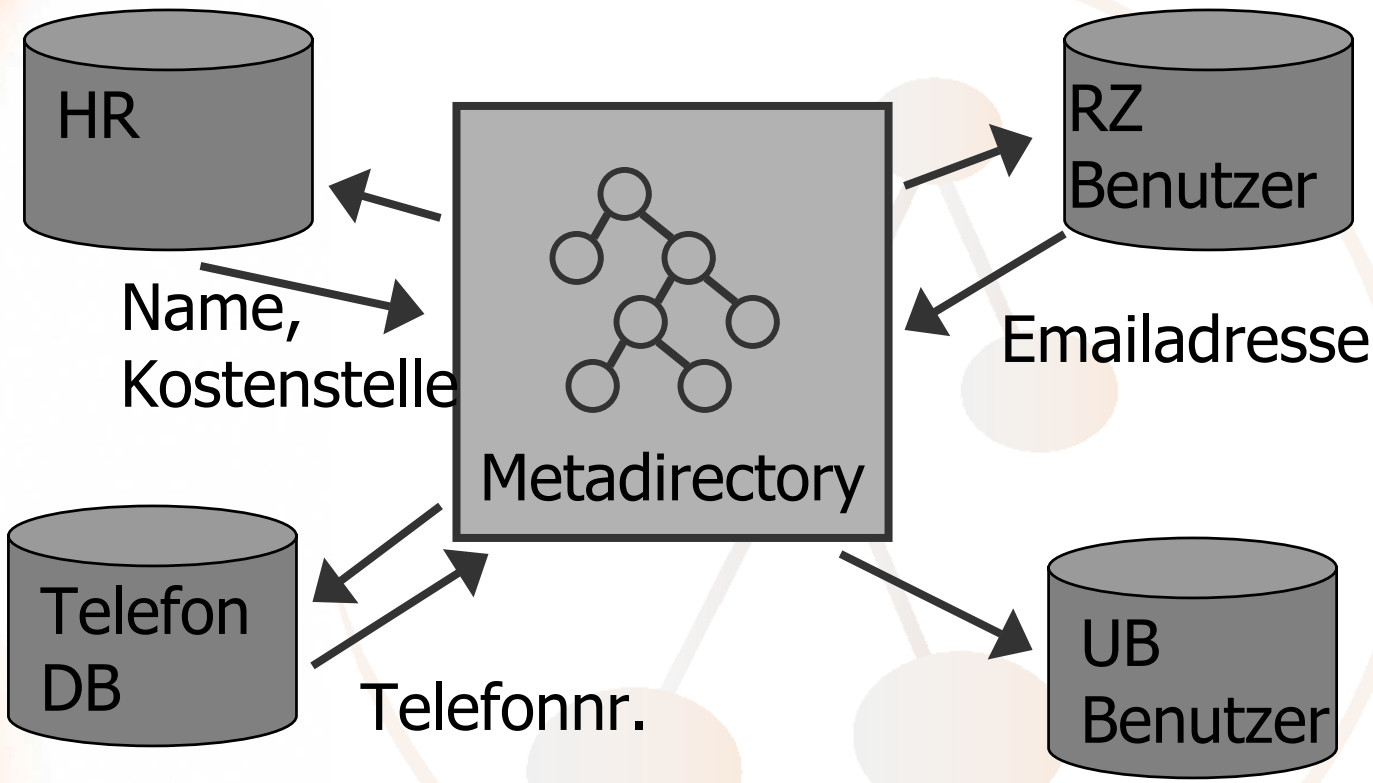
Metadirectory – die realistischere Alternative?

- 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

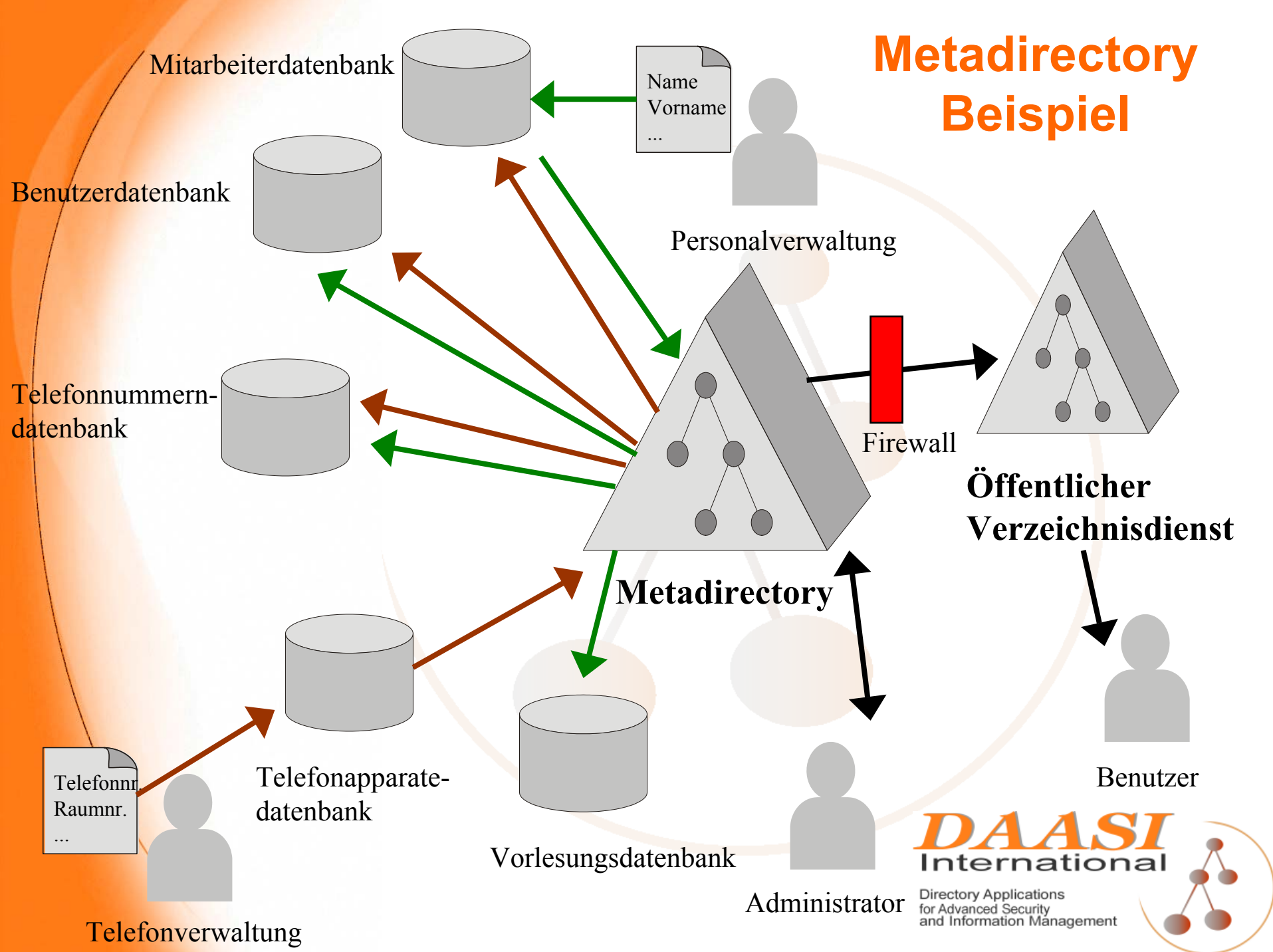
Metadirectory Beispiel einer Universität



DAASI International

Directory Applications
for Advanced Security
and Information Management

Metadirectory Beispiel



Metadirectory Implementierungen

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

DAASI International

Directory Applications
for Advanced Security
and Information Management

Provisioning Systeme

- LDAP setzt sich als offener Standard durch
- Hersteller haben aber proprietäre Provisioningsysteme die sie integrieren wollen
- Alternative: Provisioning durch LDAP
  - 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
- Vorteile:
  - wirkliche Herstellerunabhängigkeit und damit Flexibilität in derSoftwarewahl
  - Flexibilität bei den Ausnahmen
  - Kostenersparnis durch Realisierbarkeit mit Open-Source-Software

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
- Diese ZKI-Arbeitsgruppe zeigt das große Interesse am Thema Metadirectory
- Wie weit gehen die Synergie-Effekte?

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