Identity Management mit OpenLDAP

Peter Gietz, DAASI International GmbH

Perspektive Open Source Forum

Systems München, 24.10.2007

DAASI International

Directory Applications
for Advanced Security
and Information Management

Agenda

- Was ist Identity Management
  - Problemstellung
  - Organisatorische Workflows
  - Komponenten
  - Abbildung in EDV-Prozessen
- OpenLDAP und Identity Management

DAASI International
Directory Applications for Advanced Security and Information Management

Ausgangsposition vor Identity Management

- Historisch gewachsene Infrastrukturen und Prozesse
- Isolierte, voneinander unabhängige Verzeichnisse und Datenbanken mit den gleichen Identitätsdaten
  - keine Interaktion
  - kein Vertrauen bezüglich der Richtigkeit der Daten
- Jede dieser Datensammlungen hat
  - eigene Administratoren
  - Benutzerverwaltungen
  - Zugriffskontrollmechanismen
- Redundanz der Daten und der Datenpflege
  - => Mehrfacharbeit

DAASI International
Directory Applications for Advanced Security and Information Management

Probleme

- Benutzer brauchen Login-Accounts für jeden Computer und jede Anwendung
  - müssen sich viele Passwörter merken
- Administratoren
  - verwenden verschiedene Tools
  - haben verschiedene Regeln und Prozesse
- verschiedene Authentifizierungsmechanismen
- Identitätsinformationen sind in verschiedenen Datensammlungen unterschiedlich
  - unterschiedliche Daten: Meyer vs. Meier
  - unterschiedliche Datenschemata: Nachn vs. Nachname
- Jede neue Anwendung vergrößert den Leidensdruck

DAASI International
Directory Applications for Advanced Security and Information Management

Noch mehr Probleme

- Prozesse sind langsam
- 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

DAASI International
Directory Applications for Advanced Security and Information Management

Identity Management löst solche Probleme

- **Definition von Spencer C. Lee:**
  - ***Identity Management bezieht sich auf den Prozess der Implementierung neuer Technologien zum Verwalten von Informationen über die Identität von Nutzern und zur Kontrolle des Zugriffs auf Firmenressourcen.***
  - ***Das Ziel von Identity Management ist es Produktivität und Sicherheit zu erhöhen und gleichzeitig Kosten der Verwaltung von Benutzern, ihrer Identitäten, Attribute und Berechtigungsnachweise zu senken***

DAASI International
Directory Applications for Advanced Security and Information Management

Was ist neu an Identity Management?

- Benutzerverwaltungen gibt es seit den Anfängen der EDV
  - etc/passwd in Unix ist auch Benutzerverwaltung!
  - Die Probleme sind die alten
- Identity Management Systeme sorgen dafür dass
  - man ein Gesamtkonzept der IT-Landschaft entwickelt
  - Daten aus autoritativen Datenquellen kommen und nicht überall neu eingetippt werden müssen
  - Die Benutzerverwaltung automatisiert wird
- Automatisierte Prozesse bewirken, dass
  - Berechtigungen gleich nach der Einstellung zur Verfügung stehen
  - aber auch gleich nach dem Austritt aus der Organisation entzogen werden können

DAASI International
Directory Applications for Advanced Security and Information Management

Organisatorische Prozesse

- Mitarbeiter
  - 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

DAASI International
Directory Applications for Advanced Security and Information Management

Welche Prozesse finden genau statt?

- HR-Abteilung trägt Mitarbeiterdaten in Datenbank(en) ein
- Mitarbeiter
  - füllt für verschiedene Dienste am RZ (Email, Rechneraccount, ...) verschiedene Formulare aus
  - beantragt ein Telefon
  - wird in verschiedenen Verzeichnissen aufgenommen
  - arbeitet mit verschiedenen Rechnern und Anwendungen
- Weitere Prozesse werden beim Wechsel des Namens, Wohnorts, Arbeitsplatzes, Arbeitsvertrag, sowie bei der Beendigung des Arbeitsverhältnisses angestoßen

DAASI International
Directory Applications for Advanced Security and Information Management

Datenverwaltung z.B. an einer Kommune

- IdM-Daten werden an verschiedenen stellen verwaltet:
  - von der Personalverwaltung in einer Mitarbeiter-Datenbank, z.B. für Lohnbuchhaltung und Abrechnung der Urlaubstage
  - von der Systemadministration in einer Benutzerdatenbank, z.B. für 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 Betriebsamt, z.B. für die Verwaltung von Telefonapparaten und –anschlüssen
  - vom Presseamt, z.B. für die Erstellung eines gedruckten/elektronischen Mitarbeiterverzeichnisses und für Adressenlisten für postalischen Versand von Mitteilungen etc.
- Identity Management kann nur von der Organisationsleitung durchgesetzt werden!

DAASI International
Directory Applications for Advanced Security and Information Management

Was gehört zu Identity Management?

- Quelldatenbanken
  - authoritative Datenquellen
- Verzeichnisdienste sind zentrale Bestandteile
  - speichern Identitätsinformation, Passwörtern, Zertifikate, Rollen und Berechtigungen, Policy
  - Standards: X.500, LDAP
  - Implementierungen: OpenLDAP, Novell eDirectory, MS Active Directory
- Metadirectories dienen zur
  - Synchronisierung verschiedener Datenspeicher
  - Vermeidung von Inkonsistenzen
  - Passwort-Verwaltung und –Synchronisierung
- Konnektoren verbinden
  - Datenquellen mit Metadirectory
  - Metadirectory mit Zielsystemen (Provisioning)

DAASI International
Directory Applications for Advanced Security and Information Management

Vorteile von LDAP

- Standardisiertes Netzwerkprotokoll
- Objektorientiertes Datenmodell
  - Objektklassen
  - MUST und MAY-Attribute
  - Matching Rules
  - Multi Value Felder
- Hierarchische Datenstruktur
- Standardisiertes Schema
- Flexible Erweiterungsmöglichkeiten
- Optimiert für Lesezugriff
- Standard Authentifizierungsmechanismen
  - viele Anwendungen unterstützen LDAP anstelle einer eigenen Benutzerverwaltung

DAASI International
Directory Applications for Advanced Security and Information Management

Was gehört noch zu Identity Management?

- Policy Management
  - Oberfläche zur Verwaltung von Berechtigungen
  - Kann rollenbasierte Zugriffskontrolle konfigurieren
- Work Flow Management
  - Grafische Oberfläche zum Spezifizieren der Abläufe bei Neueinstellung, Datenänderungen, etc.
  - Spezifiziert genau welche Attribute von wo nach wo fließen sollen
- Auditing
  - Logged alle Transaktionen in eine Datenbank
  - Lässt jede Änderung der Account-Daten und Berechtigungen verfolgen

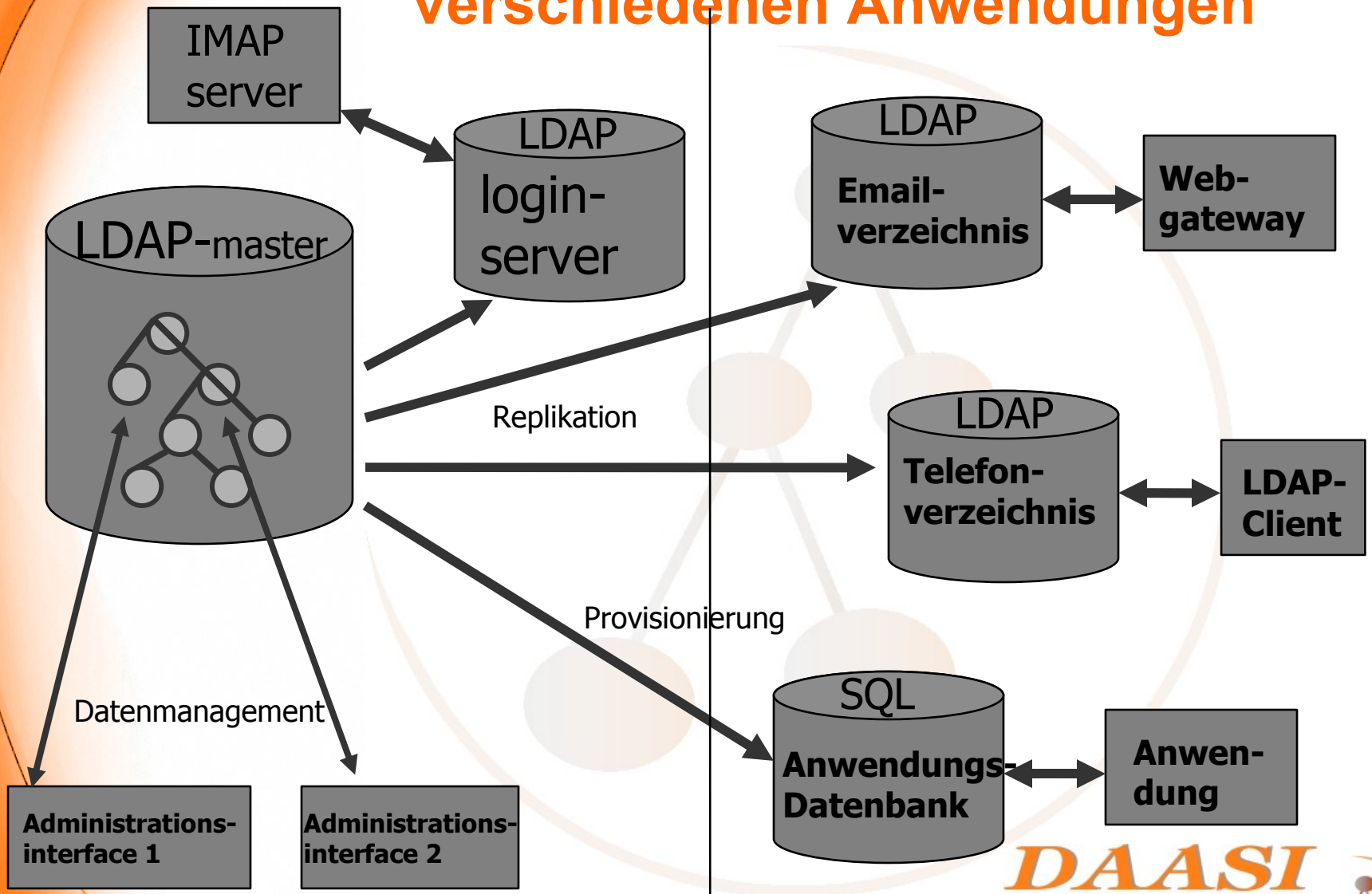
DAASI International
Directory Applications for Advanced Security and Information Management

Zentraler Verzeichnisdienst

- Konsolidierung durch Migration einzelner Anwendungen auf Verzeichnis-Datenbasis
- Eine Datenbasis für verschiedene Dienste
  - Z.B.: Eine Datenstruktur, beliebig verteilt und/oder (teil)repliziert für:
    - Emailverzeichnis
    - elektronisches Telefonbuch
    - Benutzerverwaltung und Authentifizierungsdienst
    - Elektronisches Adressenverzeichnis
  - Dies führt zu erheblichen Kosteneinsparungen
- Verschiedene Daten können in verschiedene Verzeichnisdienste repliziert werden
  - Ausfallssicherheit
  - Lastverteilung

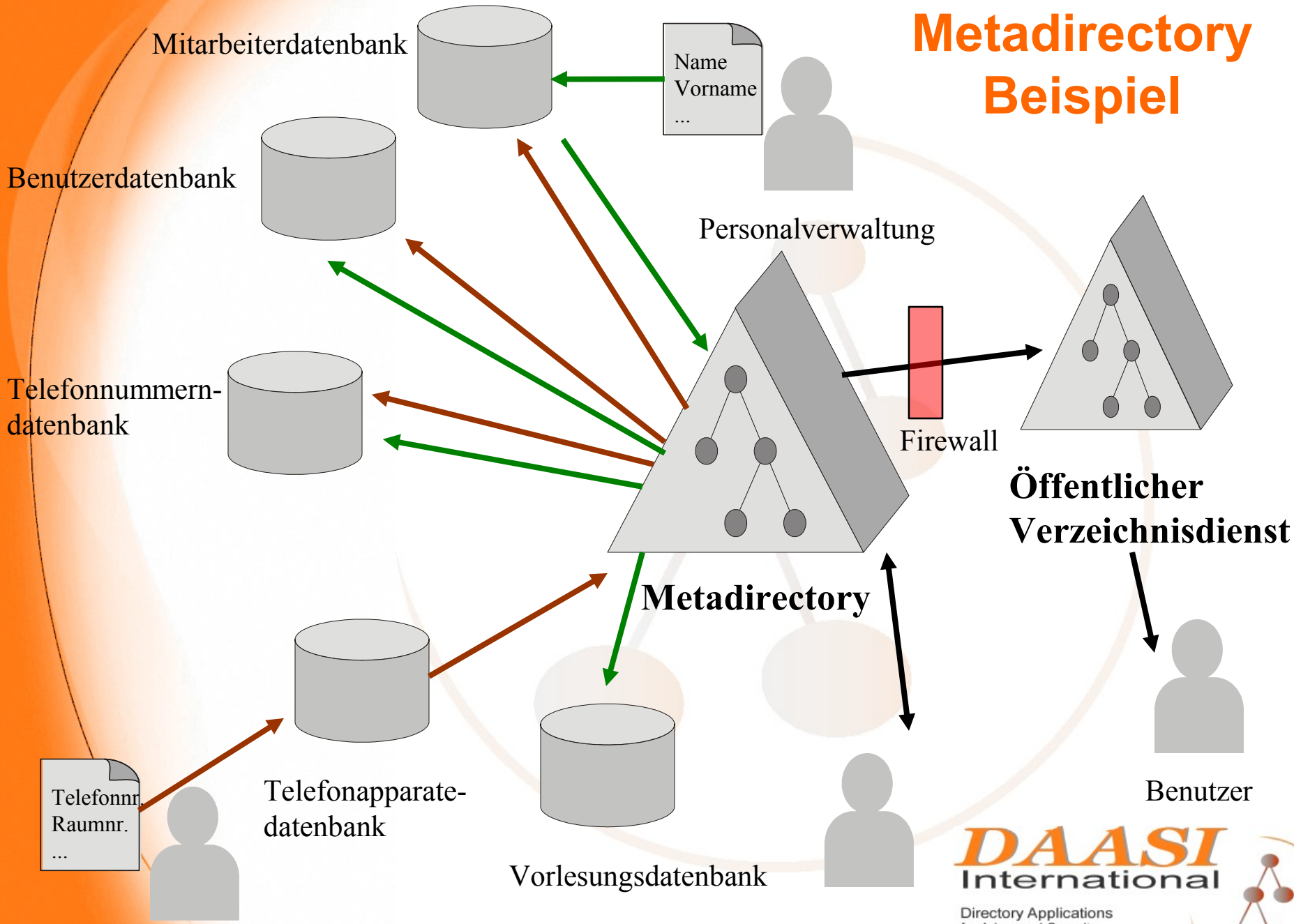
DAASI International
Directory Applications for Advanced Security and Information Management

Beispiel für zentrales Verzeichnis mit verschiedenen Anwendungen



DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory Beispiel



DAASI International
Directory Applications for Advanced Security and Information Management

Open Source vs. kommerzielle Produkte 1/2

- Da Identity Management ein neuer großer Markt ist, gibt es sehr viele kommerzielle Lösungen
  - IBM, Novell, SUN, Siemens, etc.
  - hohe Lizenzgebühren (oft pro Eintrag berechnet)
  - trotzdem kein Produkt von der Stange
    - jede IT-Landschaft ist anders
    - es gibt nicht für jede Datenbank fertige Konnektoren
    - es fallen also weitere Kosten für Support, Anpassung und Entwicklung an
  - Die Hauptprobleme sind organisatorischer Art und werden nicht durch Software gelöst

DAASI International
Directory Applications for Advanced Security and Information Management

Open Source vs. kommerzielle Produkte 2/2

- Open Source Produkte sind auch keine fertigen Lösungen
  - eingesparte Kosten bei Lizenz, nicht bei Support, Anpassung und Entwicklung
  - Kann sehr flexibel an die Gegebenheiten angepasst werden
  - bedient offene Standards, sodass verschiedene Komponenten zusammenpassen

DAASI International
Directory Applications for Advanced Security and Information Management

Vorteile durch Open Source

- Flexible Anpassung an die Anforderungen
- Keine Herstellerbindung
  - Sie können mit dem Code machen, was Sie wollen
- Beliebig weiterentwickelbar
  - z.B. Webservices
  - Automatisch aktuelles Mitarbeiterverzeichnis
  - Integration einer PKI
  - Integration in ein Identity Management System
  - Offen für weitere Anwendungen
- Keine Lizenzgebühren

DAASI International
Directory Applications for Advanced Security and Information Management

OpenLDAP

- Open Source Implementierung von LDAPv3
- Ausgangssource von verschiedenen kommerziellen Produkten
- Internationales Entwicklerteam
  - 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

OpenLDAP

- Voll LDAPv3 kompatibel
  - Einschließlich sicherer Verschlüsselung via TLS
- Stabil und performant
- Gute Zugriffskontrollmechanismen (ACLs und ACIs)
- Konfiguration entweder in Konfigurationsdatei oder in den Daten selber
- Stabile Replikationsmechanismen (slurpd und Syncrepl)
- Sehr flexibles Design
  - dynamische Module
  - Anpassungen durch Overlay-Interface
  - verschiedene Datenbackends

DAASI International
Directory Applications for Advanced Security and Information Management

Umfang der OpenLDAP-Distribution

- OpenLDAP Release enthält:
  - C-Bibliotheken für LDAP
  - Slapd LDAP-Server
    - mit eine ganzen Reihe von Daten-Backend-Modulen, die auch parallel eingesetzt werden können.
    - mit sog. Overlays kann das Verhalten des Servers ebenfalls modifiziert werden
  - Slurpd Replikationsdaemon
  - Client tools
    - Ldapsearch
    - Ldapmodify
    - Ldapdelete
    - Ldapmodrdn
    - ldappasswd

DAASI International
Directory Applications for Advanced Security and Information Management

Vorausgesetzte Software

- BerkeleyDB als Database Management System
- Cyrus-SASL als Authentifizierungs-System
- OpenSSL für sicheren und verschlüsselten Datentransport.
- Gegebenenfalls Kerberos zur Anwender-Authentifzierung.

DAASI International
Directory Applications for Advanced Security and Information Management

OpenLDAP

- Gleichzeitig mehrere unterschiedliche Datenbankends betreibbar, u.a.:
- LDAP-Backend
  - ermöglicht Einbindung z.B. eines Active Directory
- Meta-Backend
  - ermöglicht Metadirectoryfunktion (Konnektor als Backend)
- Perl-Backend
  - noch flexibler (man schreibt seine eigene Perl-Funktion für search, add, delete, etc.)
- SQL-Backend
  - zur Anbindung von RDBMs

DAASI International
Directory Applications for Advanced Security and Information Management

OpenLDAP

- Overlays für
  - referentielle Integrität
  - Password Policy
  - Attributmapping und DN-Konvertierung
  - proxycache
- Unterschiedliche Authentifizierungsmechanismen
  - Start_TLS
  - Digest-MD5
  - Kerberos
  - X.509-basierte Authentifizierung

DAASI International
Directory Applications for Advanced Security and Information Management

Open-Source-LDAP-Administrations-Tools

- Grafische Benutzerschnittstellen zur Datenverwaltung
  - GQ (gq-project.org)
  - JXPlorer (www.jxlorer.org)
  - Luma (luma.sourceforge.org)
  - Gosa (gosa.gonicus.de)
  - phpLDAPadmin (phpldapadmin.sourceforge.org)
  - Web2LDAP (www.web2ldap.org)
  - etc., etc. etc.

DAASI International
Directory Applications for Advanced Security and Information Management

Samba

- Ermöglicht Integration einer heterogenen Rechnerlandschaft
- Kann als Server für Windows-Clients eingesetzt werden
- Kann zur Synchronisierung von Passwörtern verwendet werden
- Kann OpenLDAP als Datenbackend verwenden
- www.samba.org

DAASI International
Directory Applications for Advanced Security and Information Management

Programmbibliotheken für LDAP

- Python-ldap (python-ldap.sourceforge.org)
- Perl-LDAP Net::LDAP (ldap.perl.org)
- Java: JLDAP (www.openldap.org/jldap)
- JDBC-LDAP Bridge Drive (www.openldap.org/jdbcldap)

DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit!

- Noch Fragen?

- Literaturtip: Gietz, Peter: Identity Management als zentraler Service, in: Open Source im Public Sector – Leitfaden für Entscheider und IT-Verantwortliche
  Zu beziehen bei bwcon baden-württemberg: connected
  www.bwcon.de (unter bwconn:boss)

- Wenn Sie später Fragen haben:
  - Peter Gietz, DAASI International GmbH
  - www.daasi.de
  - peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management