Einführung in LDAP und seine Anwendungsmöglichkeiten

Vortrag bei Science + Computing,
Tübingen, 24.7.2003

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

DAASI International
Directory Applications
for Advanced Security
and Information Management

Agenda

- Kurzvorstellung DAASI International
- Einführung in LDAP
  - Datenmodell
  - Funktionsmodell
- LDAP und zentrales Authentifizierungsystem
  - Samba und LDAP
- Übersicht über weitere Anwendungsmöglichkeiten
- Erfahrungen in der Praxis
- LDAP Performance-Tests

DAASI International
Directory Applications for Advanced Security and Information Management

DAASI International GmbH

- Seit 1994 Verzeichnisdienstbezogene DFN Projekte mit Förderung durch BMBF
- Wegen Aufbau und Betrieb von Diensten, die nicht durch Forschungsmittel Förderungsfähig sind musste neue Organisationsform gefunden werden
- Januar 2001 wurde deshalb die DAASI International GmbH gegründet
  - Directory Applications for Advanced Security and Information Management
  - Forschung ist wichtiger Bestandteil des Konzeptes
  - 7 feste und freie Mitarbeiter

DAASI International
Directory Applications for Advanced Security and Information Management

DAASI Dienstleistungen

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

DAASI International
Directory Applications for Advanced Security and Information Management

DAASI und Forschung

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

DAASI International
Directory Applications for Advanced Security and Information Management

Technologie-Unabhängigkeit

- Produktunabhängigkeit durch Unterstützung offener Standards
- Vorzüge von Open Source Software für den Kunden
  - Keine Kundenbindung
  - Bessere Sicherheit
  - Bessere Anpassbarkeit
- Aber wir haben auch Expertise in anderen Verzeichnisdiensttechnologien
  - X.500 Implementierungen (ISODE, Syntegra)
  - Andere LDAP Implementierungen (Sun, IBM, MaXware)
  - Novell Directory Services
  - Active Directory

DAASI International
Directory Applications for Advanced Security and Information Management

Kundenzielgruppen

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

DAASI International
Directory Applications for Advanced Security and Information Management

Beispiele für Universitätsprojekte

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

DAASI International
Directory Applications for Advanced Security and Information Management

DFN Directory Services

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

DAASI International
Directory Applications for Advanced Security and Information Management

Einführung in LDAP

DAASI International

Directory Applications
for Advanced Security
and Information Management

Was ist ein Verzeichnisdienst?

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

DAASI International
Directory Applications for Advanced Security and Information Management

Konzept von X.500/LDAP

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

DAASI International
Directory Applications for Advanced Security and Information Management

Was kann gespeichert werden?

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

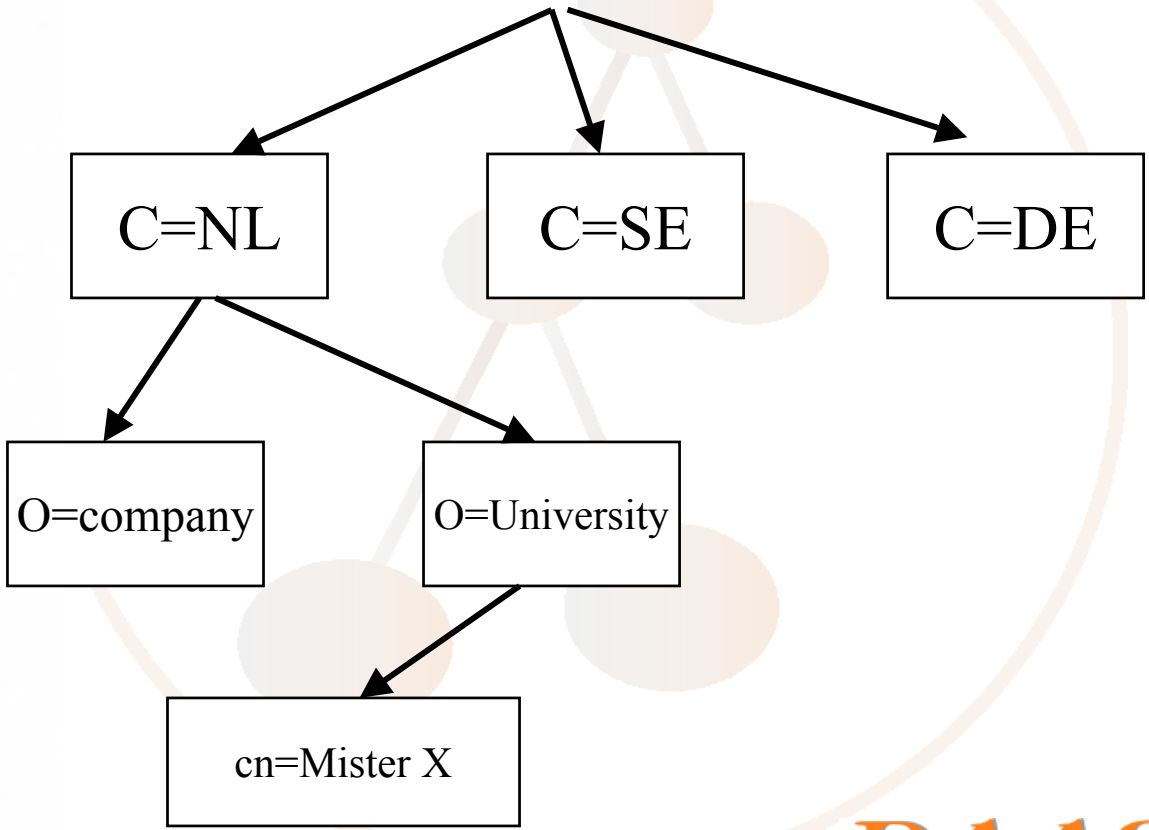
DAASI International
Directory Applications for Advanced Security and Information Management

Directory Information Tree (DIT)

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

DAASI International
Directory Applications for Advanced Security and Information Management

Directory Information Tree (DIT)



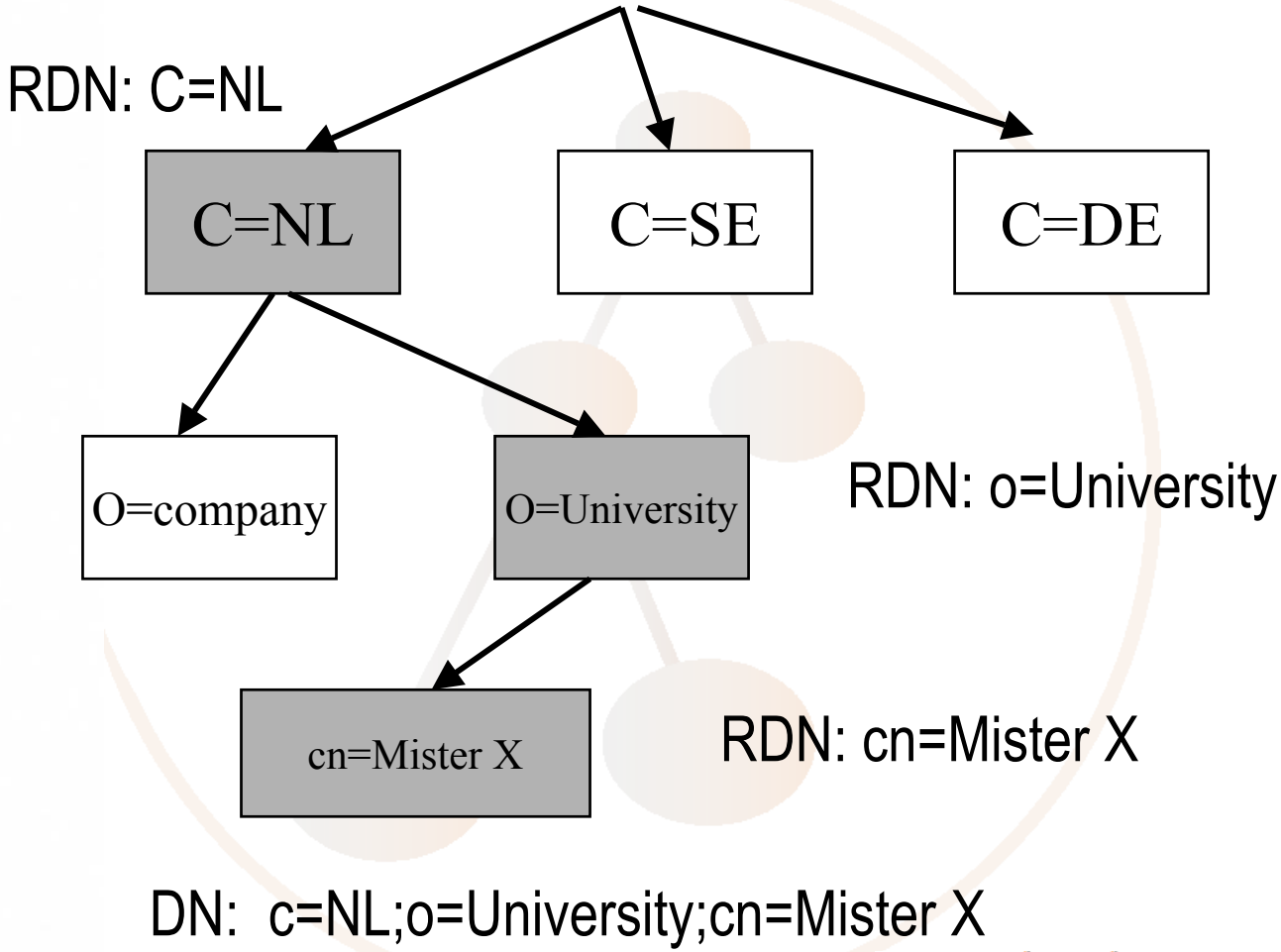
DAASI International
Directory Applications for Advanced Security and Information Management

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)

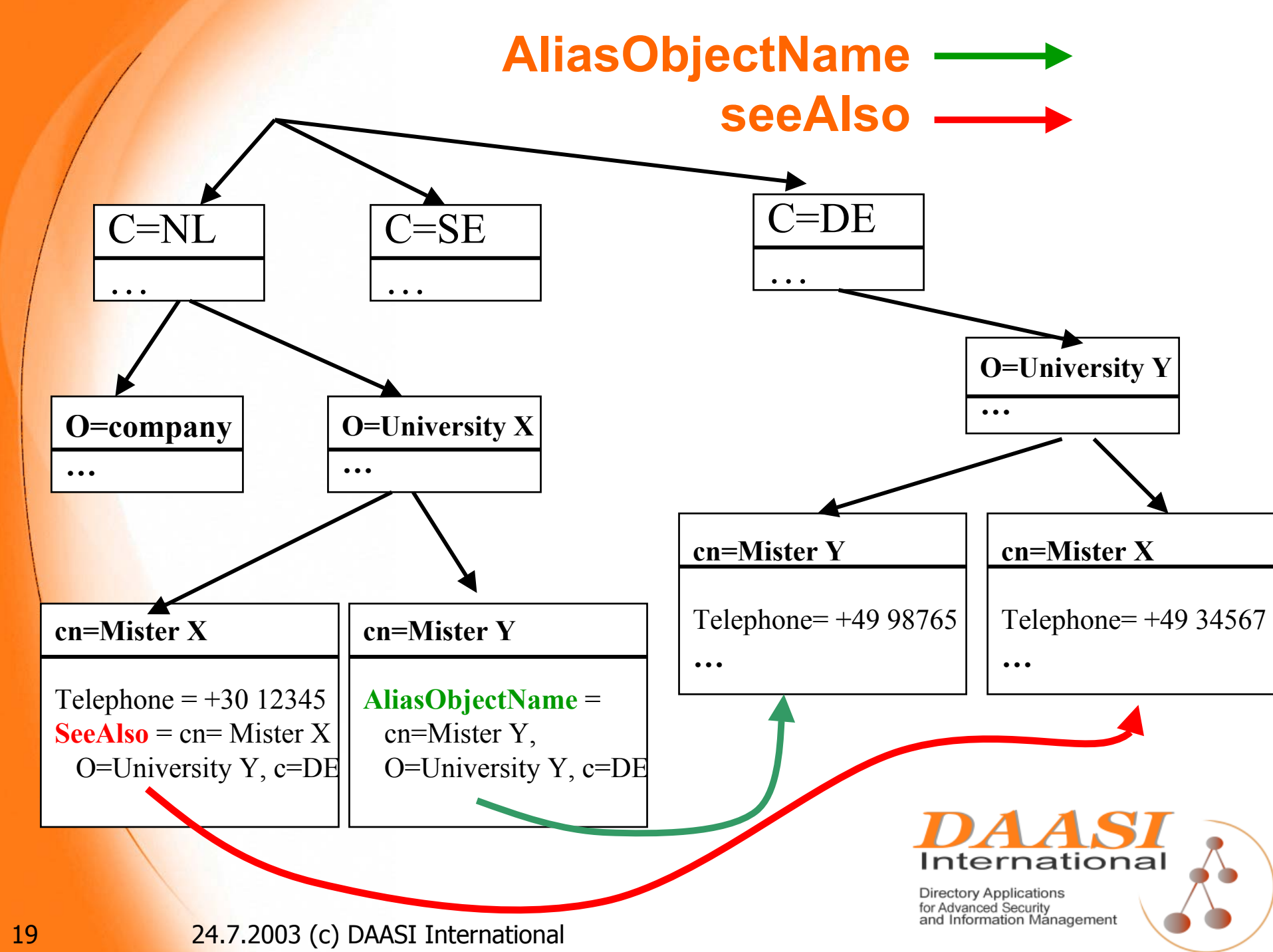


DAASI International
Directory Applications for Advanced Security and Information Management

DN Zeiger

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

DAASI International
Directory Applications for Advanced Security and Information Management



DAASI International

Directory Applications for Advanced Security and Information Management

LDAP Informationsmodell

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

DAASI International
Directory Applications for Advanced Security and Information Management

Spezielle Attribute

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

DAASI International
Directory Applications for Advanced Security and Information Management

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

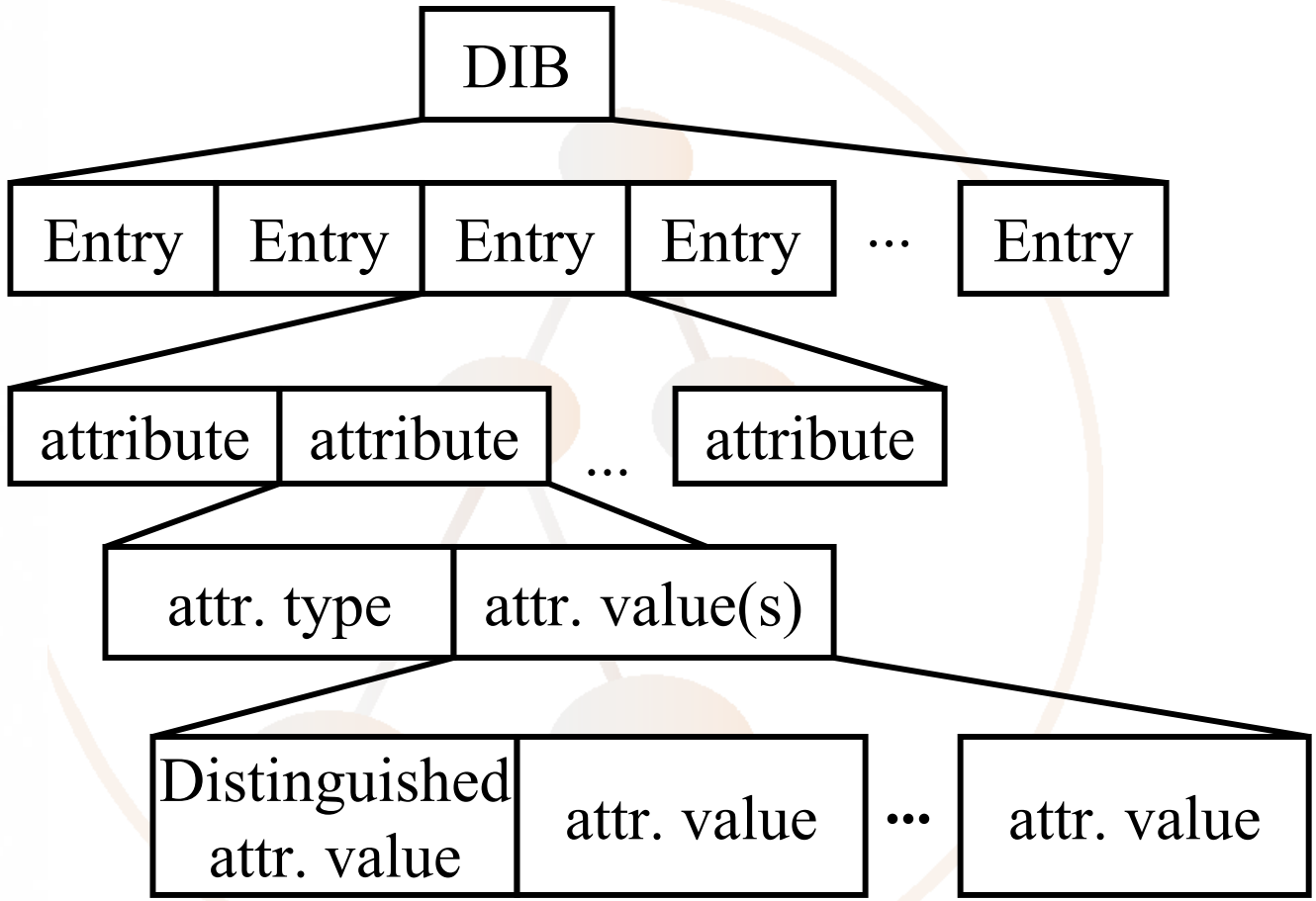
DAASI International
Directory Applications for Advanced Security and Information Management

Schema

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

DAASI International
Directory Applications for Advanced Security and Information Management

Directory Information Base



DAASI International
Directory Applications for Advanced Security and Information Management

Standardisierte Objektklassen

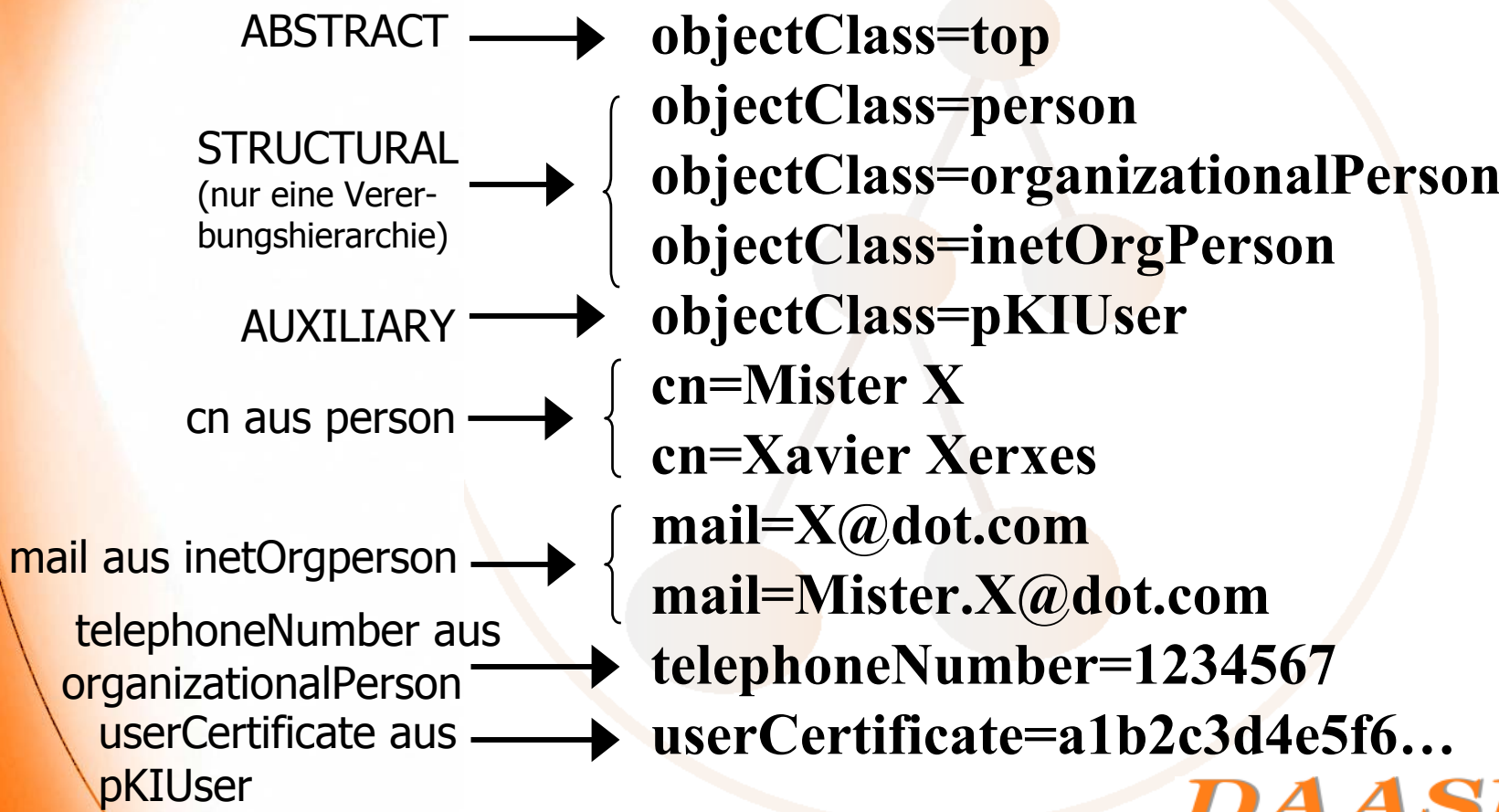
ObjectClass	distinguished Attr. and abbreviation	other Attributes
country	countryName or c	description, searchGuide, ...
locality	localityName or l	description, ...
organization	organizationName or o	description, postalAdress, ...
organizational Unit	organizationalUnit-Name or ou	description, postalAdress,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

DAASI International

Directory Applications for Advanced Security and Information Management

Beispiel

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



DAASI International
Directory Applications for Advanced Security and Information Management

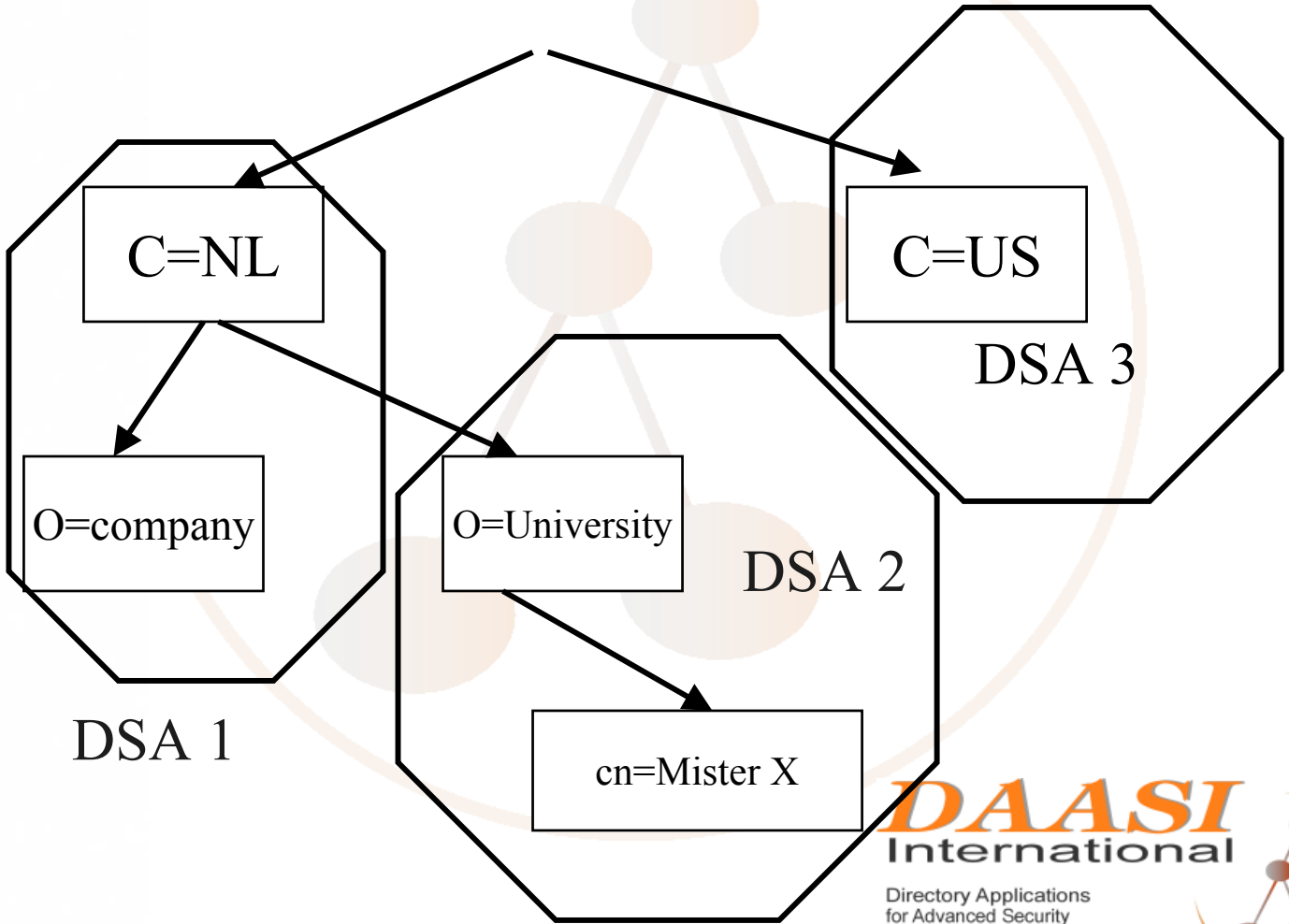
Offene Struktur

- 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:



DAASI International
Directory Applications for Advanced Security and Information Management

Funktionsmodell

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

DAASI International
Directory Applications for Advanced Security and Information Management

Authentifizierung

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

DAASI International
Directory Applications for Advanced Security and Information Management

LDIF (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, ...
```

DAASI International
Directory Applications for Advanced Security and Information Management

LDAPv3 Standard

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

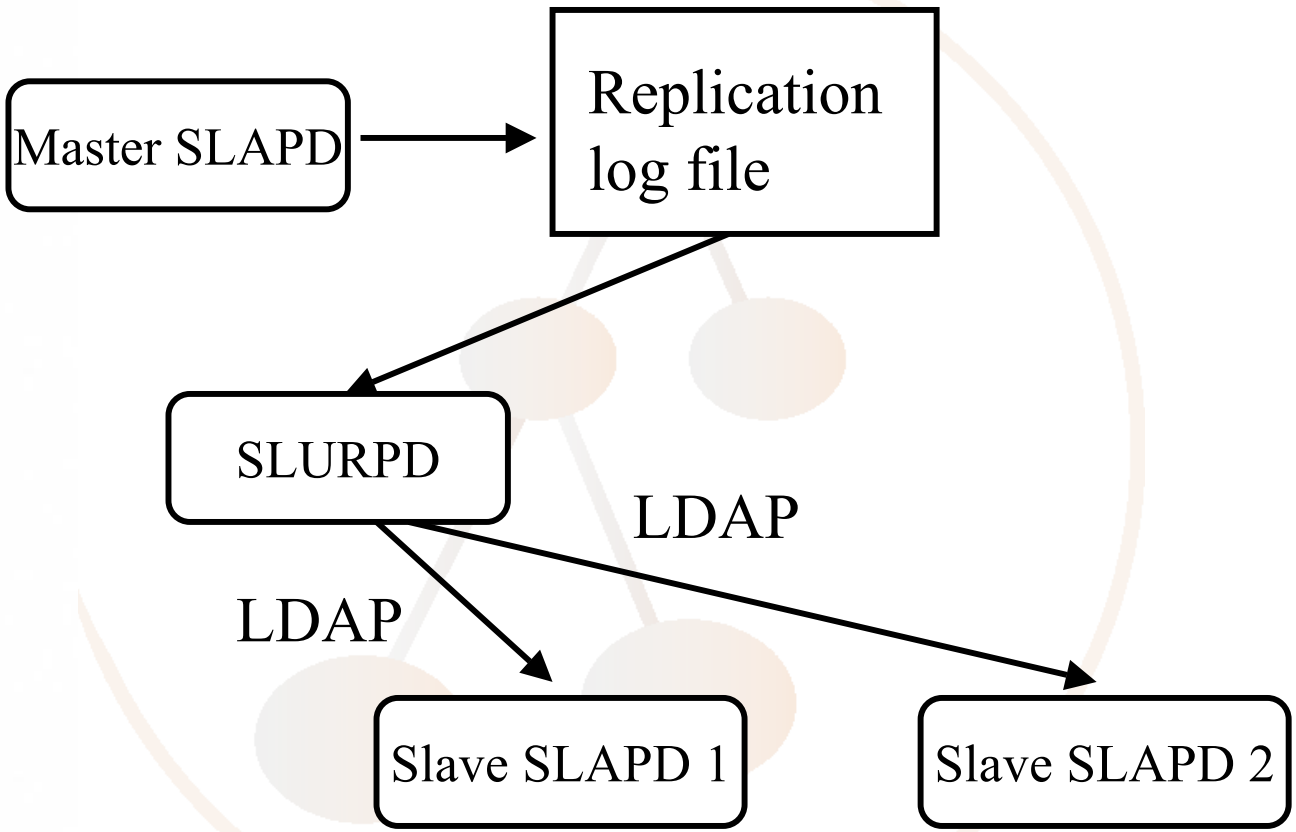
DAASI International
Directory Applications for Advanced Security and Information Management

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 berücksichtigt
  - IMAP, SMTP Auth, etc.
  - Apache Webserver

DAASI International
Directory Applications for Advanced Security and Information Management

Open LDAP

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

DAASI International
Directory Applications for Advanced Security and Information Management

Vorteile von OpenLDAP

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

DAASI International
Directory Applications for Advanced Security and Information Management

Zusammenfassung: Vorteile von LDAP

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

DAASI International
Directory Applications for Advanced Security and Information Management

Zentraler Authentifizierungsdienst mit LDAP und SAMBA

DAASI International

Directory Applications
for Advanced Security
and Information Management

Useful Technologies 1

- Kerberos
  - Network authentication protocol with strong authentication for client/server environments
  - Each participant shares a secret key with a central Key Distribution Center (KDC)
  - KDC consists of Authenticate Service and Ticket Granting Service
- GSSAPI (Generic Security Service Application Program Interface)
  - Security framework that abstracts from underlying protocols
  - Includes a Kerberos mechanism

DAASI International
Directory Applications for Advanced Security and Information Management

Useful Technologies 2

- X.509
  - Certificate based strong authentication via assymetric encryption
  - Certificate issued by a third trusted party (CA)
- Security Layers
  - Integrity and privacy protection via encryption
  - Secure Socket Layer (SSL) / Transport Layer Security (TLS)
    - X.509 Certificate based
  - Kerberos and SASL also can establish Security Layers
  - IPSec: X.509 certificate based security at the network layer

DAASI International
Directory Applications for Advanced Security and Information Management

Useful Technologies 3

- SASL (Simple Authentication and Security Layer)
  - Method for adding authentication support to connection-based protocols
  - Supported by LDAP Servers
  - Specified mechanisms:
    - PLAIN (plain text password, we don‘t want that!)
    - DIGEST-MD5 (challenge Response no clear text PW)
    - GSSAPI (and thus Kerberos)
    - EXTERNAL (e.g. X.509 certificate used in the underlying SSL / TLS)

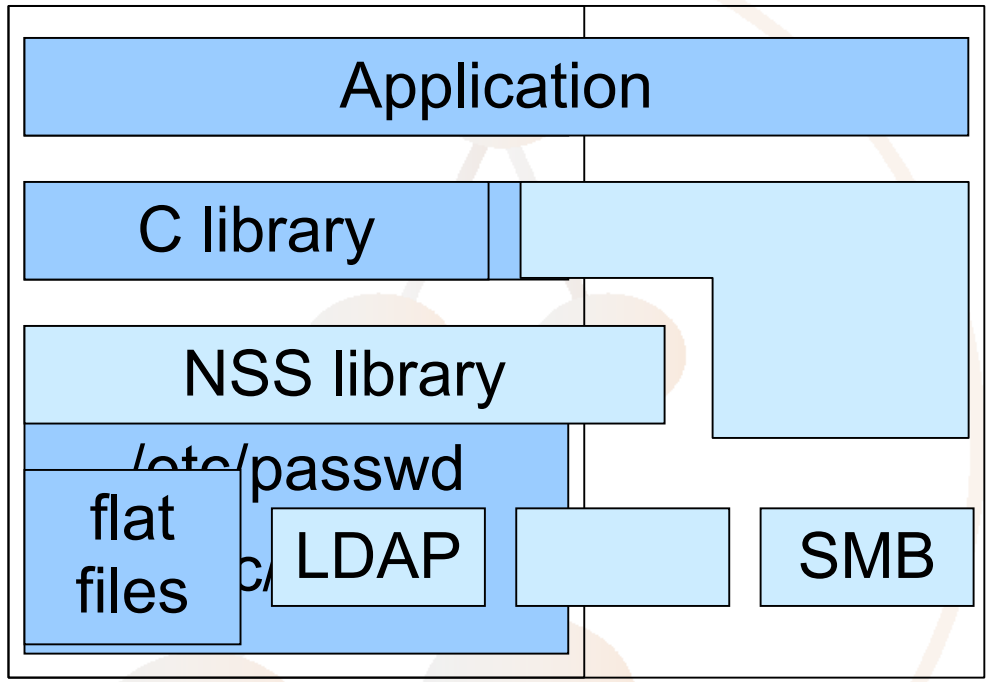
DAASI International
Directory Applications for Advanced Security and Information Management

Useful Technologies 4

- Name Service Switch (NSS)
  - Layer in Unix C libraries that provides different means for listing or searching users, groups, IP services, networks, etc.:
    - Flat files (etc/passwd, etc.) = hard to administrate
    - NIS (Network Information Service) = security holes
    - LDAP = ☺
- Pluggable Authentication Modules (PAM)
  - Framework for login services
  - Manages authentication, accounts, sessions and passwords
  - Modules exist for LDAP, Kerberos, etc.

DAASI International
Directory Applications for Advanced Security and Information Management

Unix authentifizierung



DAASI International
Directory Applications for Advanced Security and Information Management

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

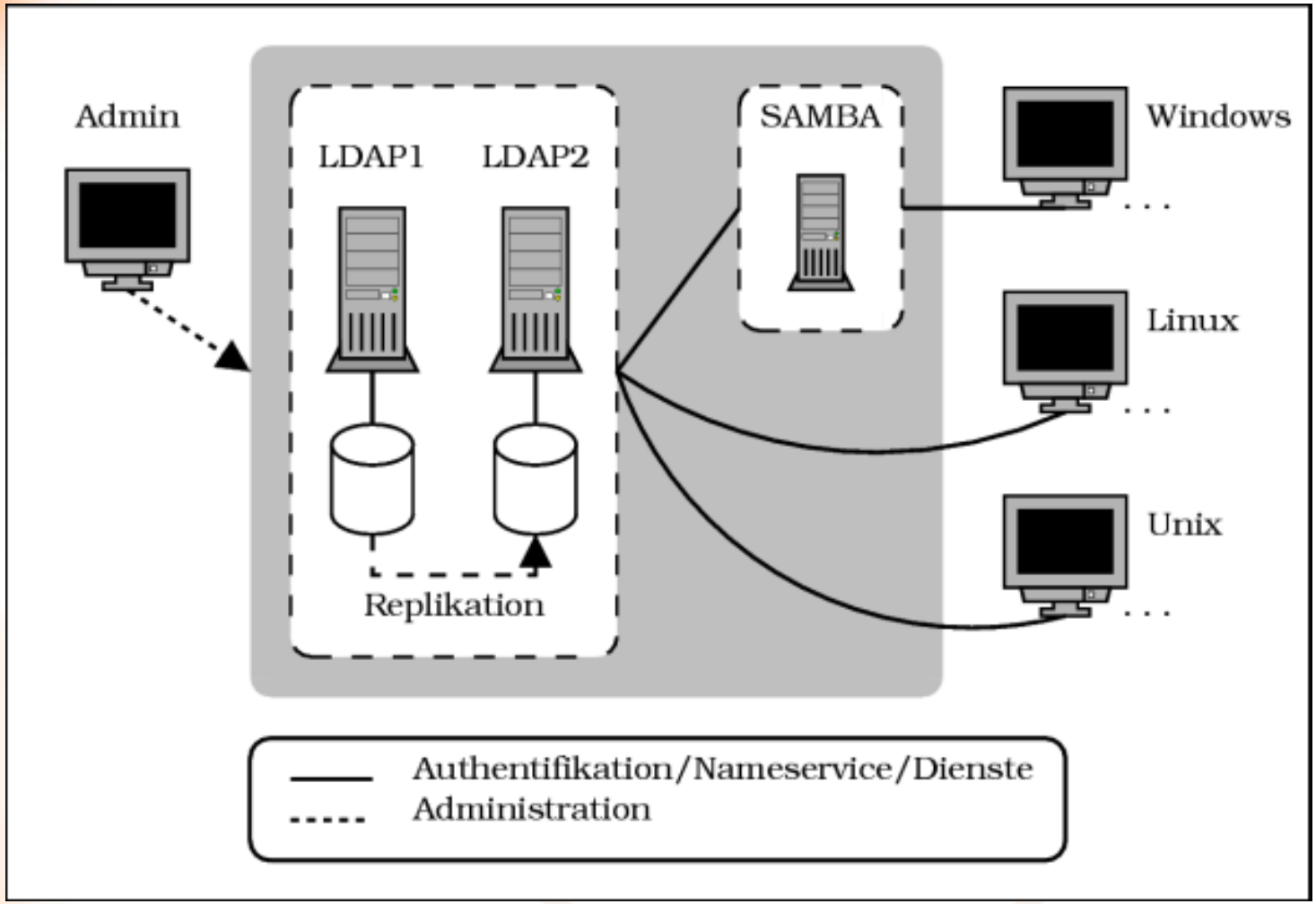
DAASI International
Directory Applications for Advanced Security and Information Management

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

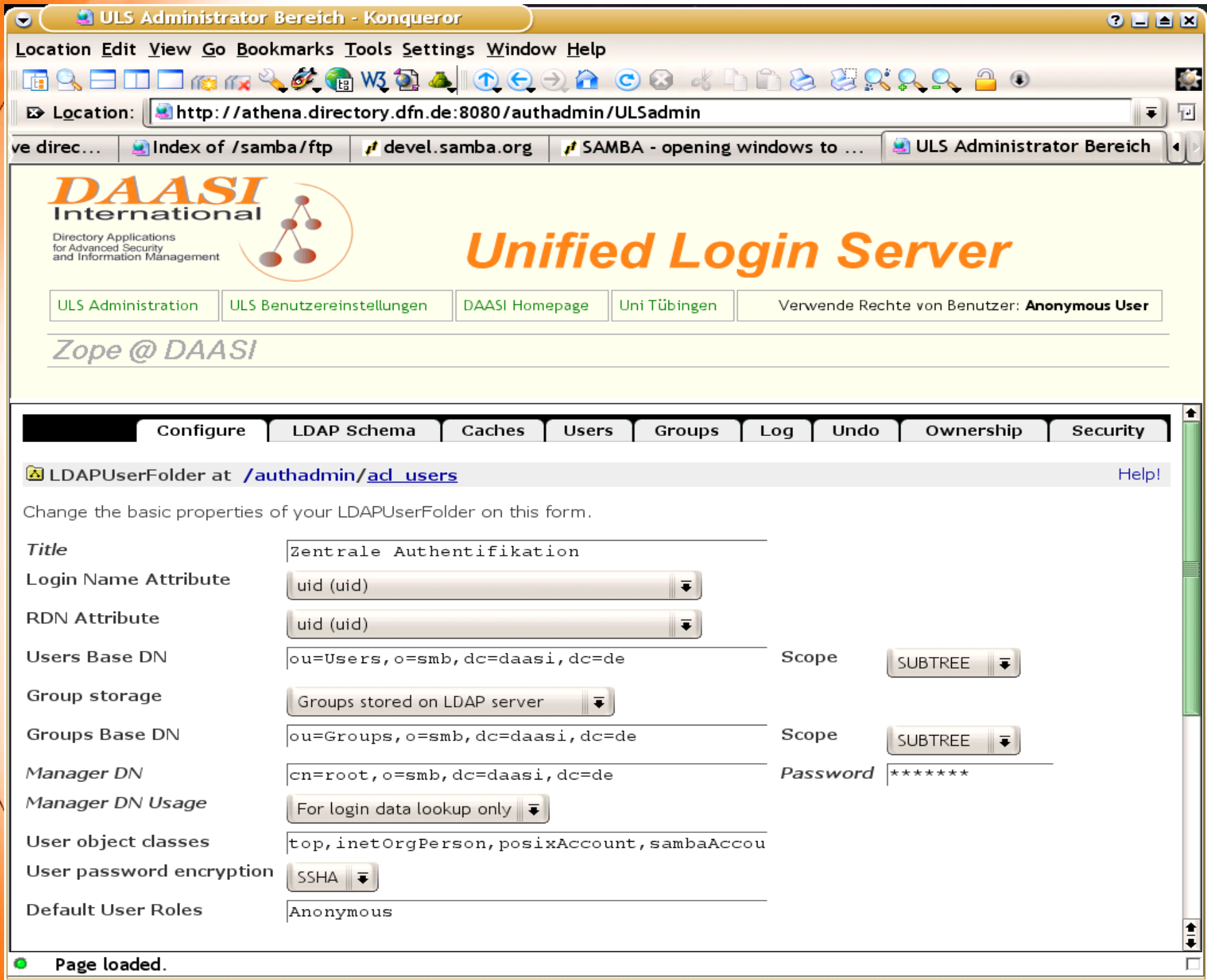
Problems

- 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

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


ULS Administrator Bereich - Konqueror
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
Page loaded.

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)

DAASI International
Directory Applications for Advanced Security and Information Management

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

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

Our view on Samba 3.0

- The "ldap passwd sync" feature main reason to switch to Samba 3.0.
  - Users can change their password using the standard windows password change dialog.
  - Samba cares for the necessary steps to update both, the passwords used by windows (LDAP attributes: ntPassword and lmPassword) an the userPassword attribute that is used by Unix clients.
  - Samba can delete a complete DN if the user is to be deleted from the Samba account database (= ldapsam) or only remove the attributes concerning windows.

DAASI International
Directory Applications for Advanced Security and Information Management

Samba 3.0 (contd.)

- The "ldap trust ids" feature
  - assumes that user ids returned from the LDAP database are always correct
  - So no need to lookup the corresponding Unix user.
  - This is very useful for our setup since we use nss_ldap and thus have valid UIDs in our database anyway.
- The upgrade process was clean and easy.
  - Having the account data in an LDAP directory does really help this process.
- Now the Code must prove its stability in our production environment, the beta3 is already quite stable
- Not yet experimented with:
  - PDC replication stuff to set up a multimaster environment with Samba.
  - Samba Active Directory emulation.
  - group mapping of Samba 3.0 (still incomplete ?)

DAASI International
Directory Applications for Advanced Security and Information Management

Weitere LDAP Anwendungsmöglichkeiten

DAASI International

Directory Applications
for Advanced Security
and Information Management

Kontaktdateninformationsdienste

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

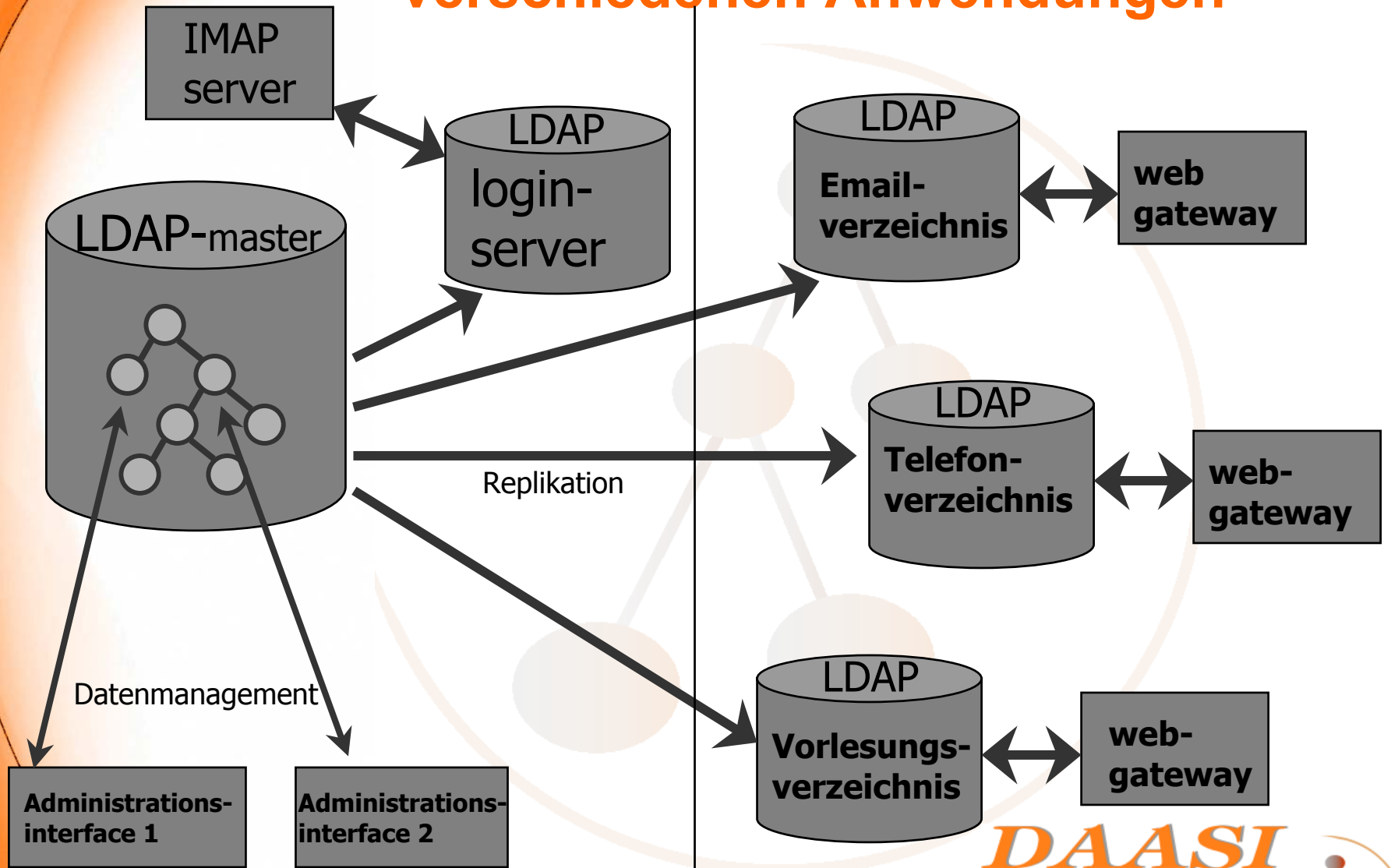
DAASI International
Directory Applications for Advanced Security and Information Management

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



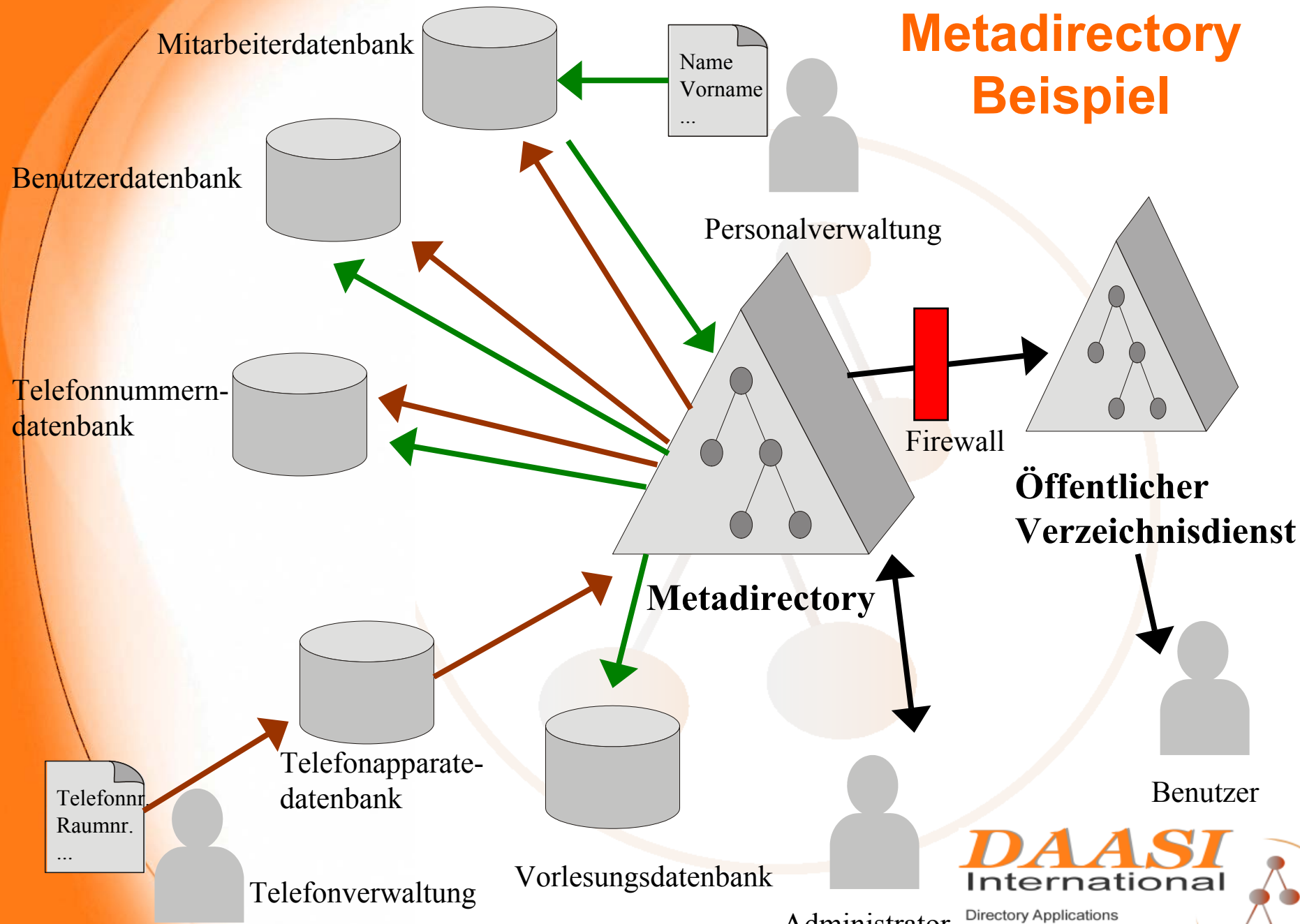
DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory

- 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 existierende Organisationsabläufe anpassbar

DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory Beispiel



DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory Implementierungen

- Verschiedene Implementierungen (alphabet. Ordnung)
  - IBM Tivoli Identity Manager
  - Microsoft Metadirectory Service
  - Novell DirXML
  - Siemens DirX Metahub
  - SUN One Directory Server Metadirectory Lösung
  - MaxWare Meta Center
- OpenLDAP kann Grundlage für eine OpenSource-Lösung sein

DAASI International
Directory Applications for Advanced Security and Information Management

Ressourcen-Verwaltung

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

- Auch diese Anwendungen lassen sich in ein zentralen Verzeichnisdienst integrieren

DAASI International
Directory Applications for Advanced Security and Information Management

Viele weitere Nutzungsmöglichkeiten

- Informationsdienst für asymmetrische Verschlüsselung
  - Zertifikatsserver für X.509 Zertifikate
  - PGP Keyserver
- Informationsserver im Bereich Digital Library
  - Metadaten
  - Ontologien
  - XML-Daten lassen sich gut in LDAP speichern
- Content Management System
- Verzeichnisdienstbasiertes Netzwerk-Policy-Repository
  - Regeln für Routen und zum Prioriesieren von IP-Packeten
  - Regeln und Informationen für Authentizitätsprüfungen
- ...

DAASI International
Directory Applications for Advanced Security and Information Management

Praktische Erfahrungen

DAASI International

Directory Applications
for Advanced Security
and Information Management

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
- Design der Client-Anwendungen

DAASI International
Directory Applications for Advanced Security and Information Management

OpenLDAP tweaks

- Entwicklung geht sehr schnell voran
  - Man sollte bei Update eines Produktionsdienst vorher neue Version gut testen!
  - Bald wird OpenLDAP 2.1.x historic, dennoch ist 2.1.20 im Augenblick die beste Wahl
  - 2.2. Ist im Alpha-stadium aber bereits zum Testen verfügbar
  - 2.3. Soll noch dieses Jahr rauskommen
- Welches Backend?
  - Bdb backend ist schnell und sehr stabil
    - Benötigt Sleepycat Berkeley DB 4.1
  - Hdb wird für writes sehr perfomant sein

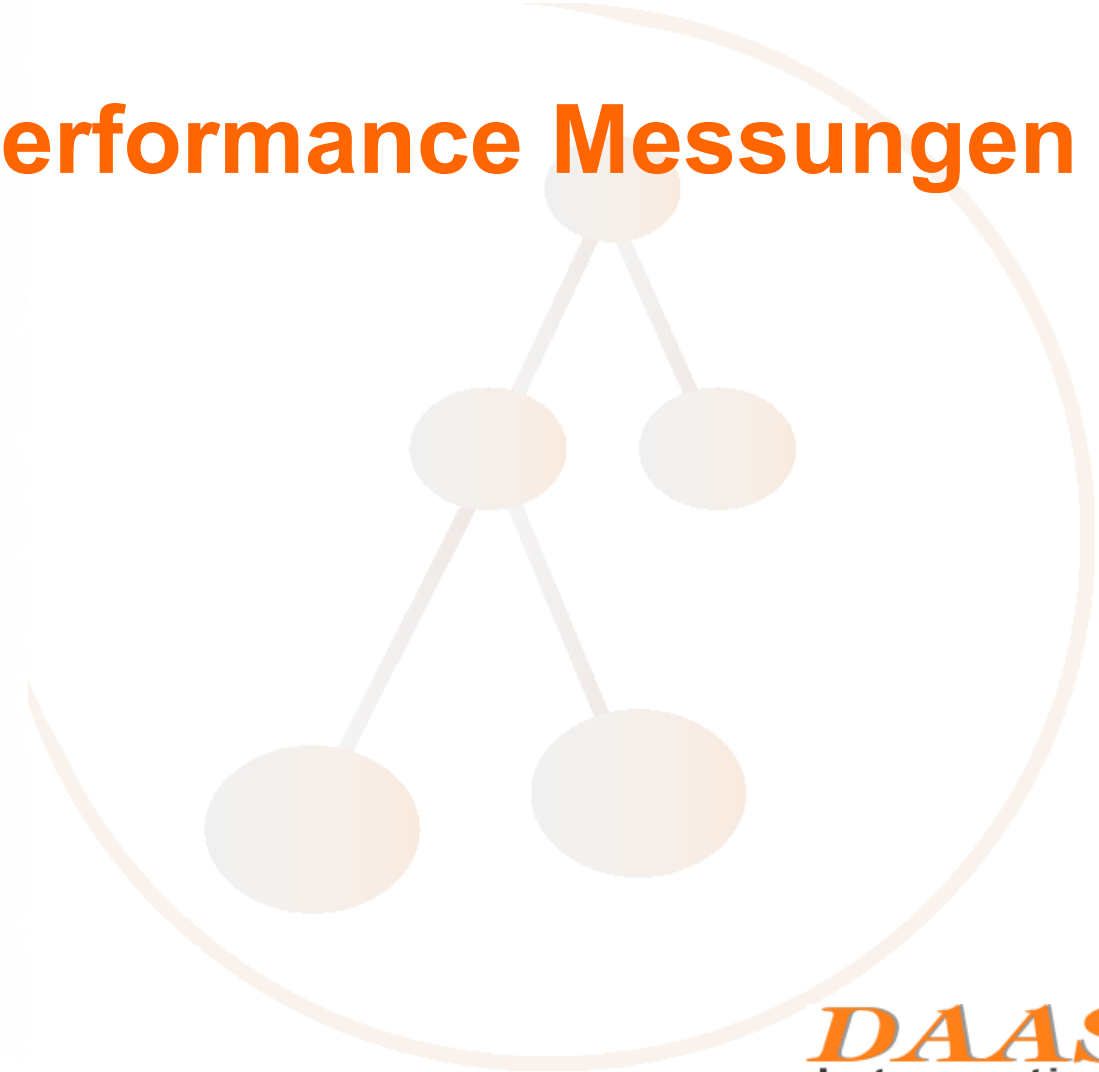
DAASI International
Directory Applications for Advanced Security and Information Management

Neues in OpenLDAP 2.2

- Functional enhancements and improved scalability:
  - "LDAP Sync"-based Lightweight Replication
  - NS-SLAPI Support
  - Proxy Cache Support
  - Hierarchical Backend
  - Backend Layering
  - LDAPv3 extensions:
    - ACID extensions (Transaktionen)
    - Cancel Operation
    - Content Synchronization Operation
    - DIT Content Rules
    - Duplicate Entry Extension
    - Simple Paged Results Extension
    - Proxy Authorization Extension

DAASI International
Directory Applications for Advanced Security and Information Management

Performance Messungen



DAASI International

Directory Applications
for Advanced Security
and Information Management

Diplomarbeit Klasen

- Getestet wurden:
  - Windows 2000 Active Directory
  - Novell eDirectory 8.5
  - Messaging Direct M-Vault R6.0v3p2 X.500(93) Implementierung. Heute: ISODE
  - Netscape Directory Server 4.13 (=iPlanet). Heute nur noch in SUN One Directory Server weiterentwickelt
  - IBM SecureWay Directory 3.2
  - OpenLDAP 2.0.7
- Plattform war: AMD Athlon 750, 256MB RAM, SuSE linux 7.0 / Windows 2000 Server SP1
- Testsuite: DirectoryMark 1.2
- 20.000 Datensätze

DAASI International
Directory Applications for Advanced Security and Information Management

Directory Server	Tool	Time [m:ss]
Active Directory	ldapmodify (1)	33:43
eDirectory	ice (2)	255:53
M-Vault	dbulk	1:02
Netscape Directory Server	ldif2db	2:23
OpenLDAP	slapadd (3)	4:22
SecureWay Directory	ldapmodify (4)	66:55

Figure 11.1: Bulk-load times for 20,000 accounts

Directory Server	Operations/s	Average Time (ms)	Max Time (ms)
Active Directory	637	1	24
eDirectory	204	4	76
M-Vault	89	38	2967
Netscape Directory Server	606	1	269
OpenLDAP	270	3	208
SecureWay Directory	48	20	148

Figure 11.2: Results for the messaging scenario

Directory Server	Operations/s	Average Time (ms)	Max Time (ms)
Active Directory	582	4	254
eDirectory	142	27	2826
M-Vault	99	9	151
Netscape Directory Server	356	8	2883
OpenLDAP	128	25	10203
SecureWay Directory	26	150	29695

Figure 11.3: Results for the address look-up scenario

Directory Server	Operations/s	Average Time (ms)	Max Time (ms)
Active Directory	123	2	136
eDirectory	20	90	449
M-Vault	45	32	372
Netscape Directory Server	162	5	258
OpenLDAP	151	4	497
SecureWay Directory	(20)[3]	(61)	(1107)

Figure 11.4: Results for the authentication scenario

DAASI International
Directory Applications for Advanced Security and Information Management

And the winner is ....

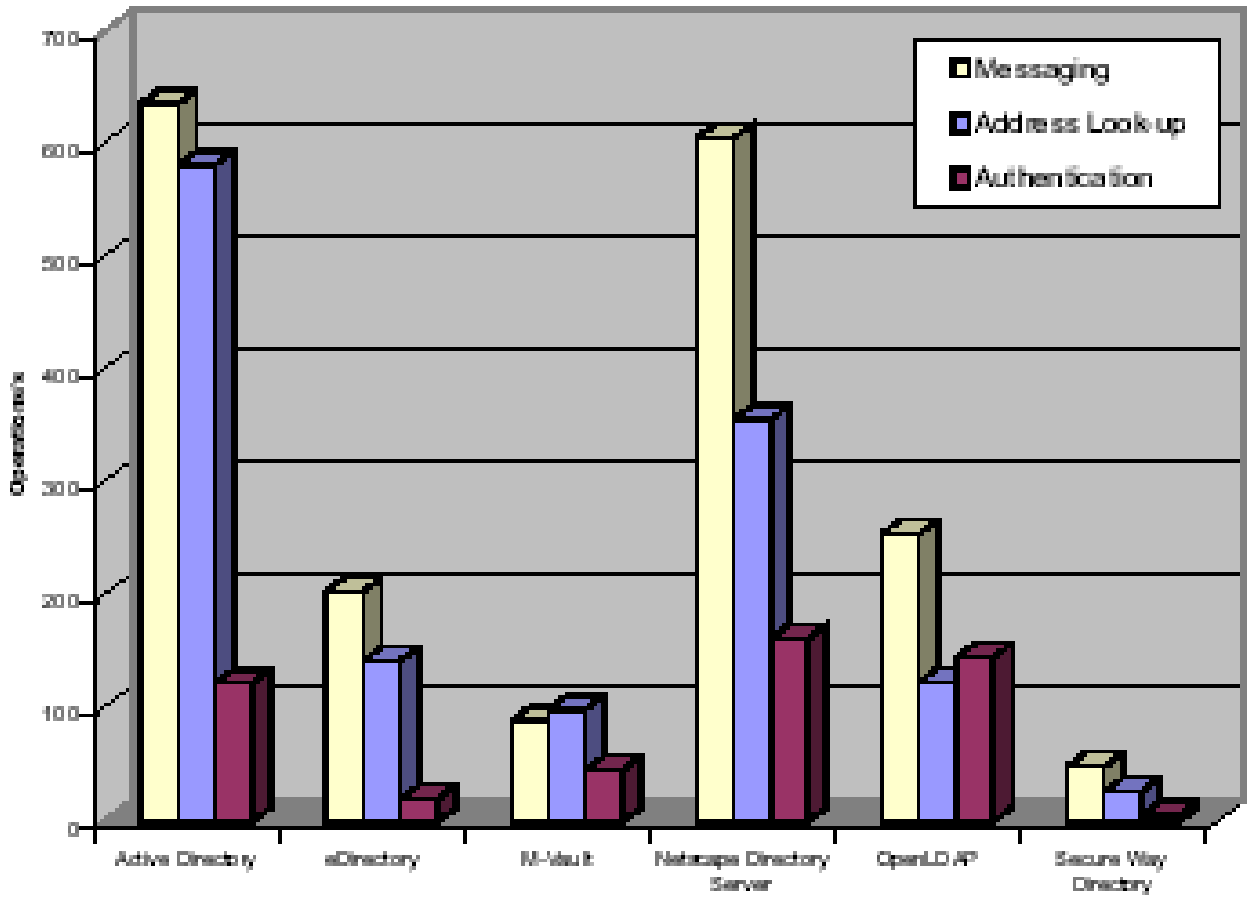


Figure 11.5: Results overview

DAASI International
Directory Applications for Advanced Security and Information Management

Performance Tests von Chadwick et.al.

- **Getestet wurden:**

Directory/Vendor	Operating System	Notes
Critical Path InJoin Directory Server 4.0	Windows 2000 Server	Loaned for evaluation from Critical Path @ http://www.cp.net
IBM SecureWay Directory 3.2.2	Windows 2000 Server	Free full product download available at http://www-3.ibm.com/software/network/directory/
iPlanet/SunONE Directory Server 5.1 (evaluation)*	Windows 2000 Server	Free trial download available at http://wwws.sun.com/software/products/directory_srvr/home_directory.html
Microsoft Active Directory	Windows 2000 Server	Integrated into Windows 2000 operating system.
Novell e-Directory 8.6	Windows 2000 Server	Free full product download available at http://www.novell.com
OpenLDAP 2.0.23	RedHat Linux 7.2	Free to full product download and source code available at http://www.openldap.org/
Syntegra Aphelion 2002	Windows 2000 Server	Loaned for evaluation from Syntegra @ http://www.syntegra.com

Table 1 – Directories Tested

DAASI International
Directory Applications for Advanced Security and Information Management

Performance Tests von Chadwick et.al.

- Plattform war Intel Pentium 3 - 1GHz, 512MB RAM Microsoft Windows 2000 Server/Red Hat Linux 7.1 Dual Partitioned Operating System
- Testsuite DirectoryMark 1.2.1
- Datensätze, jeweils 4 Tests mit:
  - 10,000
  - 100,000
  - 1,000,000
  - 10,000,000

DAASI International
Directory Applications for Advanced Security and Information Management

	10K	100K	1 million	10 million
Critical Path IDS 4.0	00:01:32	00:22:31	11:00:34	-
IBM SecureWay Directory 3.2.2	00:01:58	00:14:04	02:21:58	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	00:00:10	00:01:22	00:12:13	29:54:13
Microsoft Active Directory	00:05:03	00:61:54	22:36:06	-
Novell eDirectory 8.6	00:14:12	-	-	-
OpenLDAP 2.0.23	00:00:37	00:08:36	13:12:36	-
Syntegra Aphelion 2002	00:00:07	00:00:35	00:04:29	01:54:05

Table 3 – Indexed Directory Load Times (HH:MM:SS)

	10K	100K	1 million	10 million
Critical Path IDS 4.0	00:01:12	00:09:11	01:35:49	-
IBM SecureWay Directory 3.2.2	00:01:49	00:12:57	02:08:12	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	00:00:08	00:01:02	00:09:10	02:08:12
Microsoft Active Directory	00:04:55	00:54:44	21:01:33	-
OpenLDAP 2.0.23	00:00:14	00:01:15	02:01:11	-

Table 4 – Un-Indexed Directory Load Times (HH:MM:SS)

DAASI International

Directory Applications for Advanced Security and Information Management

	10K	100K	1 Million	10 Million
Critical Path InJoin Directory Server 4.0	1562.5	1562.5	1562.5	-
IBM SecureWay Directory 3.2.2	1666.7	1562.5	1666.7	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	2173.9	2272.7	2381.0	2272.7
Microsoft Active Directory	2000.0	2000.0	2000.0	-
Novell e-Directory	342.5	-	-	-
OpenLDAP 2.0.23	2272.7	1923.1	2173.9	-
Syntegra Aphelion 2002	2173.9	2000.0	2083.3	2272.7

Table 5 – Simulated Read (Base entry search on distinguished name) (operations/second)

DAASI International
Directory Applications for Advanced Security and Information Management

	10K	100K	1 Million	10Million
Critical Path InJoin Directory Server 4.0	1515.2	1515.2	1515.2	-
IBM SecureWay Directory 3.2.2	1724.1	1612.9	1724.1	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	2272.7	2173.9	2272.7	2272.7
Microsoft Active Directory	2272.7	2272.7	1562.5	-
OpenLDAP 2.0.23	2381.0	1923.1	2381.0	-
Syntegra Aphelion 2002	2381.0	2173.9	2272.7	2381.0

Table 6 – Full subtree exact match search on common name (operations/second)

	10K	100K	1 Million	10Million
Critical Path InJoin Directory Server 4.0	1470.6	1470.6	1470.6	-
IBM SecureWay Directory 3.2.2	595.2	581.4	588.2	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	2381.0	2272.7	2381.0	2500.0
Microsoft Active Directory	2272.7	2272.7	1666.7	-
OpenLDAP 2.0.23	2500.0	1923.1	2500.0	-
Syntegra Aphelion 2002	2381.0	2173.9	2272.7	2381.0

Table 7 – Full subtree substring search on common name (operations/second)

	10K	100K	1 Million	10 Million
Critical Path InJoin Directory Server 4.0	83.3	6.8	3.8	-
IBM SecureWay Directory 3.2.2	20.0	16.7	11.5	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	28.6	16.1	15.9	11.6
Microsoft Active Directory	31.3	32.3	10.4	-
OpenLDAP 2.0.23	6.7	5.3	2.1	-
Syntegra Aphelion 2002	8.4	8.5	7.0	2.8

Table 9 – Add organizationalPerson Entry to Indexed Directory (operations/second)

	10K	100K	1 Million	10 Million
Critical Path InJoin Directory Server 4.0	200.0	200.0	31.3	-
IBM SecureWay Directory 3.2.2	21.3	19.6	15.6	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	40.0	43.5	30.3	18.5
Microsoft Active Directory	34.5	17.5	10.9	-
OpenLDAP 2.0.23	12.2	13.7	13.7	-

Table 10 – Add organizationalPerson Entry to Un-Indexed Directory (operations/second)

	10K	100K	1 Million	10 Million
Critical Path InJoin Directory Server 4.0	188.7	333.3	59.9	-
IBM SecureWay Directory 3.2.2	40.3	34.0	23.0	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	40.0	37.3	30.2	13.0
Microsoft Active Directory	96.2	98	32.8	-
OpenLDAP 2.0.23	3.3	2.4	1.3	-
Syntegra Aphelion 2002	12.5	12.2	9.4	2.7

Table 13 – Modify indexed attribute cn (operations/second)

	10K	100K	1 Million	10 Million
Critical Path InJoin Directory Server 4.0	312.5	277.8	45.2	-
IBM SecureWay Directory 3.2.2	78.1	70.4	48.1	-
iPlanet/SunONE Directory Server 5.1 (evaluation)	50.8	51.8	36.5	21.0
Microsoft Active Directory	99	95.2	48.1	-
OpenLDAP 2.0.23	5.8	4.2	1.6	-
Syntegra Aphelion 2002	26.5	27.5	23.1	37.5

Table 14 – Modify un-indexed attribute telephoneNumber (operations/second)

And the winner is ...

- **Bei der Evaluation wurden entschieden:**
  - Critical Path IDS best choice for repositories up to 100K entries
  - SunONE best choice for repositories of over a 1 million entries.
- Die Leseperformance von OpenLDAP wurde hervorgehoben
- Bei Verwendung des HDB-Backends wäre die Schreibperformance ähnlich stark gewesen

DAASI International
Directory Applications for Advanced Security and Information Management

Zusammenfassung

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

DAASI International
Directory Applications for Advanced Security and Information Management

Verweise

- RFC 1510, „The Kerberos Network Authentication Service (V5)“
- RFC 1964, „The Kerberos Version 5 GSS-API Mechanism“
- RFC 2222, „Simple Authentication and Security Layer (SASL)“
- RFC 2246, „The TLS Protocol Version 1.0“
- RFC 2307, „An Approach for Using LDAP as a Network Information Service“
- RFC 2743, „Generic Security Service Application Program Interface Version 2, Update 1“
- RFC 2829, „Authentication Methods for LDAP“
- RFC 2830: „Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security“
- RFC 2831, „Using Digest Authentication as a SASL Mechanism“
- RFC 2849, „The LDAP Data Interchange Format (LDIF) – Technical Specification“
- RFC 3377, „Lightweight Directory Access Protocol (v3) Technical Specification“

DAASI International
Directory Applications for Advanced Security and Information Management

Weitere Verweise

- Samba: www.samba.org
  - IDEALX tools: www.idealx.org/prj/samba/index.en.html
- LDAP:
  - New drafts: www.ietf.org/html.charters/ldapbis-charter.html
  - OpenLDAP: www.openldap.org
  - NSS_LDAP: www.padl.com/OSS/nss_ldap.html
  - PAM_LDAP: www.padl.com/OSS/pam_ldap.html
  - Reentry patch from Rein Tollevik: www.openldap.org/lists/openldap-software/200108/msg00594.html
  - DirectoryMark Testsuite: www.mindcraft.com/directorymark
- X.509:
  - www.ietf.org/html.charters/pkix-charter.html
- Cyrus project (SASL, IMAP): asg.web.cmu.edu/cyrus/
- Zope: www.zope.org
- Tutos: www.tutos.org

DAASI International
Directory Applications for Advanced Security and Information Management

TERENA/DAASI Projekt Directory Schema Registry

- TERENA: Europäische Vereinigung der Nationalen Forschungsnetze (DFN, SurfNet, etc.)
- Projektziel: Informationssystem zum Auffinden bzw. Registrieren von definiertem Schema
- Policy für Datenaufnahme
  - Bedingung: gute Dokumentation und Metadaten
- OpenLDAP basierte Datenbank
- WWW.Schemareg.org

DAASI International
Directory Applications for Advanced Security and Information Management

Verweise zu Performance Tests

- Diplomarbeit, die von DAASI Betreut wurde:

Norbert Klasen: „Directory Services for Linux in comparison with Novell NDS and Microsoft Active Directory“, http://www.daasi.de/staff/norbert/thesis/

- Performance Tests von Chadwick, et.al:

Thornton, Mundy, Chadwick: „A Comparative Performance Analysis of 7 Lightweight Directory Access Protocol Directories“ http://www.terena.nl/conferences/tnc2003/programme/papers/p1d1.pdf

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