LDAP und Security -
Identity Management, Authentifizierung, Autorisierung und Verschlüsselung

ZDV-Seminar Security,
Tübingen, 15.6.2005

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management

Agenda

- Einführung in Identity Managemnent
- Einführung in LDAP
- Das LDAP-Protokoll
- Authentifizierung
- Sicherheitsbedrohungen
- PKI und LDAP (werden wir heute nicht schaffen)

DAASI International
Directory Applications
for Advanced Security
and Information Management

Einführung in Identity Management

DAASI International

Directory Applications
for Advanced Security
and Information Management

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

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
- Außenstehende wollen Kontaktinformationen

DAASI International
Directory Applications for Advanced Security and Information Management

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

DAASI International
Directory Applications for Advanced Security and Information Management

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

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.

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 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

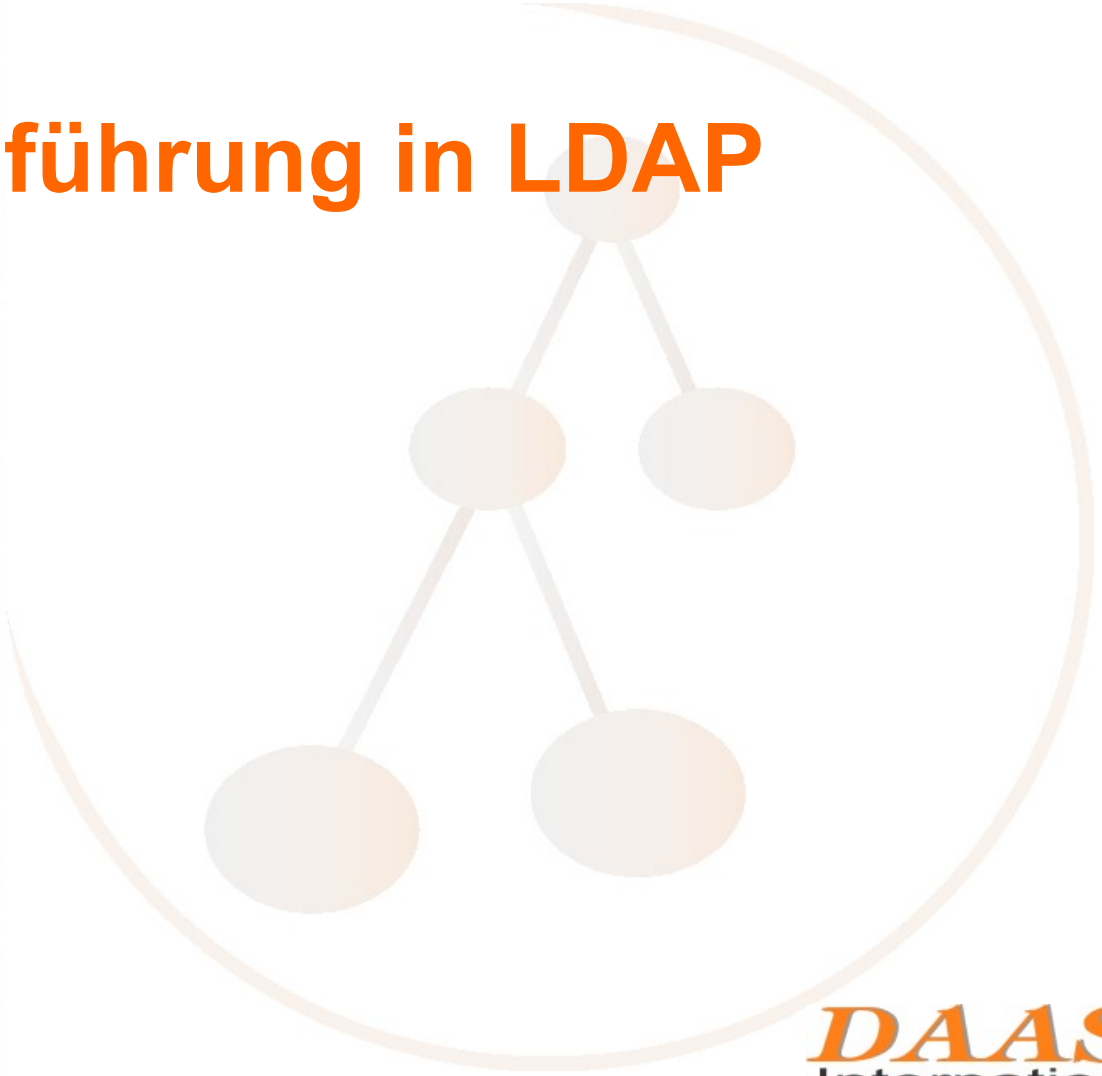
DAASI International
Directory Applications for Advanced Security and Information Management

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

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

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

Vergleich RDBMS vs. LDAP 1/2

Aspekt	RDBMS	LDAP
Schema	Es gibt keine standardisierten Tabellenschemata.	Es gibt insbesondere zur Abbildung von Organisations- und Personendaten, inklusive Gruppen und Rollenkonzepte international standardisierte Datenschemata.
Organisation	Entitätsinformationen werden logisch auf verschiedene Tabellen aufgeteilt.	Entitätsinformationen bleiben logisch an einem Platz, nämlich in einem Informationsobjekt, welches einen Knoten in einem hierarchischen Baum darstellt
Mehrfachwerte	Mehrfachwerte erzwingen eine neue Tabelle (Normalisierung) oder verschiedene Datenfelder wie z.B. Telefonnummer_1, Telefonnummer_2.	Beliebig viele Mehrfachwerte lassen sich problemlos speichern.
Datentypen	Begrenzte Anzahl von Datentypen wie String, Integer, Float, und Datum.	Theoretisch unbegrenzte Anzahl von Datentypen (hier Syntax genannt), de facto eine Vielzahl von Datentypen, insbesondere für Personendaten, z.B. eigene Syntax für Telefonnummern.

DAASI International
Directory Applications for Advanced Security and Information Management

Vergleich RDBMS vs. LDAP 2/2

Aspekt	RDBMS	LDAP
Vergleichs-regeln	Vergleichsregeln sind nicht Teil des Datenmodells, sondern müssen in den jeweiligen Abfrageprogrammen implementiert werden.	Vergleichsregeln sind Teil des Datenmodells. Man kann also z.B. bei der Schemadefinition bestimmen, ob bei Wertvergleichen Groß- und Kleinschreibung berücksichtigt werden soll oder nicht. Es gibt unterschiedliche Vergleichs-regeln für Gesamt- und Teilvergleiche.
Flexibilität	Änderungen des Datenschemas, also der Tabellenstruktur sind nur schwer möglich. Änderungen betreffen die gesamte Datenbank	Änderungen des Datenschemas einfach möglich: man fügt einem Informationsobjekt eine neue Objektklasse hinzu und kann dann entsprechende neue Attribute speichern. Änderungen betreffen jeweils nur die gewünschten Informationsobjekte.
Netzwerk-zugriff	Netzzugriff ursprünglich nicht vorgesehen. Wird meistens über ein Gateway realisiert.	Netzprotokoll ist Hauptteil des LDAP-Standards. eine Verteilung der Daten im Netz ist einfach möglich.
Authentifi-zierung	Meist nur ein proprietärer Authentifizierungsmechanismus.	Verschiedene standardisierte und über das Netz funktionierende Authentifizierungsmechanismen

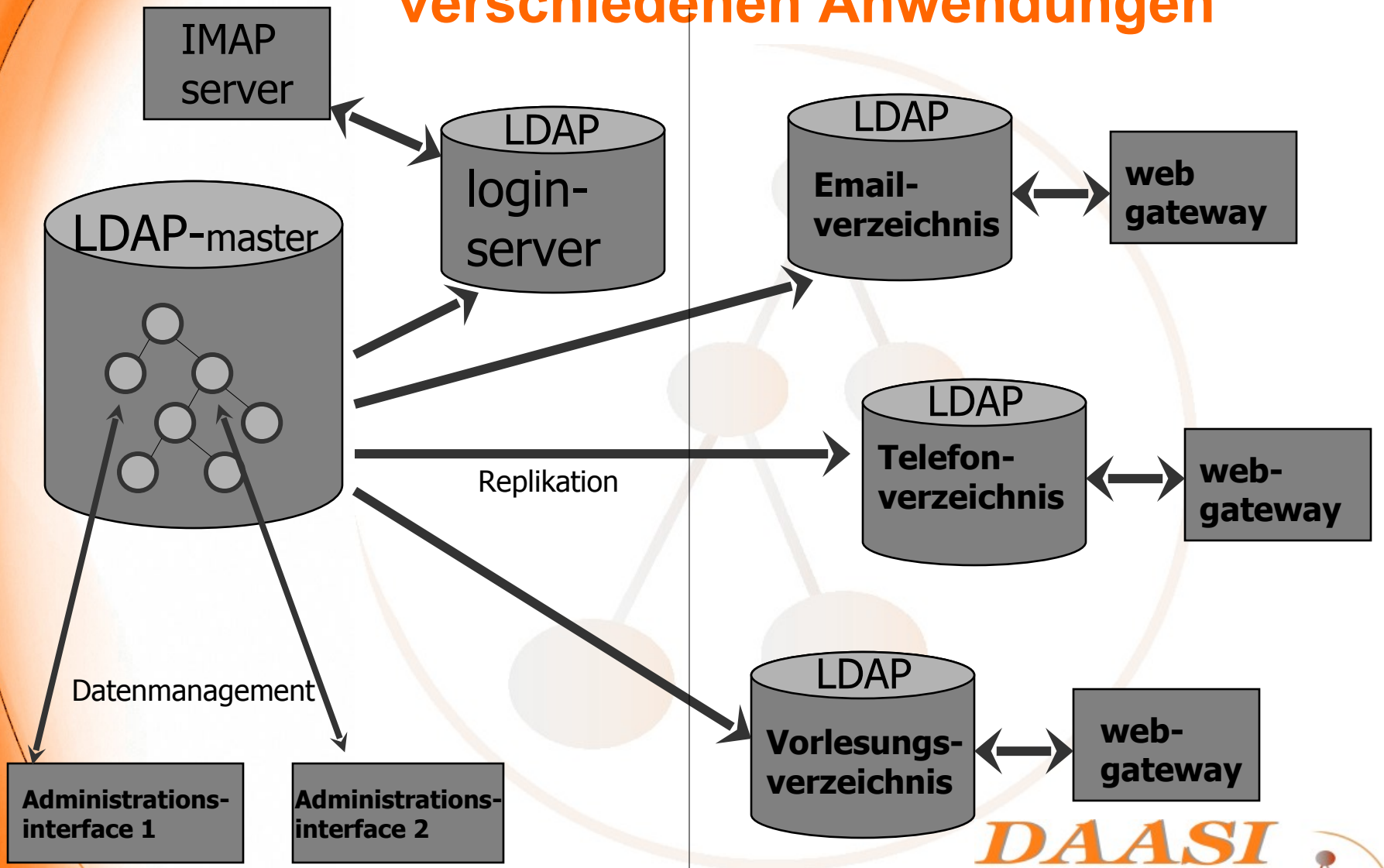
DAASI International
Directory Applications for Advanced Security and Information Management

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



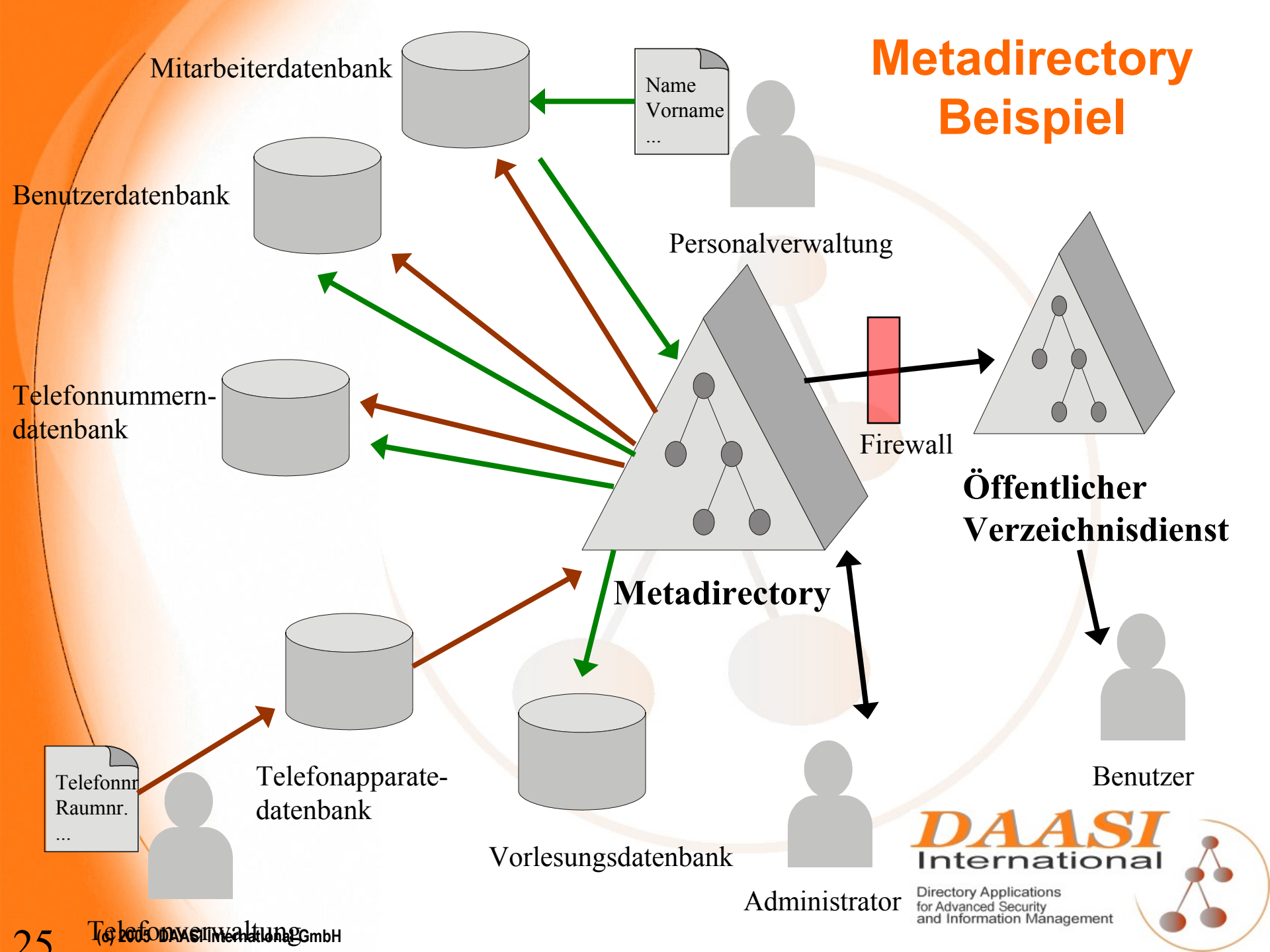
DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory – 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

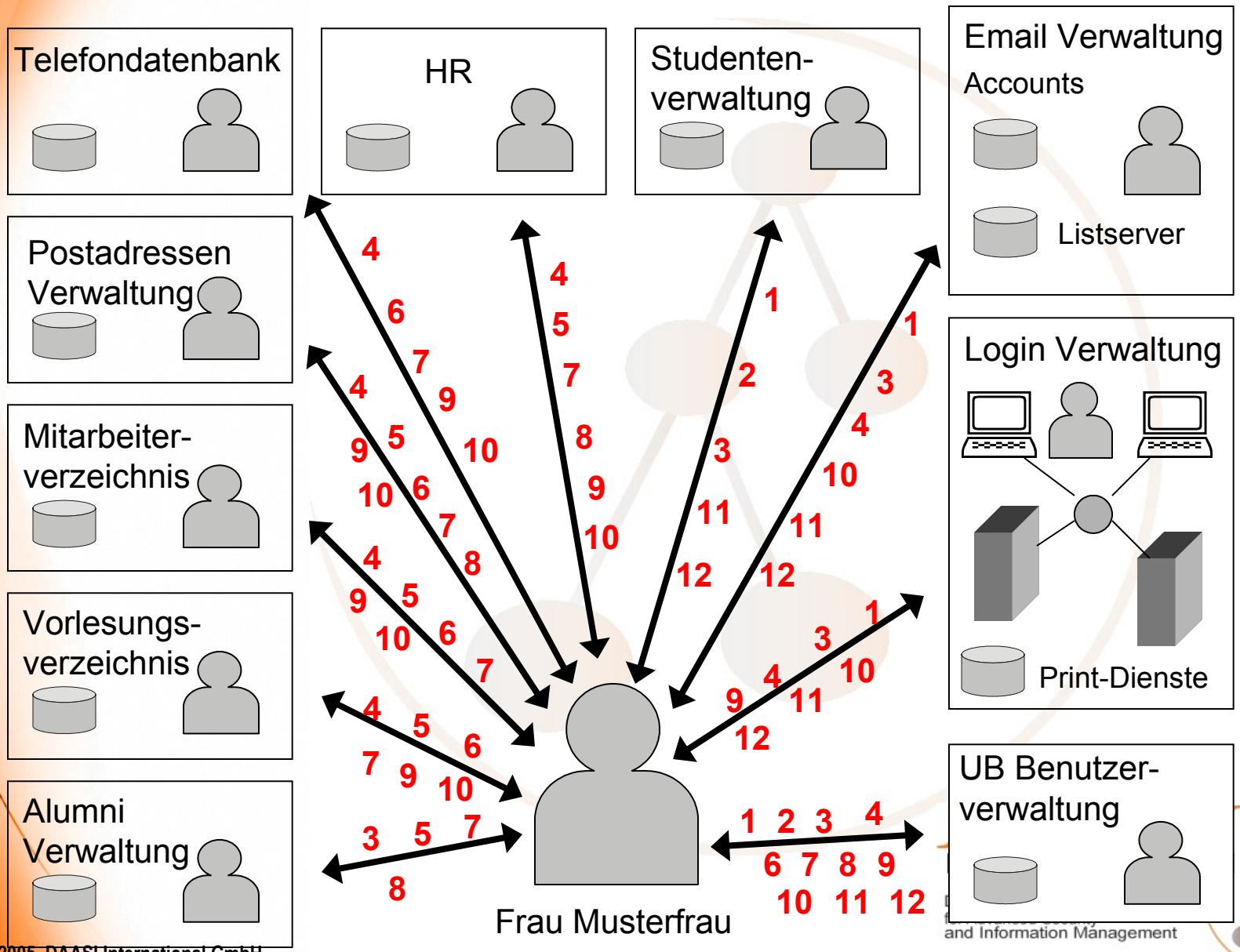
DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory Beispiel



DAASI International
Directory Applications for Advanced Security and Information Management

Worst Case Scenario: Interaktionen

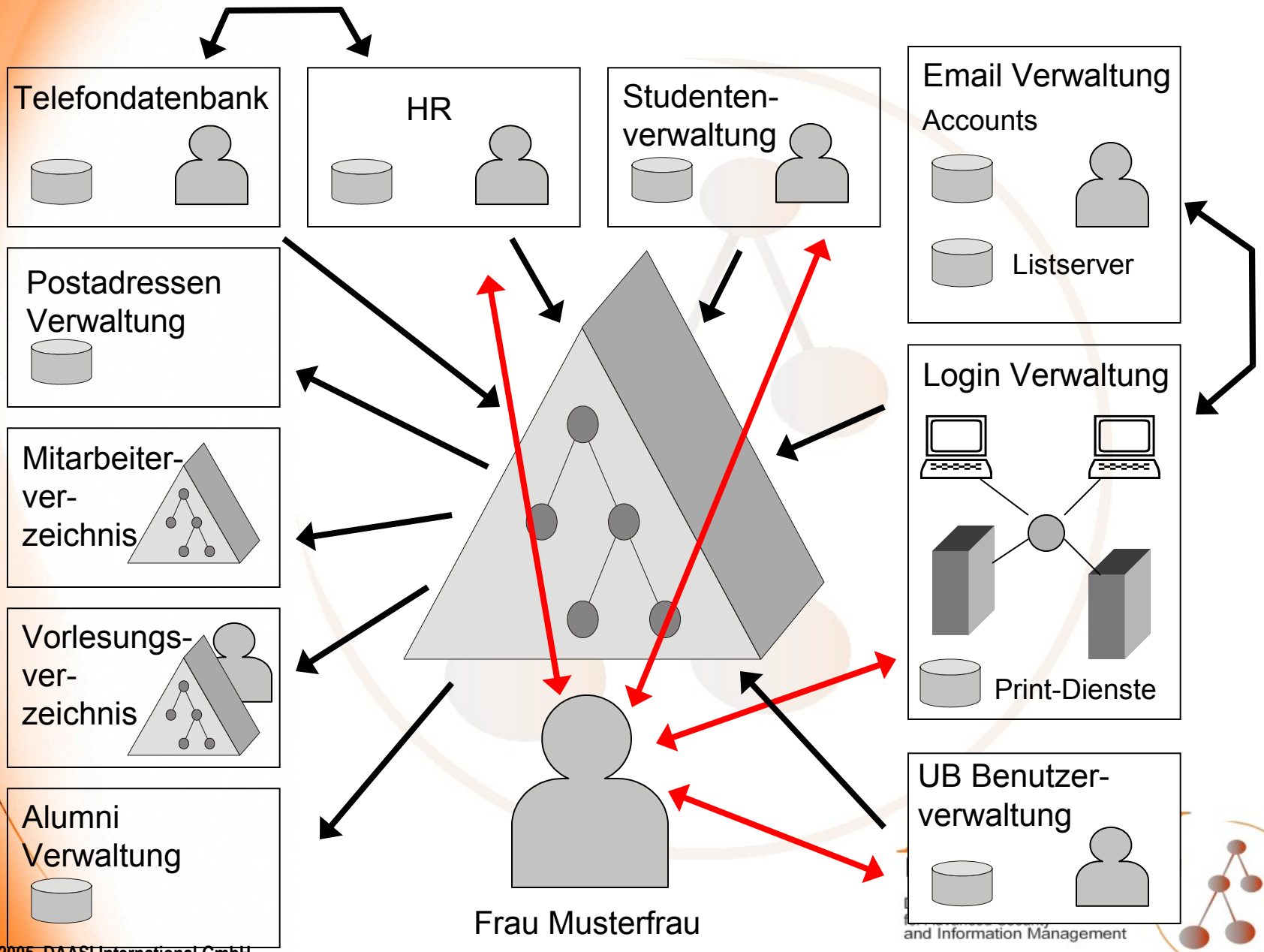


Ergebnis des Worst Case Scenario

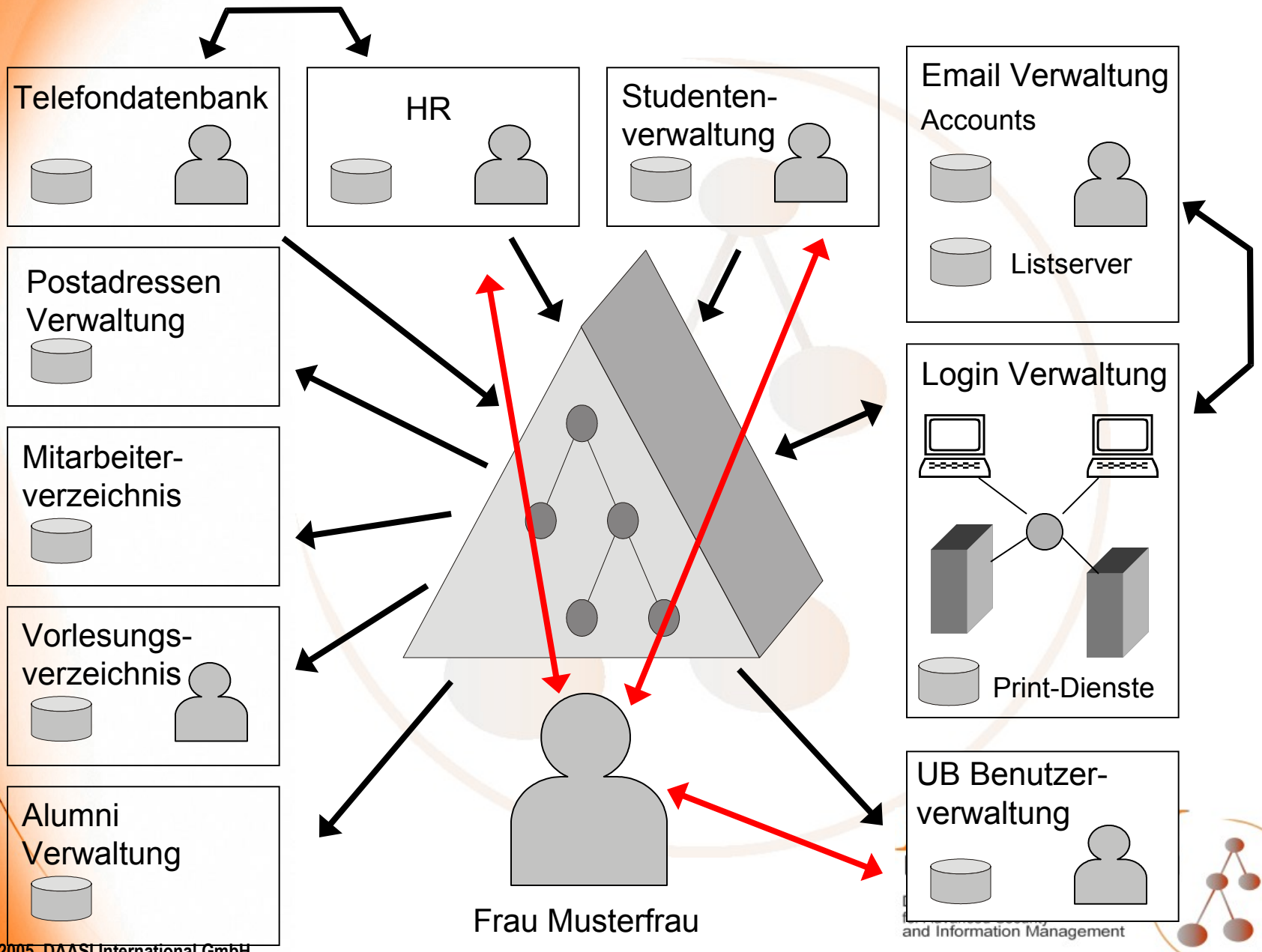
- Frau Musterfrau hat:
  - 63 mal Formulare ausgefüllt
  - und ist mit 10 verschiedenen Verwaltungsmitarbeitern in Kontakt getreten.
  - Ihre persönlichen Daten werden in 15 verschiedenen Datenbanken vorgehalten.
- Es warten schon weitere Benutzerverwaltungen:
  - Grid Computing Services
  - Kommunikationsplattformen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



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

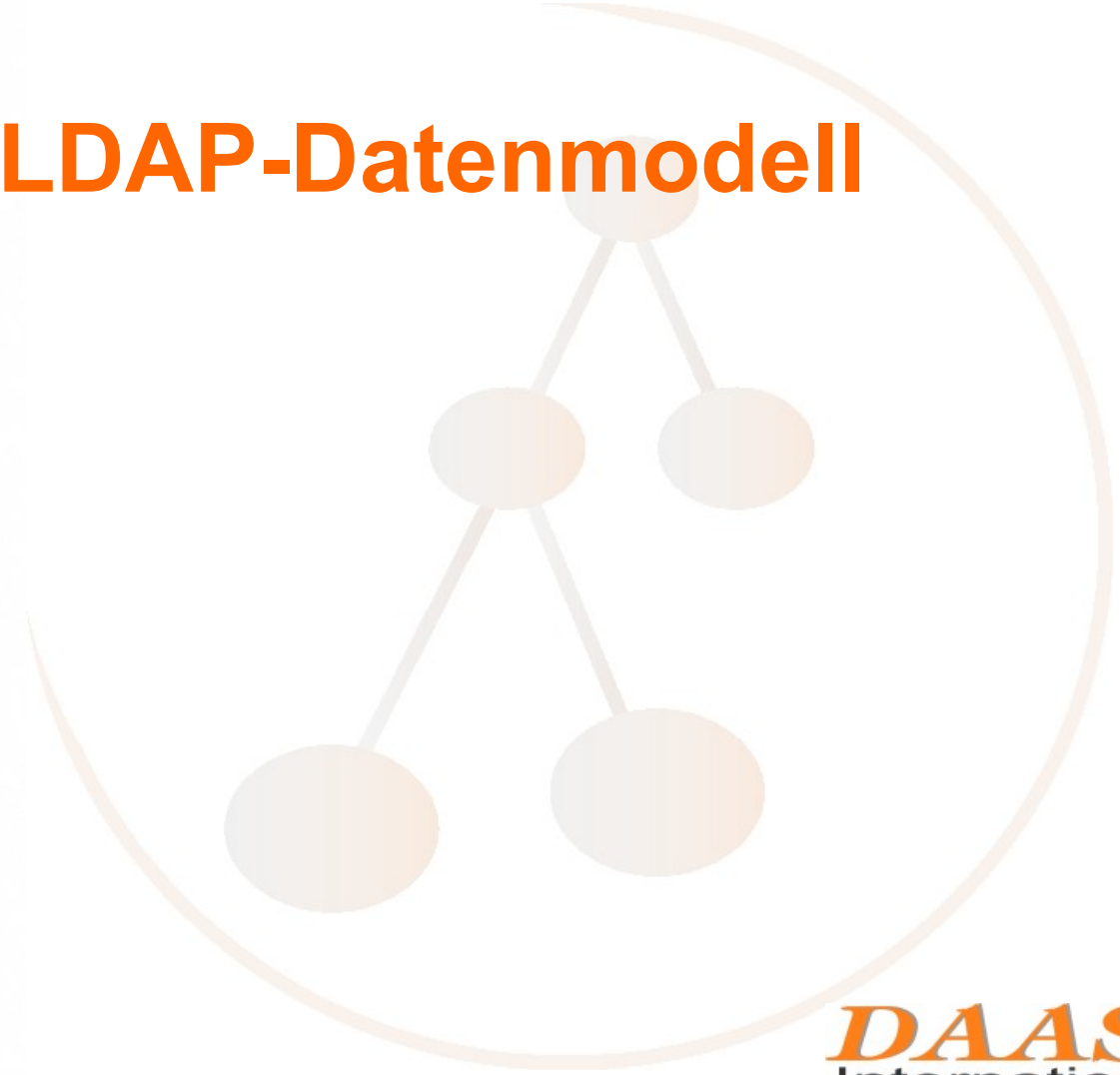
DAASI International
Directory Applications for Advanced Security and Information Management

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

Das LDAP-Datenmodell



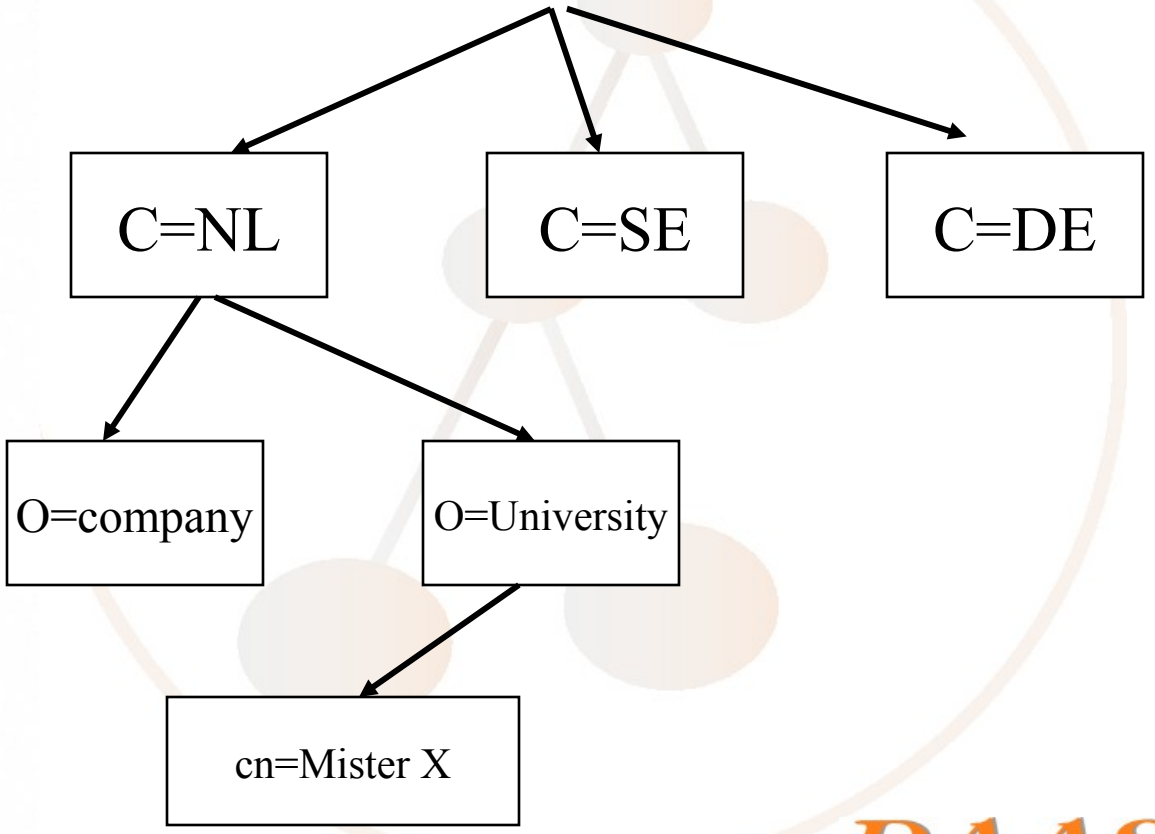
DAASI International
Directory Applications
for Advanced Security
and Information Management

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)



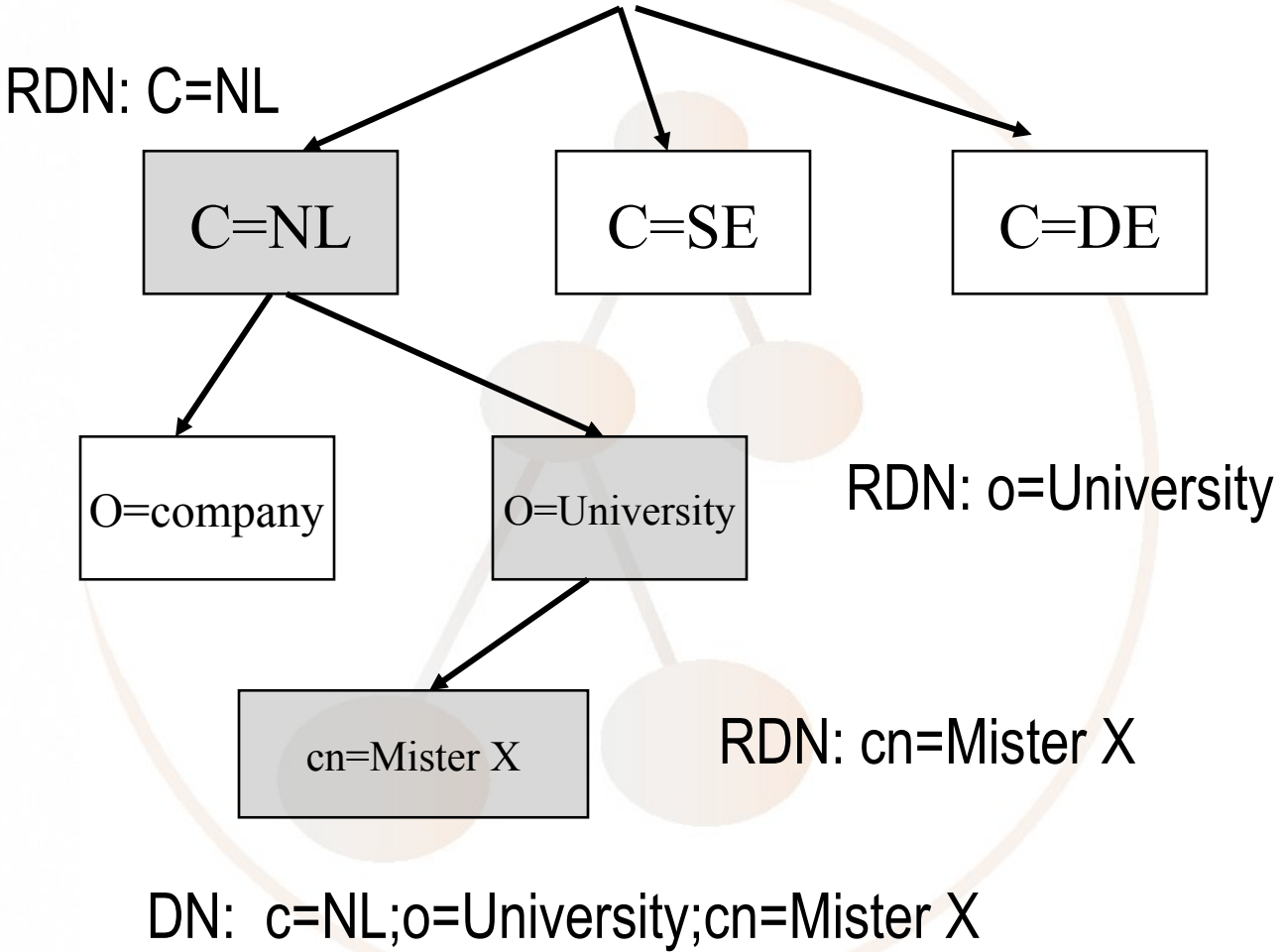
DAASI International
Directory Applications for Advanced Security and Information Management

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)

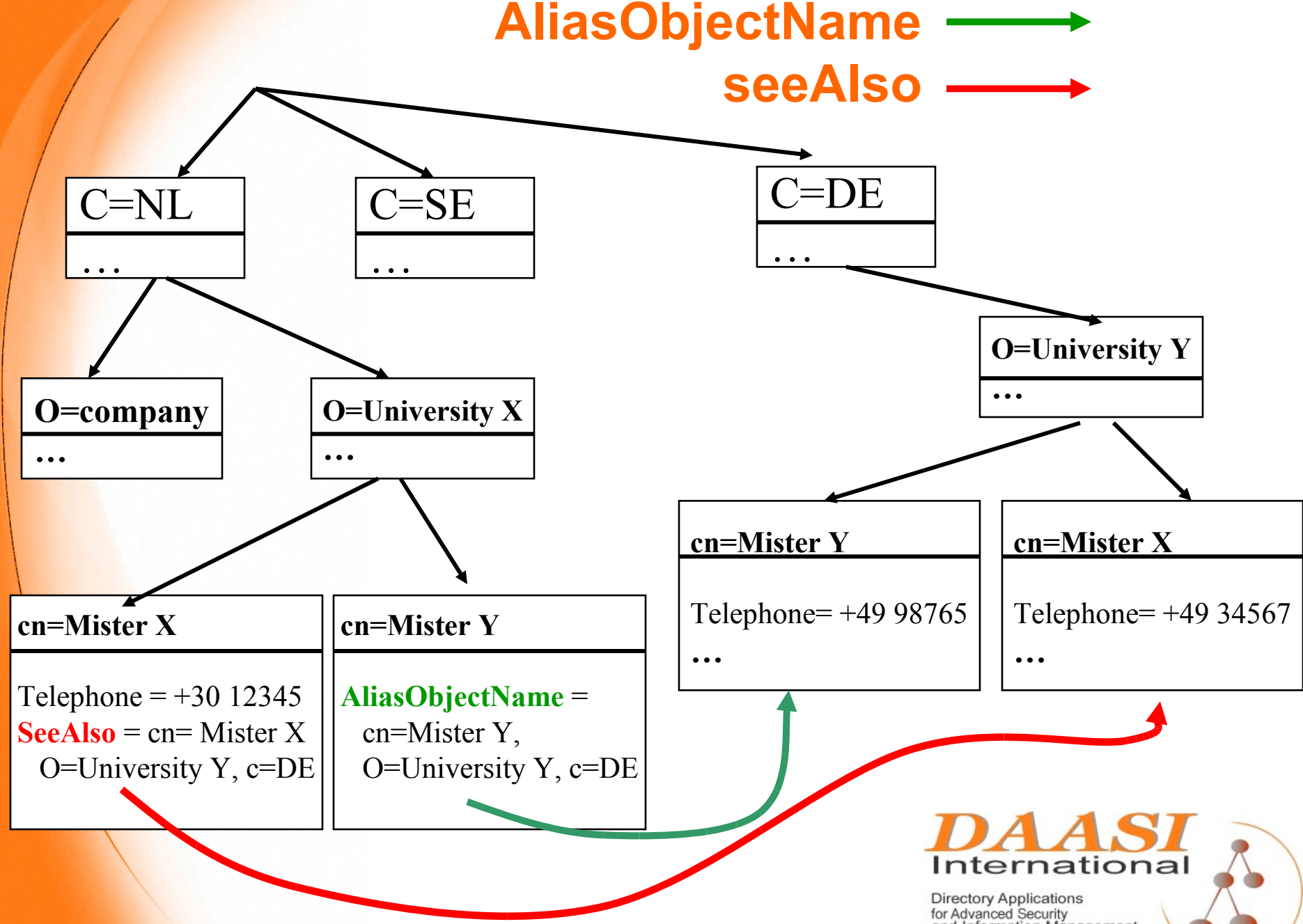


DAASI International
Directory Applications for Advanced Security and Information Management

DN Zeiger

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

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 erben

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP-Objektklassen

- Eine Objektklassendefinition spezifiziert eine LDAP-Objektklasse
- Die Objektklasse spezifiziert v.a. welche Attribute in einem von der Objektklasse modellierten Eintrag vorhanden sein müssen (MUST-Attribute) und welche vorhanden sein dürfen (MAY-Attribute)
- Man kann eine Objektklasse von einer anderen ableiten
  - die abgeleitete Klasse erbt alle Eigenschaften (Attribute) der Oberklasse, z.B.:
    - objectclass person enthält surname
    - organizationalPerson hat zusätzliche Attribute, wie RoomNumber. Surname wird aus person geerbt

DAASI International
Directory Applications for Advanced Security and Information Management

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

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, ...
```

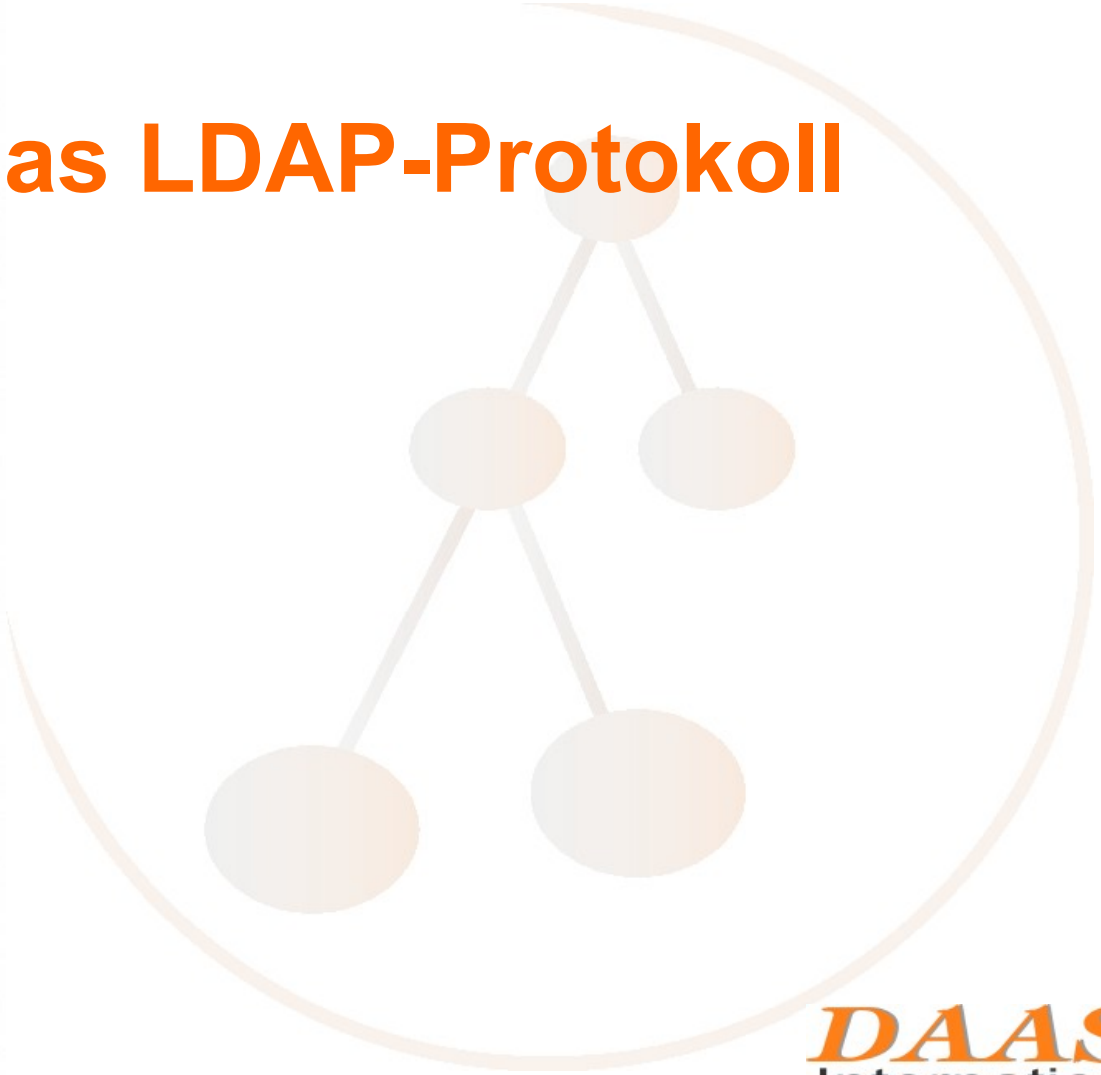
DAASI International
Directory Applications for Advanced Security and Information Management

Offene Struktur

- Man 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

25. Das LDAP-Protokoll



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

LDAP URL (RFC 2255)

- Format:
  - ldap://<host>:<portnumber>/<basedn>?<attrlist>?<scope>?<filter>?<extensions>
- Beispiel:
  - ldap://myhost.org:9999/o=University,c=NL?cn,telephonenumber?subtree?(cn=Mister X)

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 Verschlüsselungsmechanismen
  - 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

Zentrales Authentifizierungssystem

DAASI International

Directory Applications
for Advanced Security
and Information Management

Authentifizierung

- Simple Bind
  - man 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

DAASI International
Directory Applications for Advanced Security and Information Management

Authentifizierung

- Alternative Authentifizierung mittels SASL
  - Simple Authentication and Security Layer
  - vorgeschrieben: Digest MD5 (challenge response)
  - andere SASL-Mechanismen sind möglich:
    - GSSAPI (Kerberos 5)
    - X509 Strong bind
    - External: Authentifizierungsinformation kommt von tieferen Netzwerkschichten (SSL, IPSec)

DAASI International
Directory Applications for Advanced Security and Information Management

Secure sockets in LDAP

- RFC 2830
  - TLS as defined in RFC 2246
  - Client sends Start TLS extended request
  - Server sends Start TLS extended response
  - TLS version negotiation (handshake)
  - Client may bind with SASL mechanism EXTERNAL
  - Client MUST check server identity
  - Client MUST refresh cached server capability information (eg. RootDSE)

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP Authentication

- RFC 2829: Authentication Methods for LDAP, May 2000

1. Read only, public directory
   - Anonymous authentication
   - No bind or empty Bind DN
1. Password based authentication directory
   - MUST support DIGEST-MD5 SASL mechanism (RFC 2831)
   - Client binds sasl mechanism DIGEST-MD5
   - Server sends back digest-challenge
   - Client binds again sending digest-response

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP Authentication contd.

3. Directories needing session protection
   - SHOULD use certificate-based authentication with TLS (RFC2830) together with simple bind or SASL EXTERNAL
   - Client uses Start TLS operation
   - Client and server negotiate ciphersuite with encryption algorithm
   - Server requests client certificate
   - Client sends certificate and performs a private key based encryption to prove its posession
   - Server checks validity of certificate and its CA
   - Client binds simple or with SASL "EXTERNAL" mechanism

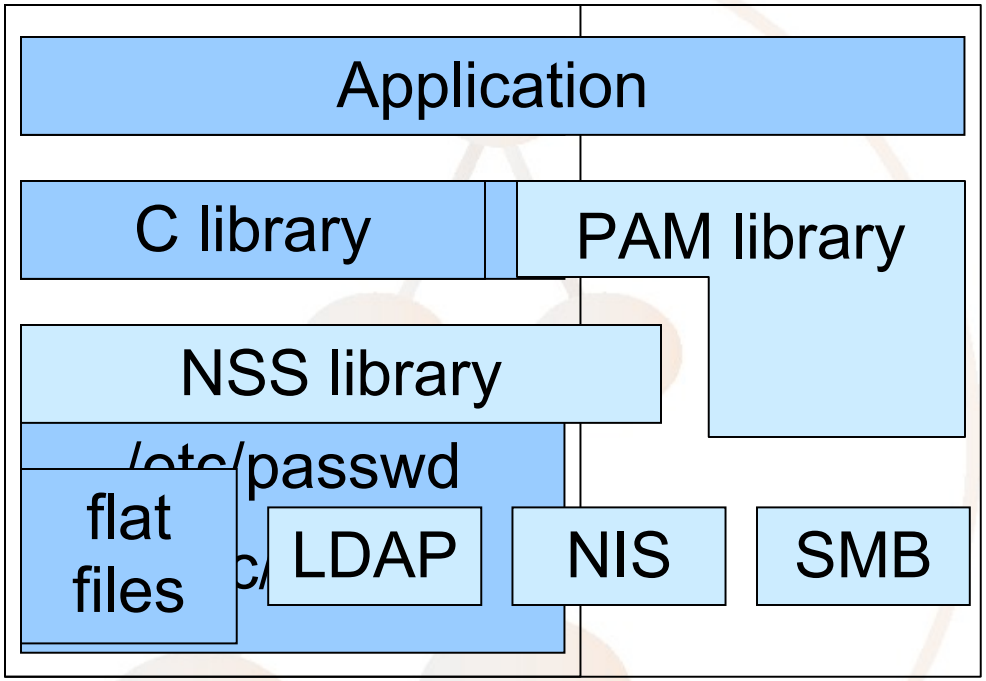
DAASI International
Directory Applications for Advanced Security and Information Management

Security threats in LDAP

- There had been a few buffer overflow holes in, e.g. OpenLDAP that could be used for DoS attacks
  - Only few and fixed quickly
- There are some password crack tools
  - Kold „Knocking on LDAPs Door“ online brute force dictionary attack in C (www.phenoelit.de)
  - The same in Perl: LDAP_Brute.pl (angreypacket.com)
  - Lumbejack offline brute force dictionary attack on LDIF files (www.phenoelit.de)
- Sniffers could read clear passwords
- None of these can harm, if you have your access control right and use encryption for LDAP connections or LDIF file transfer

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

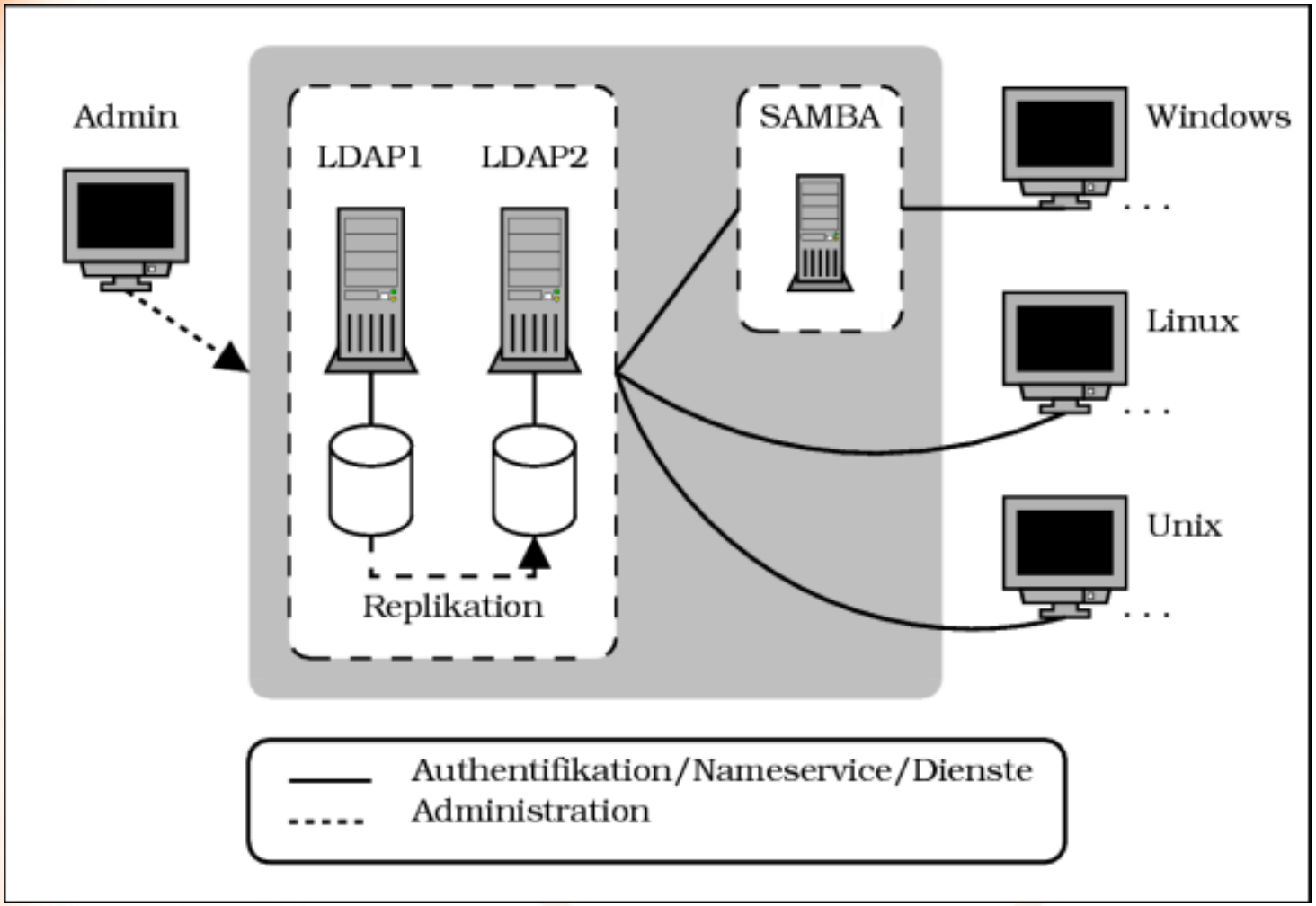
DAASI International
Directory Applications for Advanced Security and Information Management

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

Architektur der OpenLDAP-Lösung



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

Authorisierung mit LDAP

DAASI International

Directory Applications
for Advanced Security
and Information Management

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

DAASI International
Directory Applications for Advanced Security and Information Management

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.

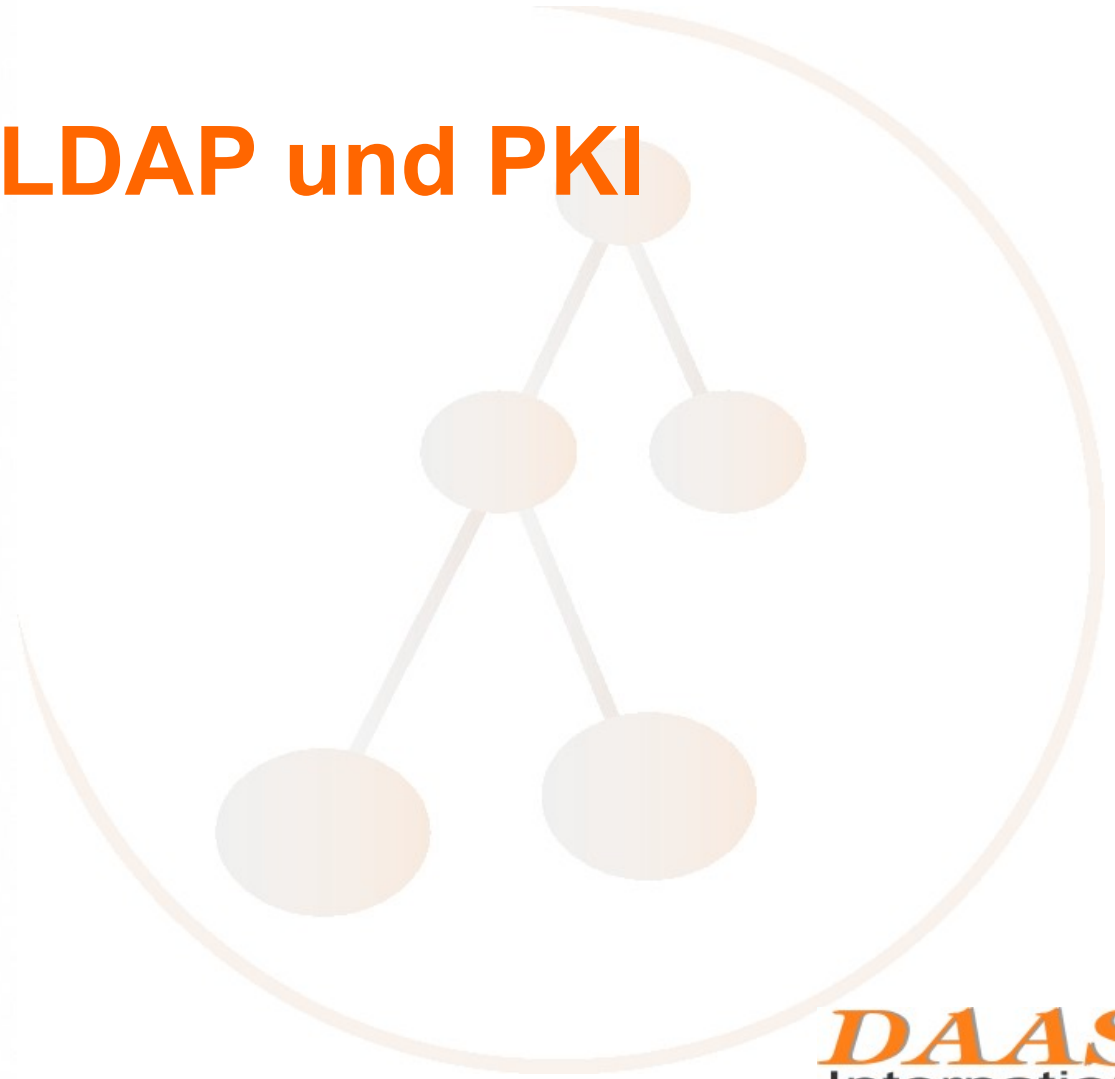
DAASI International
Directory Applications for Advanced Security and Information Management

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

LDAP und 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

DAASI International
Directory Applications for Advanced Security and Information Management

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.

DAASI International
Directory Applications for Advanced Security and Information Management

Zertifikatsserver für PKI

- Der Verzeichnisdienst
  - hält Zertifikate im Netz vor
  - Ermöglicht Zugriff durch Anwendungen
  - Dokumentiert zurückgerufene Zertifikate in sog. Certificate Revocation Lists (CRL)
  - Kann somit Grundlage eines Online Certificate Status Protocol (OCSP) Dienst bilden
- Entweder betreibt eine CA den Verzeichnisdienst selber, oder liefert Zertifikate auf einem gesicherten Weg an den Betreiber

DAASI International
Directory Applications for Advanced Security and Information Management

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

DAASI International
Directory Applications for Advanced Security and Information Management

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

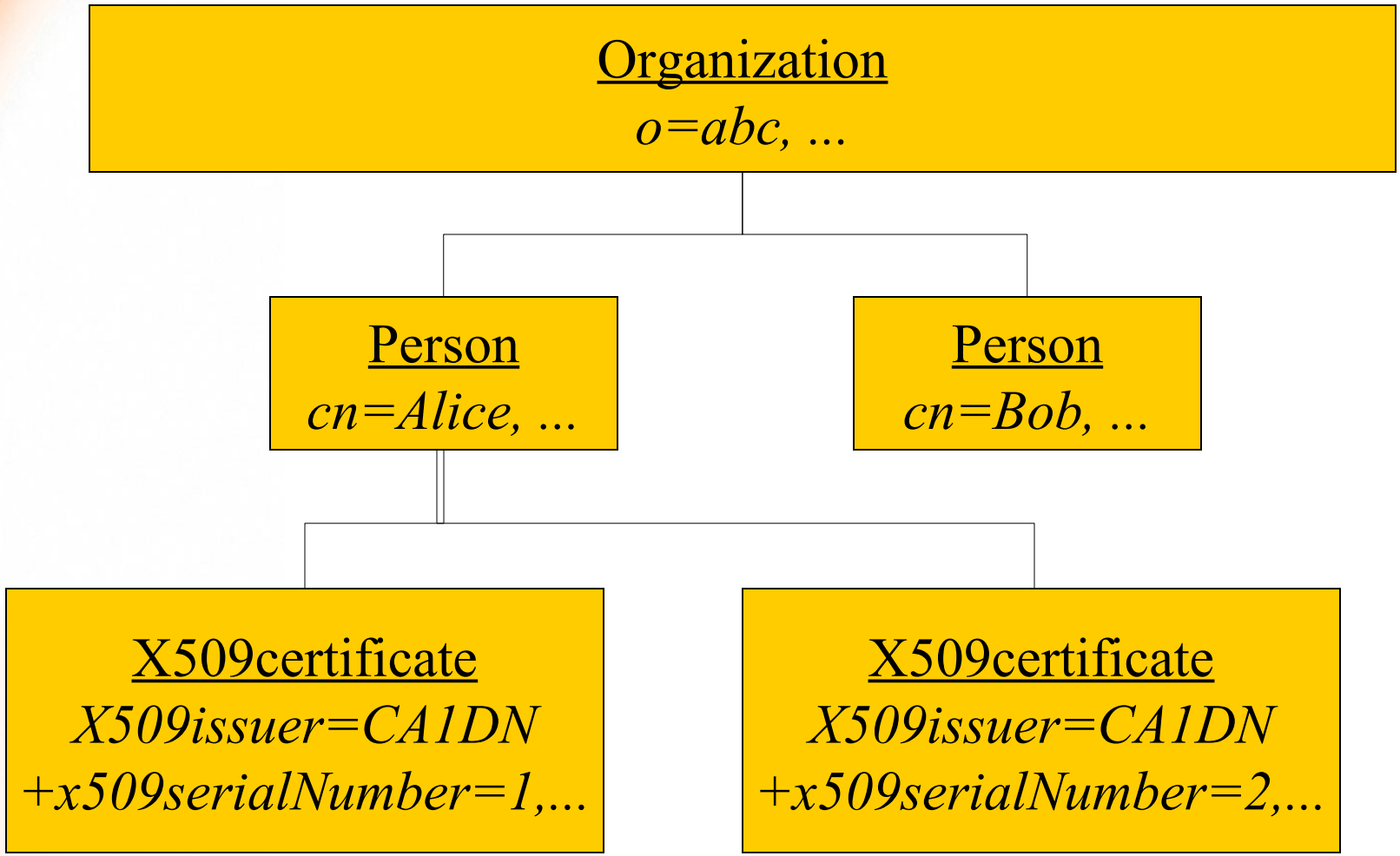
DAASI International
Directory Applications for Advanced Security and Information Management

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

DAASI International
Directory Applications for Advanced Security and Information Management

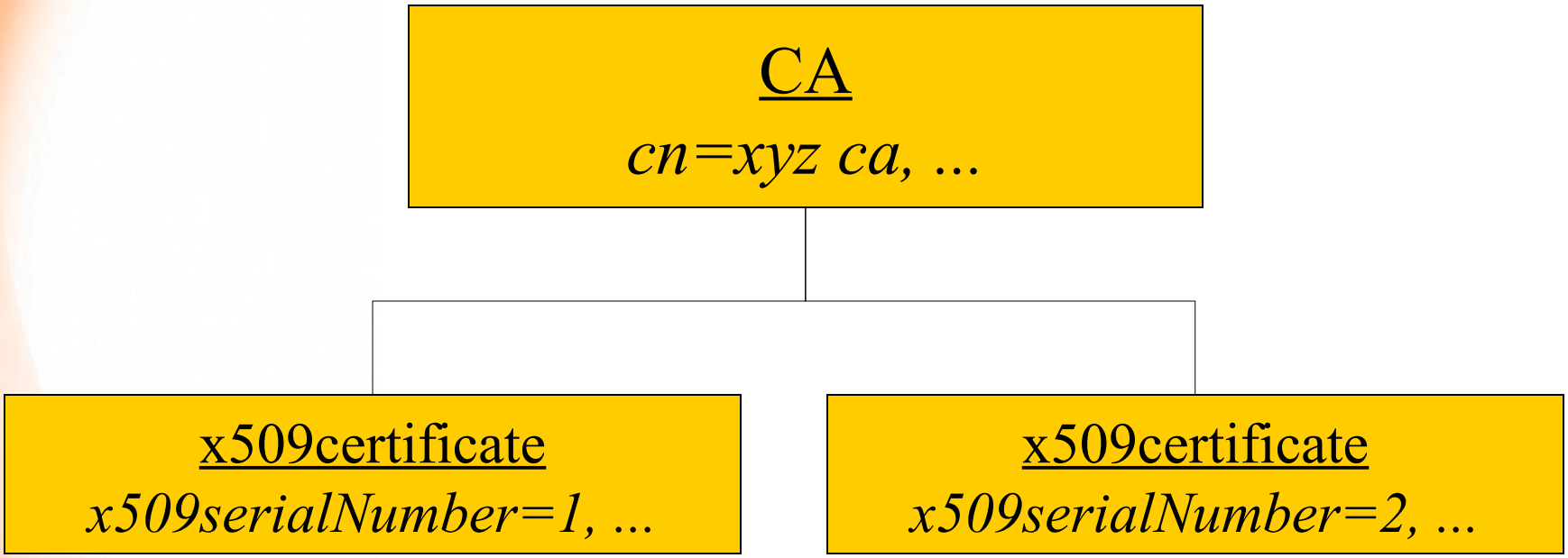
DIT-Struktur im Personenverzeichnis



DAASI International

Directory Applications
for Advanced Security
and Information Management

DIT-Struktur im Zertifikatsverzeichnis



DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit!

- Kontakt und weitere Informationen:
  - DAASI International GmbH
    Wilhelmstr. 106
    D-72074 Tübingen

    Web: http://www.daasi.de
    Mail: info@daasi.de

  - Bei späteren Fragen zum Kurs:
    Mail: peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management