# *Personenschema für das HIS-LDAP-Projekt*

Treffen des ZKI AK-Verzeichnisdienste,
Tübingen, 28.-29.6.2005

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

DAASI International
Directory Applications
for Advanced Security
and Information Management

# AGENDA

- Standardisierte Personenschemata
- Neue internationale Entwicklungen
- Stand der Arbeiten am HIS-LDAP-Projekt
  - Die Ziele
  - Die erste Version des Schemas

DAASI International
Directory Applications
for Advanced Security
and Information Management

# Personenschema im X.500 Standard

- X.500 wurde in der Version 1 1988 als weltweiter Verzeichnisdienst spezifiziert
- Erste Anwendung war internationales Telefonbuch (White-Pages und Yellow Pages)
- Deshalb wurde im Standard selbst bereits Schema u.a. zur Abbildung von Personen spezifiziert
- Diese Standard-Schemaspezifikationen wurden in LDAP übernommen (RFC 2256)

DAASI International
Directory Applications for Advanced Security and Information Management

# LDAPv3 Personenschema

## Objektklasse person:

( 2.5.6.6 NAME 'person' SUP top STRUCTURAL
MUST ( sn $ cn )
MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )

## Objektklasse organizationalPerson:

( 2.5.6.7 NAME 'organizationalPerson' SUP person STRUCTURAL
MAY ( title $ x121Address $ registeredAddress $ destinationIndicator $
preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
telephoneNumber $ internationaliSDNNumber $
facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l ) )

DAASI International
Directory Applications
for Advanced Security
and Information Management

# Probleme mit organizationalPerson

- Attributtyp title ist nur für Firmenfunktion gedacht
  - „title, such as "Vice President", of a person in their organizational context“
- personalTitle ist zwar in RFC 1274 spezifiziert aber nicht ins LDAP-Schema übernommen
- Zur vollständigen Abbildung der postalischen Adresse in Einzelattributen fehlt Attributtyp countryName / c
- Internettypische Attribute fehlen ganz

# Objektklasse inetOrgPerson (RFC 2798)

( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson'
SUP organizationalPerson STRUCTURAL
MAY ( audio $ businessCategory $ carLicense $ departmentNumber $
displayName $ employeeNumber $ employeeType $ givenName $
homePhone $ homePostalAddress $ initials $ jpegPhoto $
labeledURI $ mail $ manager $ mobile $ o $ pager $
photo $ roomNumber $ secretary $ uid $ userCertificate $
x500uniqueIdentifier $ preferredLanguage $
userSMIMECertificate $ userPKCS12 ) )

- inetOrgPerson ist anerkannter Standard und wird von allen entsprechenden Anwendungen genutzt
- Problem: Es fehlen Spezialattribute für Forschungs-Personen

DAASI International
Directory Applications for Advanced Security and Information Management

# Objektklasse eduPerson 1.5

- Von Internet2 MACE Dir entwickelt
- Als Ergänzung zu inetOrgPerson gedacht

```
( 1.3.6.1.4.1.5923.1.1.2 NAME 'eduPerson'
        AUXILIARY
        MAY ( eduPersonAffiliation $ eduPersonNickname $
                eduPersonOrgDN $ eduPersonOrgUnitDN $
                eduPersonPrimaryAffiliation $
                eduPersonPrincipalName $
                eduPersonEntitlement $
                eduPersonPrimaryOrgUnitDN )
```

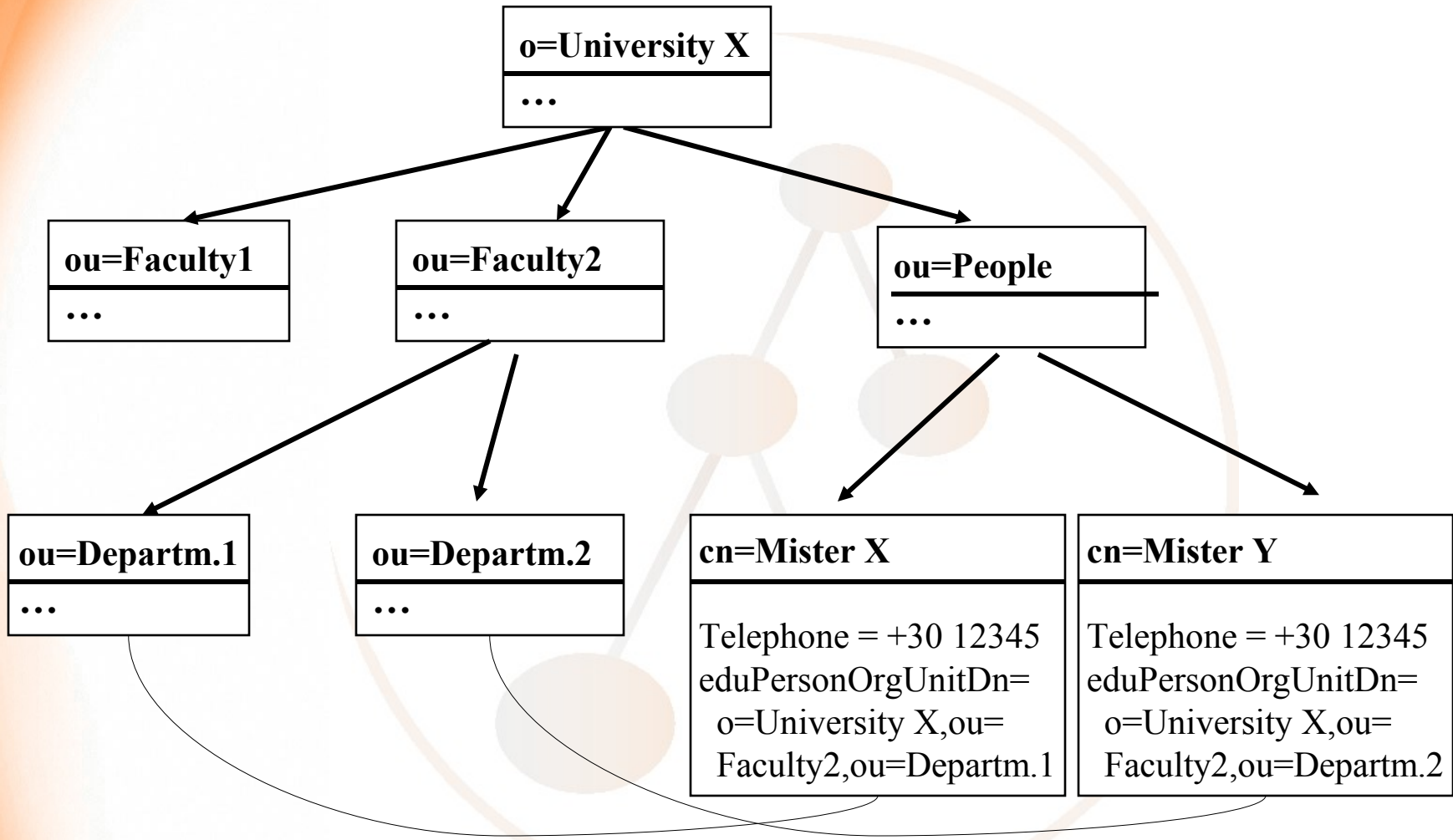
DAASI International
Directory Applications for Advanced Security and Information Management

# Diskussion über eduPerson

- Attributtypen z.T. USA-lastig spezifiziert
  - Kontrolliertes Vokabular für eduPerson(Primary)Affiliation:
    - faculty, student, staff, alum, member, affiliate, employee
- eduPersonPrincipalName ist als Identitäts-Token gedacht:
  - „The "NetID" of the person for the purposes of inter-institutional authentication“
- eduPersonEntitlement zur Abbildung von Rechten:
  - „URI (either URN or URL) that indicates a set of rights to specific resources“
- eduPersonOrgDN/eduPerson(Primary)OrgUnitDN zur Abbildung der Organisationszugehörigkeit bei einem flachen Personenbaum

DAASI International
Directory Applications for Advanced Security and Information Management

# eduPersonOrgUnitDn




DAASI International

Directory Applications
for Advanced Security
and Information Management

# TERENA Projekt DEEP

- TERENA: Europäische Vereinigung der Nationalen Forschungsnetze
- Projekt DEEP
  - Development of an European EduPerson
  - Idee: über eduPerson hinausgehende Bedürfnisse in europäischen Hochschulen zu ermitteln
  - Bedarfsanalyse via Webfrageboden
  - Wurde von DAASI durchgeführt
  - http://www.daasi.de/projects/DEEP

DAASI International
Directory Applications for Advanced Security and Information Management

# DEEP Ergebnisse

- Als relevante Attribute wurden angesehen:
  - Alle Attribute der Objektklasse person
  - 7 der 17 Attribute von organizationalPerson
  - 16 der 28 Attribute von inetOrgPerson
  - 6 der 8 Attribute von eduPerson
- Folgende Attribute wurden in den Standards vermisst:
  - socialSecurityNumber, personalTitle, areaOfInterest, unique_userid, birthdate, cv, studentnumber, classificationScheme, user_class, gender, fedID or netID, expertise, position, releasePolicy, studyBranch, expirationdate, indexingPolicy, accountstatus

DAASI International
Directory Applications for Advanced Security and Information Management

# Reaktionen von Internet 2

- Internet2 haben DEEP intensiv beobachtet und haben Interesse an Mitarbeit zu internationalEduPerson gezeigt
  - Hierzu wurde eine Internet2-Arbeitsgruppe "International Person Schema" gegründet
  - http://middleware.internet2.edu/intl-schema
  - Bisher keine Ergebnisse und die Gruppe wird als "dormant" bezeichnet

DAASI International
Directory Applications for Advanced Security and Information Management

# Reaktionen von TERENA

- Im Rahmen der TERENA Task-Force European Middleware Coordination and Collaboration, (TF EMC2) hat sich die Arbeitsgruppe SChema Harmonization Committee (SCHAC) gebildet mit den Zielen:
  - Über eduPerson hinaus
  - einen europäischen Standard
  - für Hochschulen
  - unter dem Aspekt Inter-Institutionellem Datenaustausch zu entwickeln
- Erste Vorschläge liegen vor
- Es ist sinnvoll, diese bei der Spezifizierung von HIS-LDAP-Schema zu berücksichtigen

DAASI International
Directory Applications for Advanced Security and Information Management

# Strategische Überlegungen zu HIS-LDAP 1

- Der LDAP-Server darf nicht Voraussetzung für den Betrieb von HIS-Modulen sein.
- Er soll eine einheitliche zentrale Nutzerverwaltung ermöglichen einschließlich eines Berechtigungsmanagement für HIS-GX.
- Er soll als Authentifizierungsbasis für QIS und LSF dienen können
- Die Verwaltung von Rollenmodellen für alle HIS-Module soll unterstützt werden.
- Es soll im HIS-LDAP-Server eine HIS-GX ID Nummer verwaltet werden, welche eine Person eindeutig und unabhängig von der jeweiligen Rolle identifizieren
- Die Unterstützung von Techniken wie Single Sign-On oder Unified Login sollen nicht gleich zu Beginn umgesetzt werden, aber bereits im Konzept berücksichtigt werden. Das gleiche gilt für die Unterstützung von PKI.

DAASI International
Directory Applications for Advanced Security and Information Management

# Strategische Überlegungen zu HIS-LDAP 2

- Ein Austausch von Personaldaten zwischen den HIS-Modulen soll angeboten werden.
- Unter Verwendung des LDAP-Servers soll ein Adressmanagement zur Verfügung gestellt werden. Es soll zum Beispiel möglich sein, den „Freundeskreis der Hochschule“ unter Verwendung des LDAP-Servers zu verwalten. Dies setzt die Möglichkeit der Erfassung zusätzlicher Personen direkt in LDAP voraus.
- Replikation soll zur Belieferung von hochschuleigenen LDAP-Servern aktiv unterstützt werden.
- Die Verwaltung von zentralen Tabellen (insbesondere übergreifender HIS-GX Schlüssel, ähnlich CIF) soll mit angedacht werden.
- HIS-Module sollen den HIS-LDAP-Server unter Verwendung der Stagingtabellen beliefern

DAASI International
Directory Applications for Advanced Security and Information Management

# Konkrete Festlegungen für Version 1

- Das Schema, mit welchem im HIS-LDAP-Server Personen abgebildet werden sollen, soll hisPerson heißen.
  - hisPerson wird abgeleitet von eduPerson.
  - eduPerson ergänzt als AUXILIARY-Objektklasse überlicherweise inetOrgPerson.
  - Wir gehen daher davon aus, dass auch hisPerson in diesem Sinne auf inetOrgPerson aufbaut
- Das im Rahmen des HIS-LDAP-Projekts entwickelte Schema soll mit der Objektklasse thuEduPerson (Thuringian Educational Person) des Thüringer Metadirectory-Projekts abgeglichen werden, um durch ein Mapping Interoperabilität zu gewährleisten.
- Das HIS-LDAP-Schema soll desweiteren mit Externen Arbeitsgruppen, insbesondere dem ZKI-AK Verzeichnisdienste, abgestimmt werden.

DAASI International
Directory Applications for Advanced Security and Information Management

# Vorbemerkung zum jetzigen Vorschlag

- Diskussionsvorschlag für Version 1
- Wird z.T. in die SCHAC-Gruppe eingebracht, um Interoperabilität zu erhöhen
- Steht hier im ZKI-AK zur Diskussion
  - Ihre Anregungen werden wo möglich in die Spezifikation mit eingebracht
- Die meisten Attribute sind MAY, d.h. sie müssen nicht eingepflegt werden
  - Viele spezifizierten Attribute werden wahrscheinlich nicht genutzt werden
- Der HIS-LDAP-Server ist eine interne Verwaltungsdatenbank
  - Bestimmte Attribute (Geburtsdatum, -Ort, Geburtsname, etc.) sind nur zur Ermittlung der Identität und Vergabe einer ID
  - nur ausgewählte Attribute sollten in Abstimmung mit den Datenschützern rausrepliziert werden

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Geburtsdaten

- Geburtsdatum: hisDateOfBirth
  - Singlevalue, GeneralizedTime, GeneralizedTimeMatch, Format: YYYMMDD00Z
- Geburtsort: hisPlaceOfBirth
  - Singlevalue, DirectoryString, CaseIgnoreMatch,
  - Beschreibung: Enthält den Geburtsort in der deutschen Namensansetzung
- Staatsangehörigkeit: hisCountryOfCitizenship
  - Multivalue, PrintableString, zweistelliger Landes-Code nach ISO 3166).
- Geschlecht: hisGender
  - Singlevalue, Integer, Code nach ISO 5218: 0=Not known, 1= Male, 2= Female, 9=Not specified
  - Alternativ nach RFC 2985: M/m und F/f

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Geburtsname

- Geburtsname: hisNameAtBirth
  - MUST, Single-Value
  - Beschreibung: Enthält den Nachname der Person bei ihrer Geburt. Wenn der Geburtsname nicht ermittelbar ist oder nicht erhoben wird, muss der im Attribut sn abgelegte Wert als Geburtsname angesetzt werden.
  - Da dieses Attribut zur Feststellung einer Identität verwendet wird, kann der Wert um eine Zahl erweitert werden, um bei Namensgleichheit, gleichen Geburtsort und –Datum eine Unterscheidung vornehmen zu können. Eine solche Zahl sollte jedoch nur in diesem unwahrscheinlichen Fall eingefügt werden.
  - hisNameAtBirth wird vom Attributtyp name abgeleitet.
  - Beispiel: `hisBirthName: Müller`

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Titel

- Adelstitel und sonstige Namenszusätze: hisNameExtension
  - Singlevalue, DirectoryString
  - Beschreibung: Enthält Namenszusätze zum Namen einer Person, insbesondere Adelstitel.
  - Beispiel: hisNameExtension: Freiherr von der
- Akademischer Titel: hisAcademicTitle
  - Singlevalue, DirectoryString
  - Anforderung: Man könnte das Attribut personalTitle aus RFC 1274 referenzieren, oder ein ähnliches spezifizieren.
  - Beschreibung: Enthält den/die akademische(n) Titel bzw. den akademischen Grad einer Person in der Abkürzungsform, wie sie z.B. in Adressangaben gebräuchlich sind. Also "Prof." anstelle von "Professor". Es werden alle Titel in der gebräuchlichen Reihenfolge abgebildet: "Prof. Dr. Dr. hc. Dipl. Ing."
  - Beispiel: `hisAcademicTitle: M.A.`

# HIS-LDAP-Schema: Anrede

- Anrede: hisSalutationForm
  - Singlevalue, DirectoryString
  - Anforderung: Für die Verwendung des LDAP-Servers als Grundlage eines Adress-Management-Systems ist es erforderlich, die Anredeform auszudrucken.
  - Beschreibung: Enthält vollständige Anredeformel, wie man sie am Anfang eines Briefes erwartet.
  - Beispiel: `hisSalutationForm: Sehr geehrter Herr Professor von der Mühle`

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Wohnsitz

- Wohnsitz: hisCountryOfResidence
  - Multivalue, PrintableString, zweistelliger Landes-Code nach ISO 3166).
  - Anforderung: Die Abbildung des Wohnsitzes beinhaltet zweierlei Anforderung: zum Einen geht es um eine eindeutige Kennzeichnung des Wohnsitzes, zum Anderen um die unterste Zeile einer Adressenangabe, die den Namen des Landes angibt. Name: hisPostalCountry
  - Beschreibung: Enthält Wohnsitz im zweistelligen Landes-Code nach ISO 3166
- Land in Adresse: hisPostalCountry
  - Multivalue, DirectoryString
  - Beschreibung: Enthält den Namen des Landes im Rahmen einer postalischen Adresse, wenn diese in Einzelteilen und nicht mittels des Attributs postalAddress abgebildet werden soll.
  - Beispiel: `hisPostalCountry: Österreich`

# HIS-LDAP-Schema: Gebäude

- Gebäude: hisHouseIdentifier
  - Multivalue, DirectoryString
  - Anforderung: Als Ergänzung der postalischen Adresse und des Attributs roomNumber (aus inetOrgPerson), welches erst durch eine Gebäudespezifizierung sinnvoll wird
  - Beschreibung: Enthält Name oder eine sonstiger Identifizierungsstring eines Gebäudes in dem die betreffende Person ihren hauptsächlichen Arbeitsplatz hat.
  - Beispiel: `hisHouseIdentifier: Kupferbau`

# HIS-LDAP-Schema: Adressenzusatz

- Adressenzusatz: hisPostalAdressExtension
  - Multivalue, DirectoryString
  - Anforderung: Als Ergänzung der postalischen Adresse ist manchmal ein Zusatz notwendig, wie z.B. eine Zimmernummer oder der Name eines Gastgebers bzw. Vermieters.
  - Beschreibung: Enthält einen Adressenzusatz, also ein Adressenteil, der nicht durch die anderen Adressteil-Attribute abgebildet werden kann.
  - Beispiel:

```
hisPostalAddressExtension: c/o Familie Müller
```

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Kostenstelle

- Kostenstelle: hisCostCenter
  - Multivalue, DirectoryString
  - Anforderung: Wenn einer Person ein Kostenstellenattribut zugeordnet werden soll, muss dieses als multi valued spezifiziert werden, da eine Person (siehe orgUnitDn aus eduPerson) zu mehreren Organisationseinheiten und somit Kostenstellen gehören kann. Deshalb ist es empfehlenswerter die Zuordnung Person <-> Kostenstelle über den orgUnitDn herzustellen und die Kostenstelleim OU-Eintrag zu speichern.
  - Beschreibung: Enthält die Kostenstelle auf der ein Mitarbeiter beschäftigt ist.
  - Beispiel: `hisCostCenter: 23456/78`

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Austrittsdatum

- Austrittsdatum: hisExpiryDate
  - Multivalue, GeneralizedTime, GeneralizedTimeMatch, Format: YYYMMDD00Z
  - Anforderungen: Bei Mehrfachbeschäftigung müssen mehrere Werte gespeichert werden können
  - Beschreibung: Enthält das Datum an dem voraussichtlich das Verhältnis mit der Hochschule beendet sein wird.
  - Beispiel: `hisExpiryDate: 20070201000Z`

# HIS-LDAP-Schema: Matrikulationsdaten

- Matrikelnummer: hisMatriculationNumber
  - Singlevalue, DirectoryString
  - Anforderung: Die Matrikelnummer identifiziert einen Studierenden eindeutig. Gerade wegen der geforderten Identitätsverwaltung, welche bedingt, dass eine Person, die z.B. sowohl Mitarbeiter, als auch Studierender einer Einrichtung ist, in einem LDAP-Eintrag gepflegt werden soll, macht es unmöglich, die Matrikelnummer im thematisch verwandten Attribut employeeNumber (aus inetOrgPerson) zu pflegen. Deshalb ist es unumgänglich, ein eigenes Attribut für die Matrikelnummer zu spezifizieren.
  - Beschreibung: Eindeutige ID, die einem Studierenden an einer Hochschule nur einmal vergeben wird.
  - Beispiel: `hisMatriculationNumber: 436272823`

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Matrikulationsdaten 2

- Immatrikulationsdatum: hisDateOfMatriculation
  - Sibglevalue, GeneralizedTime, GeneralizedTimeMatch, Format: YYYMMDD00Z
  - Beschreibung: Enthält das Datum ein Studierender sich an der Hochschule eingeschrieben hat. Format: YYYYMMDD00Z.
  - Beispiel: `hisDateOfMatriculation: 2002020100Z`

# HIS-LDAP-Schema: Studiengang

- Studiengang: hisCourseOfStudy
  - Multivalue, DirectoryString
  - Anforderung: Name bzw. Art des Studienganges, der zum Teil durch das Abschlussziel definiert wird. Es ist zu überlegen, ob es ein deutschlandweit gültiges kontrolliertes Vokabular über Studiengänge gibt, das man hier voraussetzen könnte.
  - Beschreibung: Enthält erstrebten Abschluss und Fachkombination des Studiengangs mit folgender Syntax:

```
CourseOfStudy :=
Abschluss:Studienfach[,Studienfach,Studienfach]
Studienfach := Fach[ (Fachart)]
Abschluss := DirectoryString
Fach := DirectoryString
Fachart := HF|NF
```

  - Beispiel: `hisCourseOfStudy: Magister: Geschichte (HF), Politikwissenschaft (NF), Philosophie (NF)`

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Studienfach

- Studienfach / Fachsemester: hisFieldOfStudy
  - Multivalued, DirectoryString
  - Anforderung: Name bzw. Art des Studienganges, der zum Teil durch das Abschlussziel definiert wird. Es ist zu überlegen, ob es ein deutschlandweit gültiges kontrolliertes Vokabular über Studiengänge gibt, das man hier voraussetzen könnte.
  - Beschreibung: Enthält jeweils ein Studienfach und Semesteranzahl mit folgender Syntax:

```
FieldOfStudy := Studienfach:Semester
Studienfach  := Fach[ (Fachart)]
Semester     := Integer
Fach         := DirectoryString
Fachart      := HF|NF
```

  - Beispiel: `hisFieldOfStudy: Geschichte (HF): 5`

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: ID

- UUID nach UUID-URN
  - Der Wert besteht aus einer 16-Oktet-Zahl (128 Bit), die als ASCII-String kodiert wurde und als URN-Namespace interpretiert wird.
  - Eine UUID (Universally Unique IDentifier), auch GUID (Globally Unique IDentifier) genannt, ist eine in Raum und Zeit universal eindeutige Kennung.
  - Die Eindeutigkeit wird erreicht durch Verwendung einer eindeutigen Kennung (die MAC-Adresse des UUID-generierenden Systems), einem timestamp, einer UUID-Versions/Varianten-Kennung sowie einer variablen Nummer, die bei Zurückschaltung der den timestamp produzierenden Systemuhr hochgezählt wird.
  - Hierdurch wird garantiert, dass jede generierte UUID mit einer sehr hohen Wahrscheinlichkeit eindeutig ist und bleibt.

# HIS-LDAP-Schema: ID

- HIS-ID: hisUuid
  - Singlevalue, OctetString
  - Anforderung: Jede Person, die in HIS-SVA oder HIS-SOS eingepflegt wird, soll über eine ID als Identität gekennzeichnet werden.
  - Beschreibung: Enthält eine universell eindeutige Kennung nach [UUIDURN] .
  - Beispiel: `hisUuid: 03a05c28-0e64-1085-872f-0002a5d5fd2e`
  - Sobald Spezielle Syntax nach [EntryUUID] implementiert ist, kann von Octetstring auf diese gewechselt werden

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Rollendaten 1

- Es gibt verschiedene Möglichkeiten Rollen im LDAP abzubilden:
- 1.) die im Standard vorgesehene Objektklasse organizationalRole mit dem Attributtyp RoleOccupant :
  - Dieses Modell sieht vor, dass von einem Teilbaum, in dem Rollen abgebildet werden auf jeweilige Personeneinträge verwiesen wird. Dies hat den Vorteil, dass Rollenhierarchien leicht abbildbar sind, allerdings ist es sehr aufwendig ein Merkmal, wie z.B. die Emailadresse aller Rolleninhaber zu erhalten. das Programm muss zuerst den Rolleneintrag suchen, und dann alle DNs die in den Werten des roleOccupant-Attributs gefunden werden in einzelnen Lesevorgängen verfolgen, um so die Emailadressen zu sammeln.

# HIS-LDAP-Schema: Rollendaten 2

- 2.) Dynamische Rollen
  - In diesem Modell würde eine Auxiliary Objectclass (etwa hisRoleMember) dem Personeneintrag eines jeden Rollenträgers hinzugefügt, welche ein Attribut zur Verfügung stellt (etwa hisRoleMemberOf) das auf ein Rollenobjekt zeigt.
  - Hierdurch sind wiederum hierarchische Rollen möglich (getrennter Rollenbaum, der mithilfe der Objektklasse organisationalRole modelliert werden kann).
  - Die Suche aller Rollenmitglieder kann jetzt aber mit einem einzigen Suchvorgang gelöst werden: Zeige mir alle Emailadressen der Einträge, deren Attribut hisRoleMemberOf auf eine bestimmte Rolle zeigt".
  - Durch Verwendung einer Substringsuche, können auch Oberrollen gesucht werden.

DAASI International
Directory Applications for Advanced Security and Information Management

# HIS-LDAP-Schema: Rollendaten 3

- 3.) Rolleninstantiierungsbaum
  - Um z.B. zeitliche Begrenzung einer Rollenübernahme abbilden zu können, kann zuzüglich dem Personenbaum und dem Rollenbaum ein dritter Baum eingeführt werden, in dem die Verknüpfungen von Personen und Rollen in eigenen Objekten (Einträgen) abgebildet werden.
  - Im Personeneintrag wäre dann ein Verweis auf ein solches Objekt zu speichern und in dem Rolleninstantiierungsobjekt wird ein Zeiger auf die Rolle gespeichert.
  - Zwar muss in diesem Modell wieder mit häufigeren Lesezugriffen gerechnet werden, allerdings lassen sich beliebige Attribute hinzufügen, z.B. um eine zeitliche Begrenzung der Rolle abzubilden, oder um einen Verweis auf eine OU  hinzuzufügen, sodass man eindeutig sagen kann, dass die Rolle in der jeweiligen Organisationseinheit ausgeübt wird.
  - Diese Lösung, ohne einen eigenen Rollenbaum wurde vom Thüringer Projekt gewählt

# HIS-LDAP-Schema: Rollendaten 4

- Rollenabbildung: hisRole
  - Multivalue, DirectoryString
  - Anforderung: In SVA werden verschiedene Rollenmerkmale gepflegt, die nicht mit den entsprechenden Attributtypen aus eduPerson abgebildet werden können. Hierfür wird ein eigenes Attribut benötigt.
  - Beschreibung: Enthält die in SVA gepflegten Rollen. Studierende erhalten die Rolle "Student". Ein Vokabular der zulässigen Werte, kann in einer späteren Version dieser Spezifikation erstellt werden. Redundanzen mit den Werten der Attributtypen eduPersonAffiliation und eduPersonPrimaryAffiliation sind notwendig.
  - Beispiel: `hisRole: Verwaltungsmitarbeiter`

DAASI International
Directory Applications for Advanced Security and Information Management

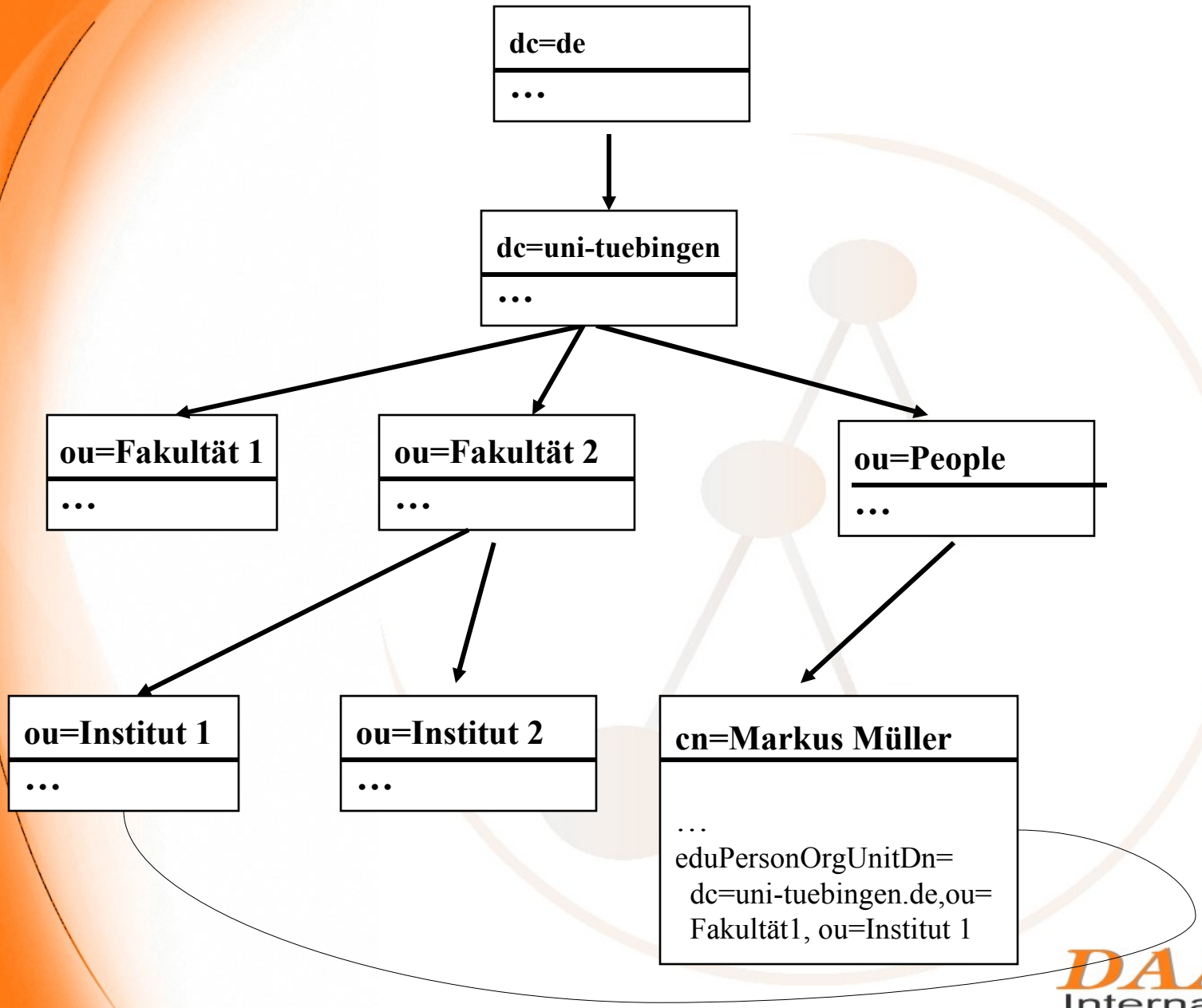
# Authentifizierungsserver

- Eine Anforderung an HIS-LDAP ist die Möglichkeit den LDAP-Server als Authentifizierungsserver verwenden zu können.
  - Dies gilt insbesondere für die Benutzerverwaltung der einzelnen HIS-Module.
  - Hierbei ist allerdings zu bedenken, dass der HIS-LDAP-Server sensible personenbezogene Daten enthält und deshalb besonders schützenswert ist.
  - Es ist dringend  abzuraten, den HIS-LDAP-Server als hochschulweiten zentralen Authentifizierungsdienst (z.B. für HIS-LSF) zu verwenden.
  - Für die Authentifizierung der Verwaltungsmitarbeiter, die die Module HIS-SVA und HIS-SOS benutzen, kann der HIS-LDAP-Server hingegen sehr wohl verwendet werden, da hierbei der Zugriff innerhalb des geschützten Verwaltungsnetz geschieht.
  - Dennoch kann der HIS-LDAP-Server als Datenquelle für einen hochschulweiten LDAP-Authentifizierungsdienst verwendet werden, indem die entsprechendenAttribute aus dem HIS-LDAP-Server repliziert werden

# Authentifizierungsserver

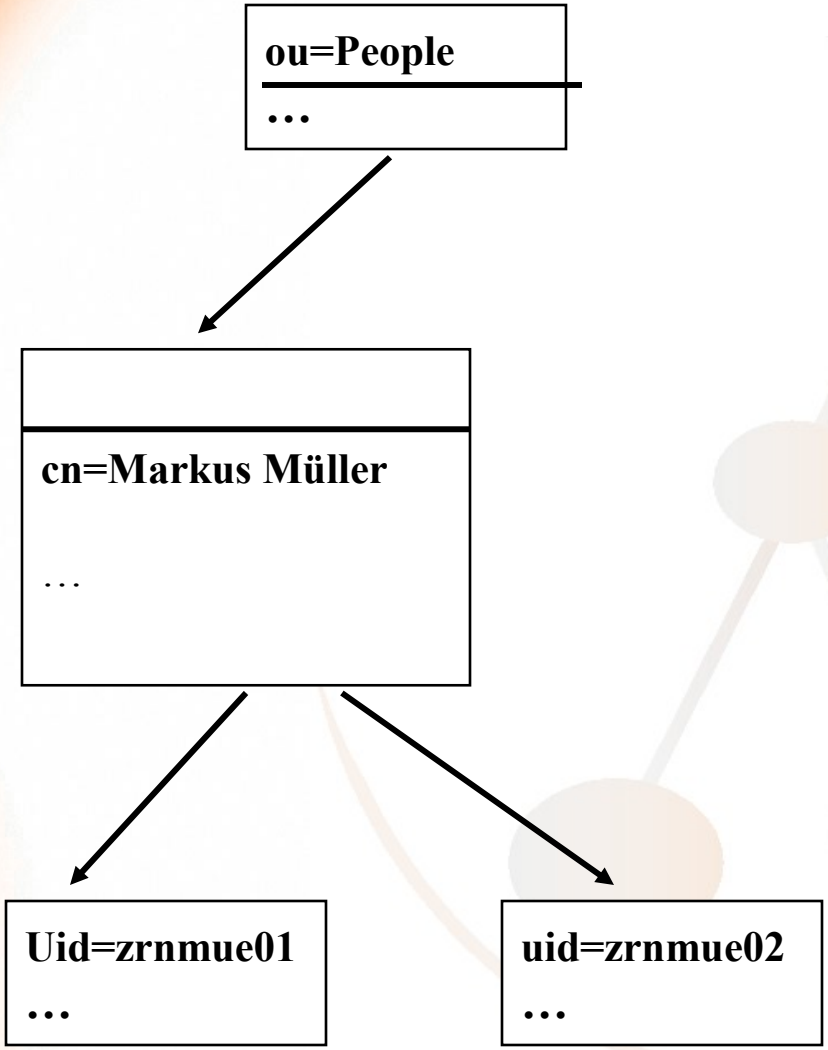
- An vielen Hochschulen kann ein Benutzer mehrere LoginIDs haben.
  - Um die Kongruenz zwischen LoginID (im Attribut uid gespeichert) und dem Passwort (im Attributtyp userPassword gespeichert) herzustellen muss unterhalb der Personeneinträge je ein weiterer Eintrag für jede LoginID eines Benutzers angelegt werden.
  - Hierfür wird ein weiterer Personeneintrag  mit der strukturellen Objektklassen person und der in [RFC 2377] spezifizierte Auxiliary Objektklasse uidObject, die nur das Attribut uid enthält, unterhalb des Personeneintrags angelegt.
  - Das Attribut uid wird auch zur Bildung des Eintragnamens (RDN)  der Login-ID-Einträge verwendet.
  - Es werden in solchen Einträgen nur die folgende Attribute belegt: sn, ·cn, ·uid, ·userPassword
  - Nur diese Login-ID-Einträge werden in den Authentifizierungsserver repliziert.

DAASI International
Directory Applications for Advanced Security and Information Management




DAASI International

Directory Applications for Advanced Security and Information Management




DAASI International
Directory Applications for Advanced Security and Information Management

# Referenzen


- RFC 1274: Barker, P., Kille, S.: The COSINE and Internet X.500 Schema, November 1991
- RFC 2256: Wahl, Mark: A Summary of the X.500(96) User Schema for use with LDAPv3, December 1997
- RFC 2798: Smith, M.: Definition of the inetOrgPerson LDAP Object Class, April 2000
- MACE Dir: http://middleware.internet2.edu/dir/
- DEEP: http://www.daasi.de/projects/DEEP
- http:/middleware.internet2.edu/intl-schema
- http://www.terena.nl/tech/task-forces/tf-emc2/schac.html
- Mealing et al: "A UUID URN Namespace", draft-mealling-uuid-urn-05.txt, December 2004, http://www.watersprings.org/pub/id/draft-mealling-uuid-urn-05.txt
- Zeilenga, Kurt, The LDAP entryUUID operational attribute, draft-zeilenga-ldap-uuid-05.txt, 20 February 2005 (work in progress), http://www.watersprings.org/pub/id/draft-zeilenga-ldap-uuid-05.txt


DAASI International

Directory Applications for Advanced Security and Information Management

# Vielen Dank für Ihre Aufmerksamkeit!

- Für Rückfragen und Anmerkungen:
  - Peter.gietz@daasi.de

- DAASI International GmbH
  - http://www.daasi.de
  - Info@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management