

# Konzeption und Umbau der Mail-Infrastruktur an der Universität Mannheim

**Dipl.-Wirtsch.-Inf. Matthias Merz**

**Dienstag, 20.03.2007**

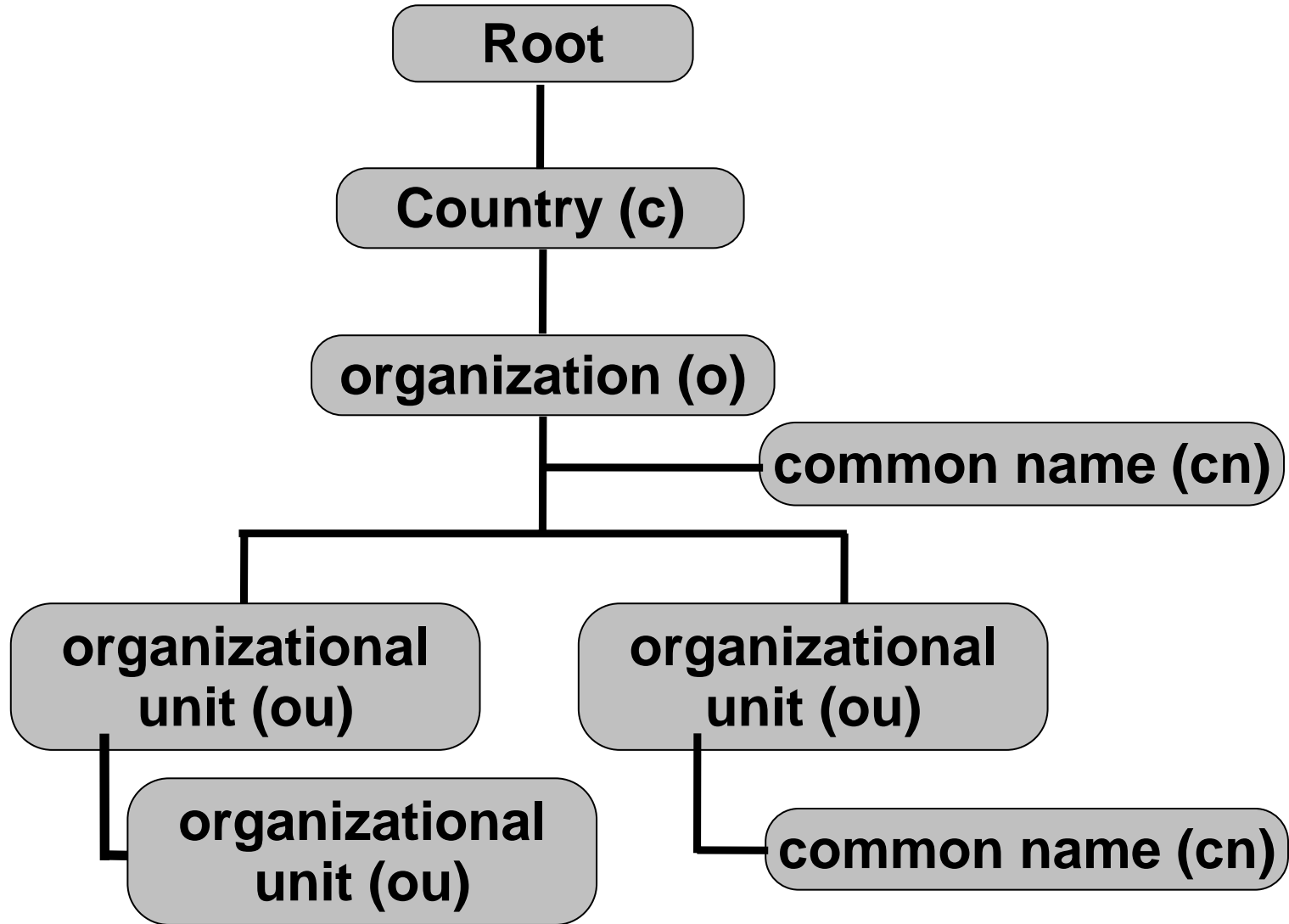
# Agenda

1. Einrichtung eines zentralen LDAP-Servers
2. Der neue Web-Mailer Horde
3. Migration der Mitarbeiter-Mailboxen

# Einrichtung eines zentralen LDAP-Servers

# LDAP

- Lightweight Directory Access Protocol
- Verzeichnisdienst mit baumartiger Datenstruktur
- Aktuelle Protokollversion: LDAPv3
- Basiert auf TCP/IP und ist optimiert für lesende Zugriffe
- Der Directory Information Tree (DIT) besteht aus Containerobjekten und Blattobjekten
- Containerobjekte sind:
  - Country (c)
  - Organization (o)
  - Organizational unit (ou)
- Blattobjekte: common name (cn)



# LDAP

Ziel:

- Etablierung einer zentralen Authentifizierungsinstanz
  - ermöglicht Anbindung unterschiedlicher Mail-Box Server
  - kann hierzu u. a. den Benutzerstatus (Student, Mitarbeiter, etc.) berücksichtigen
- Bereitstellung von Lookup-Services:
  - Verifikation von E-Mail Adressen (Reduzierung von Spam-Mails)
  - Zuordnung generischer und „echter“ E-Mail Adressen
- Zukünftig Anbindung weiterer Dienste
  - compute-Server (HPC)
  - dotlrn
  - Webserver (Webmaster)

# LDAP

- Objekte in LDAP werden durch Objektklassen (LDAP Schema) spezifiziert – diese bestimmen über welche Attribute ein Objekt verfügt
- Abhängig von der jeweiligen Objektklasse existieren Pflicht- und optionale Attribute
- Der LDAP-Server an der Universität Mannheim nutzt folgende Objektklassen:
  - **inetOrgPerson** (Mitarbeiter in einer Organisation)
  - **posixAccount** (Benutzerkennung)
  - **inetLocalMailRecipient** (E-Mail Adressen)
  - **uniMannheim**

# LDAP-Schema

- `inetOrgPerson`
  - `cn=Vorname Nachname`
  - `sn=Nachname`
  - `givenName=Vorname`
  - `ou=Fakultät_or_Einrichtung`
  
- `posixAccount`
  - `uid=RUM_Kennung`
  - `uidNumber=RUM_kennung_nummer`
  - `gidNumber=RUM_group_number`
  - `homeDir=users/fakul/uid`
  - `userPassword={SHA}xxxxxxxxxxxxxxxx`



# LDAP-Schema

- inetLocalMailRecipient
  - `mailLocalAddress=generische@mail_adresse`
  - `mailRoutingAddress=zieladresse@zb_staffmail`
- uniMannheim
  - `accountStatus=active inactive locked deleted`
  - `creationDateADMD=Datum`
  - `lastOpcodeADMD=Datum`
  - `modificationDateADMD=Datum`
  - `passwordChangeADMD=Datum`
  - `userRole=compute_webmaster_etc`
  - `userType=student staff extern absolventum`

# LDAP-Directory Information Tree

Aufbau des Directory Information Tree:

- `dc=uni-mannheim,dc=de`
  - `ou=users`
    - `uid=merz`
      - ...
      - ...
      - ...

(`dc` = Domain Component, entspricht dem Internet-Domainnamen)

# Beispiel

```
dn: uid=merz,ou=users,dc=uni-mannheim,dc=de
uid: merz
cn: Matthias Merz
userPassword: {SHA} xxxxxxxxxxxxxxxxxxxxxxxxxxxx
uidNumber: xxxxx
gidNumber: xxxxx
creationDateADMD: 19951020085456+0100
mailRoutingAddress: merz@staff.mail.uni-mannheim.de
mailLocalAddress: matthias.merz@rz.uni-mannheim.de
mailLocalAddress: merz@rz.uni-mannheim.de
mailLocalAddress: support@ipacs-benchmark.org
accountStatus: active
userType: staff
```

# LDAP

Herausforderungen beim Aufbau des LDAP-Servers:

- Planungsphase:
  - Welche Daten müssen in welcher Form vorgehalten werden?
- Daten kommen aus unterschiedlichen Quellen:
  - ADMD: Informationen über Kennungen
  - Benutzerdatenbank: Generische und echte Mail-Adressen
- ADMD:
  - Skript-Plugin mit LDAP-Schnittstelle
  - Kontinuierliches Update des LDAP-Servers

# LDAP

Herausforderungen beim Aufbau des LDAP-Servers (Fortsetzung):

- Benutzerdatenbank:
  - Keine direkte LDAP-Schnittstelle
  - Export der Tabellen als Textfiles, diese werden in den LDAP eingelesen
  - Problem:
    - Große Anzahl an Datensätzen, kann nicht jedes mal importiert werden
    - Wie kann man Änderungen feststellen, wenn in dem Export hierzu keine Informationen enthalten sind?
  - Lösung:
    - Zum Feststellen von Änderungen müssen mit komplexen Skripten und dem Vorhalten unterschiedlicher Export-Versionen aufwändig Diffs-Files erzeugt werden.
    - Diese werden stündlich per Cronjob in den LDAP importiert

# Der neue Web-Mailer Horde (Version 3.1.3)

# Horde

- Open-Source-Projekt (LGPL)
- Entwicklung
  - Beginn 1998
  - Als Ein-Mann-Projekt gestartet (Chuck Hagenbuch)
  - Ausgangspunkt: IMP (Internet Messaging Program)
- Anwendungen:
  - E-Mail
  - Groupware
  - Entwicklungstools
- Ziel: Möglichst breite Unterstützung für eine Vielzahl an Backends



# Die Horde-Architektur

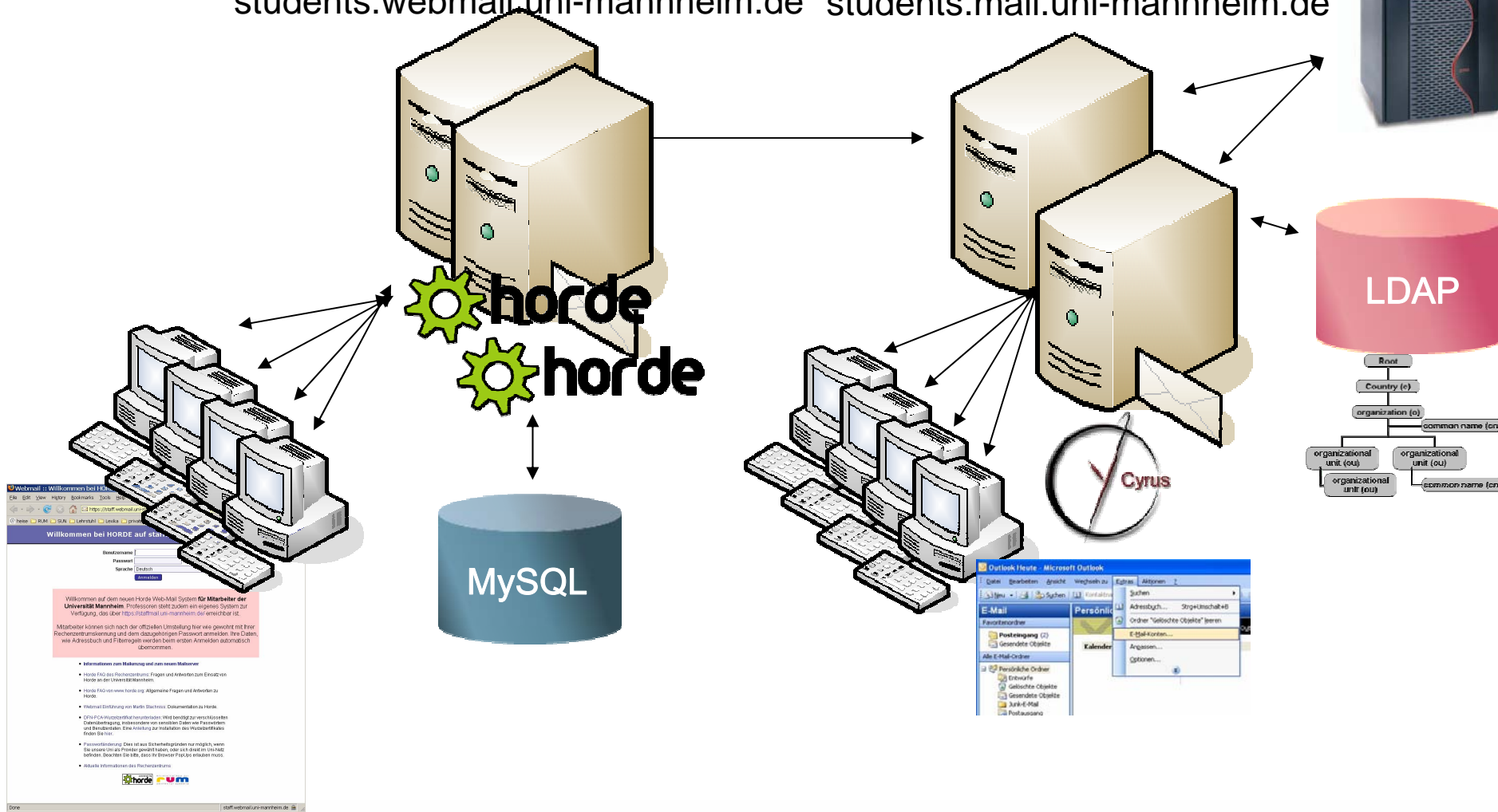
Horde bietet diverse Anwendungen in Form von Modulen:

- E-Mail:
  - **Imp** ist der Horde Web-Mail Client
  - **Ingo** ist eine Anwendung zum Verwalten von Filterregeln
  - **Mimp** Mail-Client für Mobiltelefone und PDAs
- Groupware:
  - **Kronolith** ist eine Kalenderanwendung
  - **Mnemo** ist ein Notizbuch
  - **Nag** ist ein Taskmanager
  - **Gollem** ist ein Dateimanager (Zugriff auf das AFS)
  - **Trean** ist eine Anwendung zur Verwaltung von Bookmarks
  - **Turba** ist ein virtuelles Adressbuch mit Unterstützung für vCards
- Entwicklungstools:
  - **Chora** ist eine Anwendung zum Betrachten von CVS und Subversion Repositories



# Horde an der Uni-Mannheim

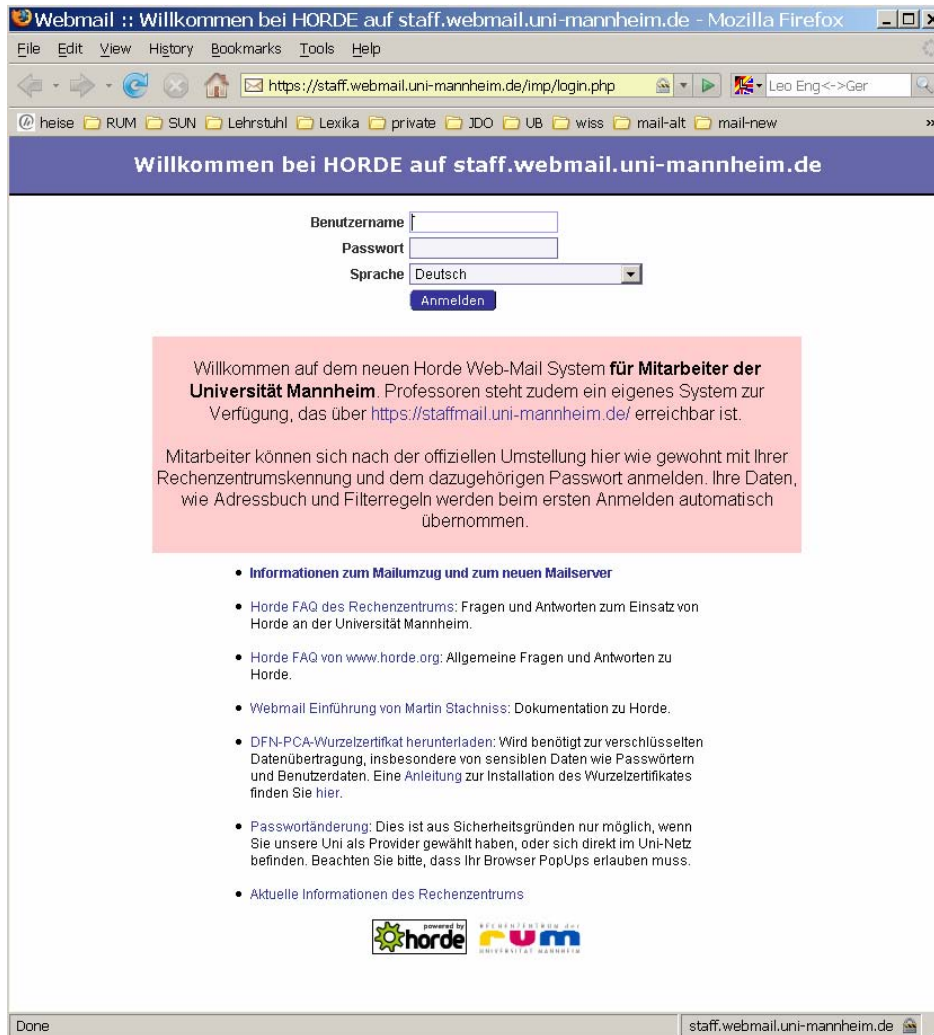
staff.webmail.uni-mannheim.de    staff.mail.uni-mannheim.de  
 students.webmail.uni-mannheim.de    students.mail.uni-mannheim.de



# Horde an der Uni-Mannheim

- Derzeit drei Webmailer im Einsatz:
  - Web-Mail für Mitarbeiter der Universität soweit Umgezogen
  - Web-Mail für Studenten und nicht Mitarbeiter
  - Web-Mail für Professoren
- Neue Funktionen:
  - Filterregel flexibler einsetzbar (z. B. Spamfilter vor der Abwesenheitsnotiz)
  - Anzeige Speicherplatz-Kontingents (Quota)
  - AFS-Anbindung
  - Mail-Client für Mobiltelefone und PDAs (für Mitarbeiter)  
`https://staff.webmail.uni-mannheim.de/mimp/`
  - Umfangreichere Überwachungstools für Administratoren

# Horde an der Uni-Mannheim



Willkommen bei HORDE auf staff.webmail.uni-mannheim.de

Benutzername

Passwort



Sprache: Deutsch

Anmelden

Willkommen auf dem neuen Horde Web-Mail System **für Mitarbeiter der Universität Mannheim**. Professoren steht zudem ein eigenes System zur Verfügung, das über <https://staffmail.uni-mannheim.de/> erreichbar ist.

Mitarbeiter können sich nach der offiziellen Umstellung hier wie gewohnt mit Ihrer Rechenzentrumskennung und dem dazugehörigen Passwort anmelden. Ihre Daten, wie Adressbuch und Filterregeln werden beim ersten Anmelden automatisch übernommen.

- Informationen zum Mailumzug und zum neuen Mailserver
- Horde FAQ des Rechenzentrums: Fragen und Antworten zum Einsatz von Horde an der Universität Mannheim.
- Horde FAQ von [www.horde.org](http://www.horde.org): Allgemeine Fragen und Antworten zu Horde.
- Webmail Einführung von Martin Stachniss: Dokumentation zu Horde.
- DFN-PCA-Wurzelzertifikat herunterladen: Wird benötigt zur verschlüsselten Datenübertragung, insbesondere von sensiblen Daten wie Passwörtern und Benutzerdaten. Eine Anleitung zur Installation des Wurzelzertifikates finden Sie hier.
- Passwortänderung: Dies ist aus Sicherheitsgründen nur möglich, wenn Sie unsere Uni als Provider gewählt haben, oder sich direkt im Uni-Netz befinden. Beachten Sie bitte, dass Ihr Browser PopUps erlauben muss.
- Aktuelle Informationen des Rechenzentrums

powered by  

Kurze Live Demo

<https://staff.webmail.uni-mannheim.de/>

# Migration der Mitarbeiter-Mailboxen

# Migration der Mitarbeiter-Mailboxen

Einige Kennzahlen:

- Anzahl betroffener Kennungen: ca. 3.000
- Datenumfang: ca. 110 GB
- Quota für Mitarbeiter: 2 GB pro Kennung

Vorgehen:

1. Kennungen werden auf dem neuen Mail-Server angelegt
2. Änderung der MailRouting-Adresse: Mails werden zum neuen Rechner geleitet
3. Benutzer werden per E-Mail benachrichtigt („dies ist ihre letzte E-Mail auf diesem System“)
4. Forward wird im alten System gesetzt
5. Umzug der Mailboxen

# Migration der Mitarbeiter-Mailboxen

Umstellungsablauf:

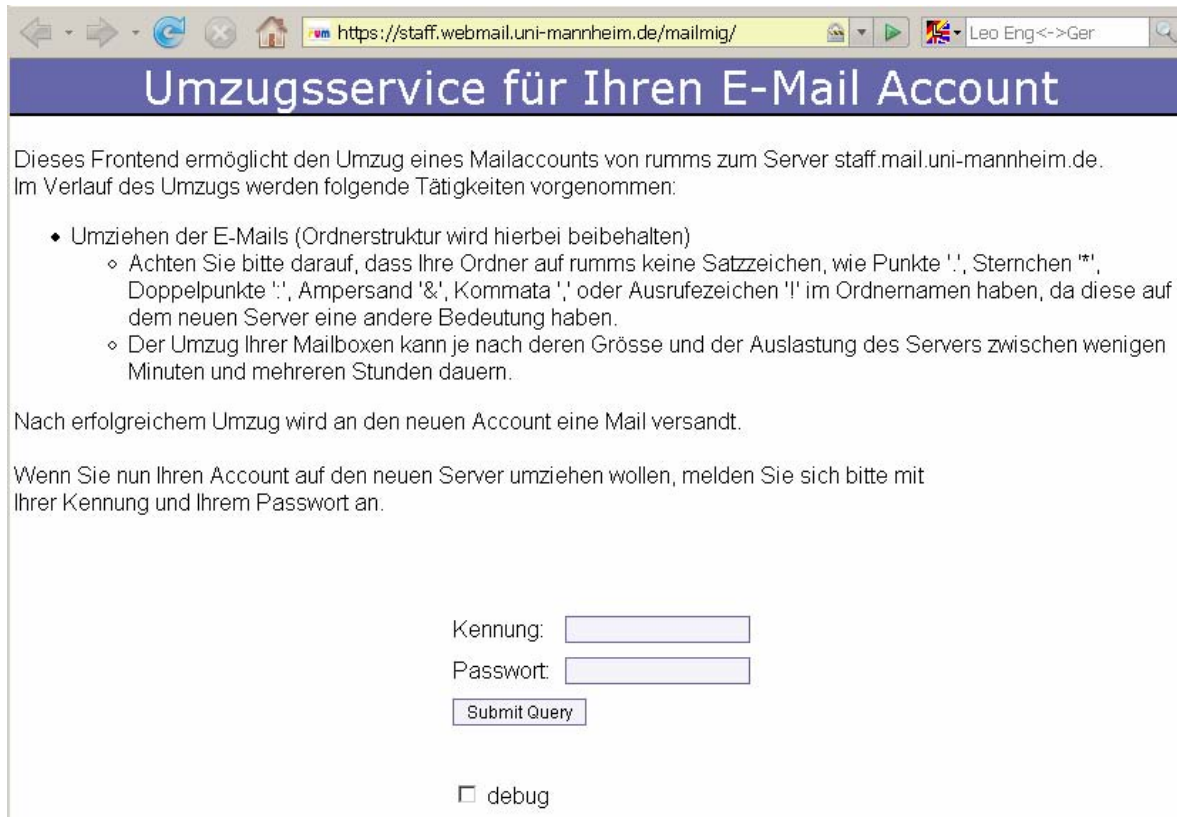
- Probe-Phase: Umstellung der Kennungen von Mitarbeitern des RUM
- Analyse: Was hat geklappt, was ging schief?
- Eigentliche Umstellungs-Phase

# Migration der Mitarbeiter-Mailboxen

Anlegen der Mailboxen:

- Ein neuer Mitarbeiter wird im Infocenter registriert
- Die Informationen gelangen automatisch über den ADMD und speziellen Skripten auf den LDAP-Server
- Sobald diese Informationen auf dem LDAP-Server verfügbar sind, können auf den neuen Mail-Server Mails gelesen und empfangen werden
- Die Kennung wird hierbei automatisch angelegt
- Einmal am Tag werden für neue Kennungen Sieve-Skripte, Mailbox-Directories und Quotas nachgetragen

# Migration der Mitarbeiter-Mailboxen



https://staff.webmail.uni-mannheim.de/mailmig/ Leo Eng<->Ger

## Umzugsservice für Ihren E-Mail Account

Dieses Frontend ermöglicht den Umzug eines Mailaccounts von rumms zum Server staff.mail.uni-mannheim.de. Im Verlauf des Umzugs werden folgende Tätigkeiten vorgenommen:

- Umziehen der E-Mails (Ordnerstruktur wird hierbei beibehalten)
  - Achten Sie bitte darauf, dass Ihre Ordner auf rumms keine Satzzeichen, wie Punkte '.', Sternchen '\*', Doppelpunkte ':', Ampersand '&', Kommata ',' oder Ausrufezeichen '!' im Ordnernamen haben, da diese auf dem neuen Server eine andere Bedeutung haben.
  - Der Umzug Ihrer Mailboxen kann je nach deren Grösse und der Auslastung des Servers zwischen wenigen Minuten und mehreren Stunden dauern.

Nach erfolgreichem Umzug wird an den neuen Account eine Mail versandt.

Wenn Sie nun Ihren Account auf den neuen Server umziehen wollen, melden Sie sich bitte mit Ihrer Kennung und Ihrem Passwort an.

Kennung:

Passwort:

debug

## Mailbox Umzugsservice:

- Benutzer melden sich mit Name und Passwort an
- Im Hintergrund werden Batchjobs gestartet
- Basieren auf dem Tool Imapsync, das die Mailboxen migriert



Danke für Eure Aufmerksamkeit!



"Didn't you get my e-mail?"