RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Einsatz und Entwicklung von LDAP an der Uni Mannheim

Heinz Kredel und Steffen Hau
Rechenzentrum der Uni Mannheim

ZKI AK Verzeichnisdienste, 8.2.2010, Uni Mannheim

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

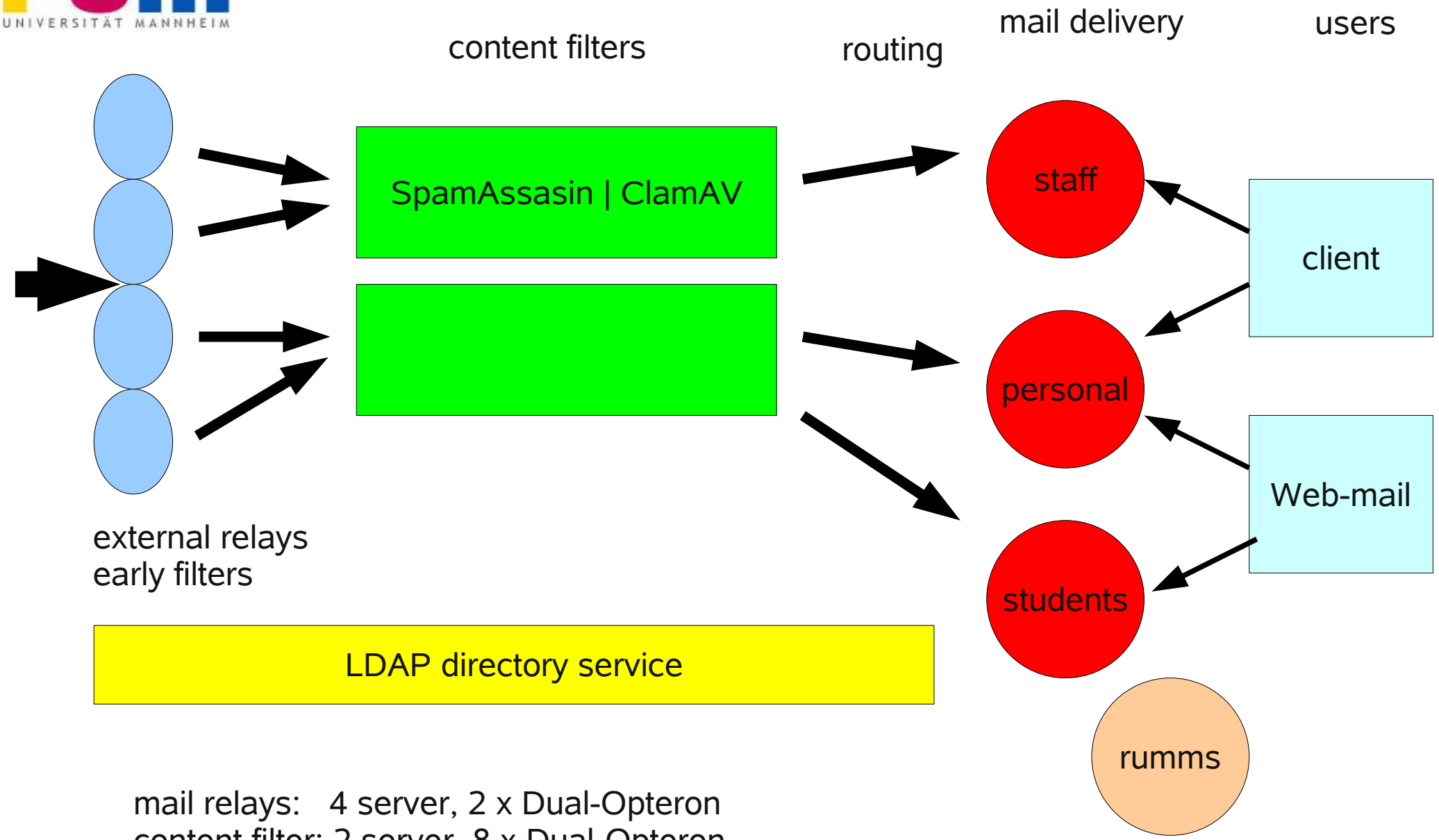
Inhalt

- Historie
  - Stand und Umfeld in 2006/2007
  - Konzeption von LDAP
- aktuelle Situation in 2010
  - LDAP
  - Provisioning für Windows-Systeme mit AD
  - CAS
- Ausblick

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Anfänge

- lange Diskussionen über PKI-LDAPs in belWü Aks ohne letztliche Einführung
- in 2006 Konzeption einer skalierbaren und verteilten Email Infrastruktur
- setzt wesentlich auf einen zentralen replizierten Verzeichnisdienst mit OpenLDAP
  - Infos über Mail-Routing und Mail Aliase
  - Authentifizierung und Autorisierung
  - Anbindung an bestehende Benutzerverwaltungen



mail relays: 4 server, 2 x Dual-Opteron
content filter: 2 server, 8 x Dual-Opteron
mail delivery: 3 server, 4 x Dual-Opteron, connection to storage system
LDAP dir: 1 server, 4 x Dual-Opteron

Target January 2007

scalable and flexible mail infrastructure

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

LDAP Design (1)

- LDAP Schemata
  - inetOrgPerson
    - cn=Vorname Nachname
    - sn=Nachname
    - gn=Vorname
  - posixAccount
    - uid=RUM_kennung
    - uidNumber=RUM_kennung_nummer
    - gidNumber=RUM_group_number
    - homeDir=/users/fakul/uid
    - userPassword={SHA}xxxxxxxxxxxxx

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

LDAP Design (2)

- inetLocalMailRecipient
  - mailLocalAddress=generische@mail_adresse
  - mailRoutingAddress=xy@zb_staffmail
- uniMannheim Schema (zusätzlich)
  - accountStatus=active inactive locked deleted
  - userRole=compute_webmaster_etc
  - userType=student staff extern absolventum

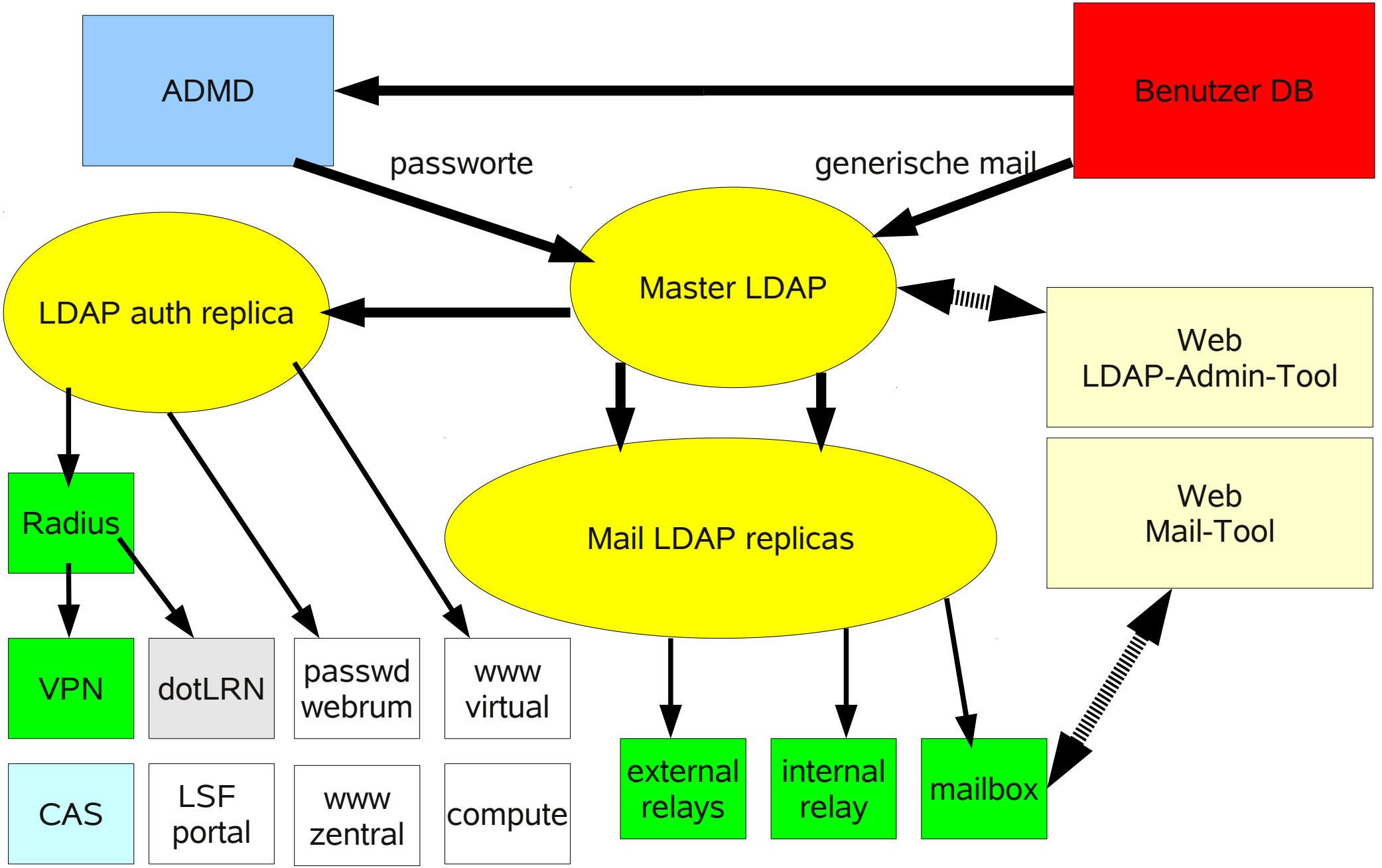
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

LDAP Tree Design

- dc=uni-mannheim,dc=de
  - ou=users
    - uid=RUM_Kennung
      - all required attributes
  - ou=institut
    - ou=insitut@uni-mannheim.de
      - mailRoutingAddress
  - ou=relay-domains
    - ou=ipacs-benchmark.org
  - ou=virtual-domains
    - ou=summacum.com

RECHENZENTRUM der UNIVERSITÄT MANNHEIM

LDAP 2007/08



Bemerkungen (1)

- Diagramme zeigen Abhängigkeiten bezüglich der Kennungsdaten und Passworte
- Pfeile zeigen die Richtung des Datenflusses
- Push und Pull/Request wird nicht unterschieden
- grüne Systeme sind in Betrieb
- weiße, graue und hellgrüne Systeme sind nicht in Betrieb
  - entweder im Test, Planung, Umbau oder inaktiv
  - in Vorbereitung zur Abschaltung

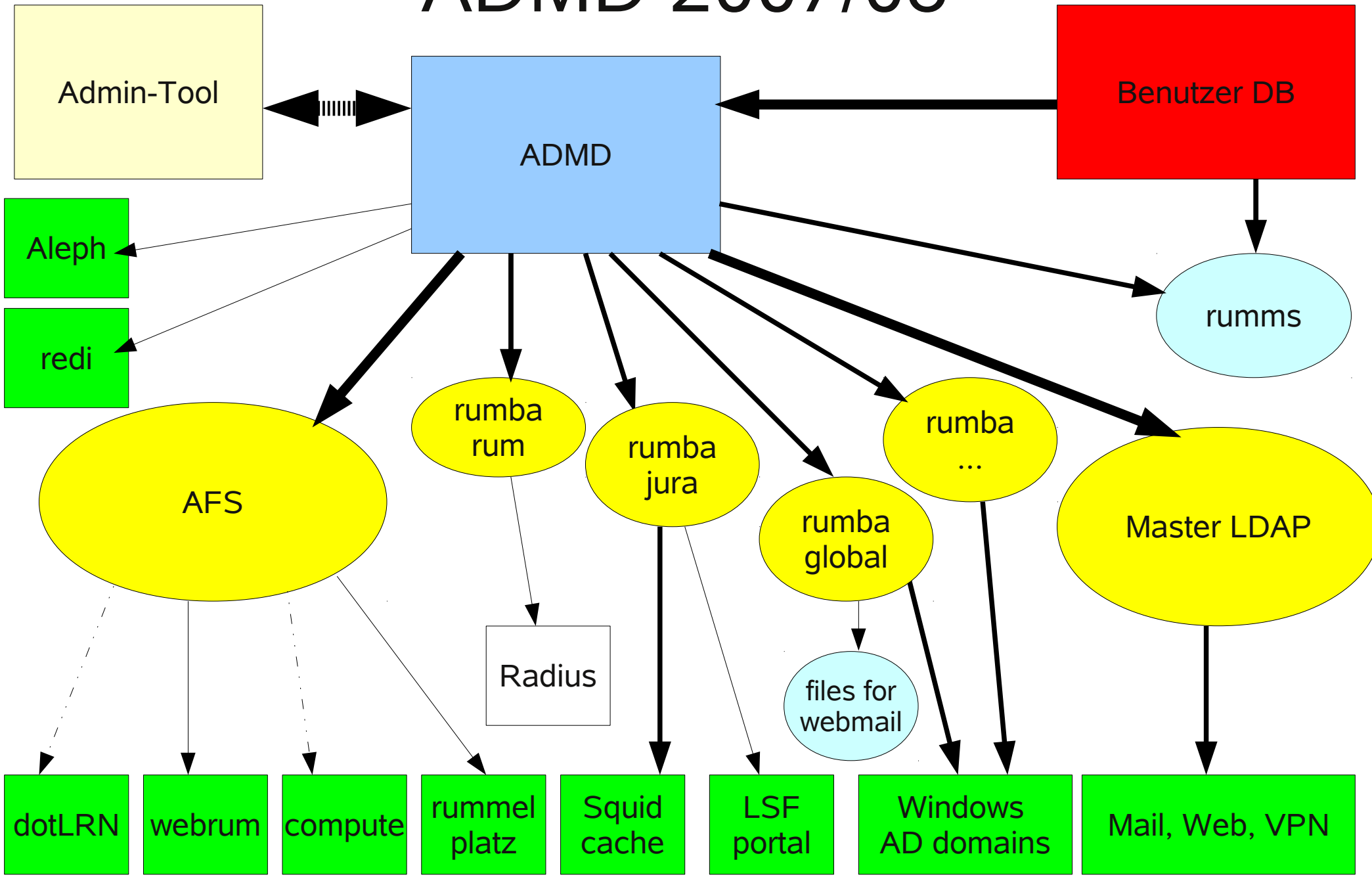
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Fragen

- Modellierung von Rollen?
  - Web-Master
  - bwGRiD User
- Abbildung der Rollen durch Attribute?
  - userType?
  - ✔ **userRole**?
- LDAP Baumstruktur für Rollen?
  - zusätzliche OUs
  - zusätzliche Schemata

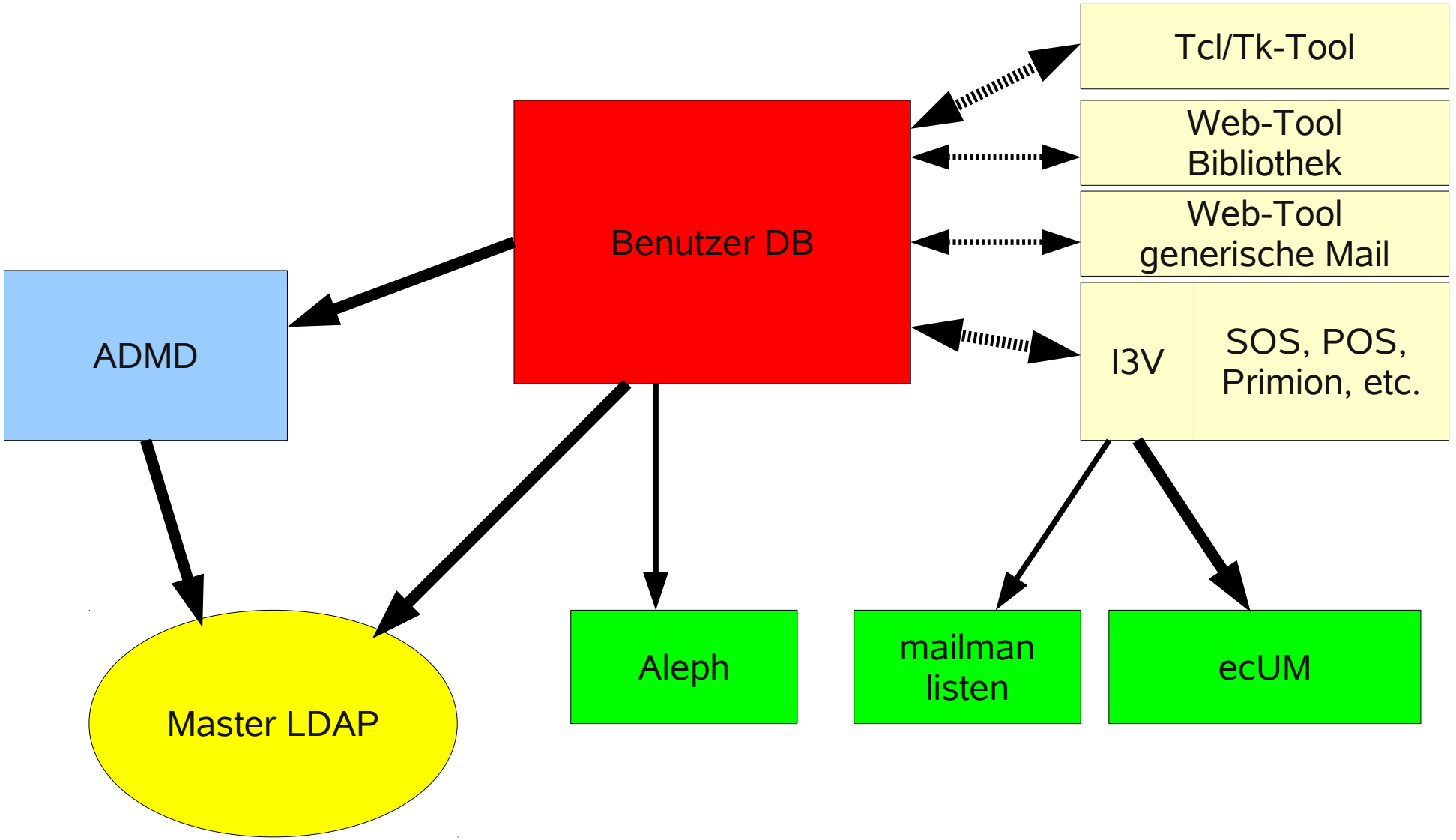
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

ADMD 2007/08



RECHENZENTRUM der UNIVERSITÄT MANNHEIM

Benutzer DB 2007/08 Überblick



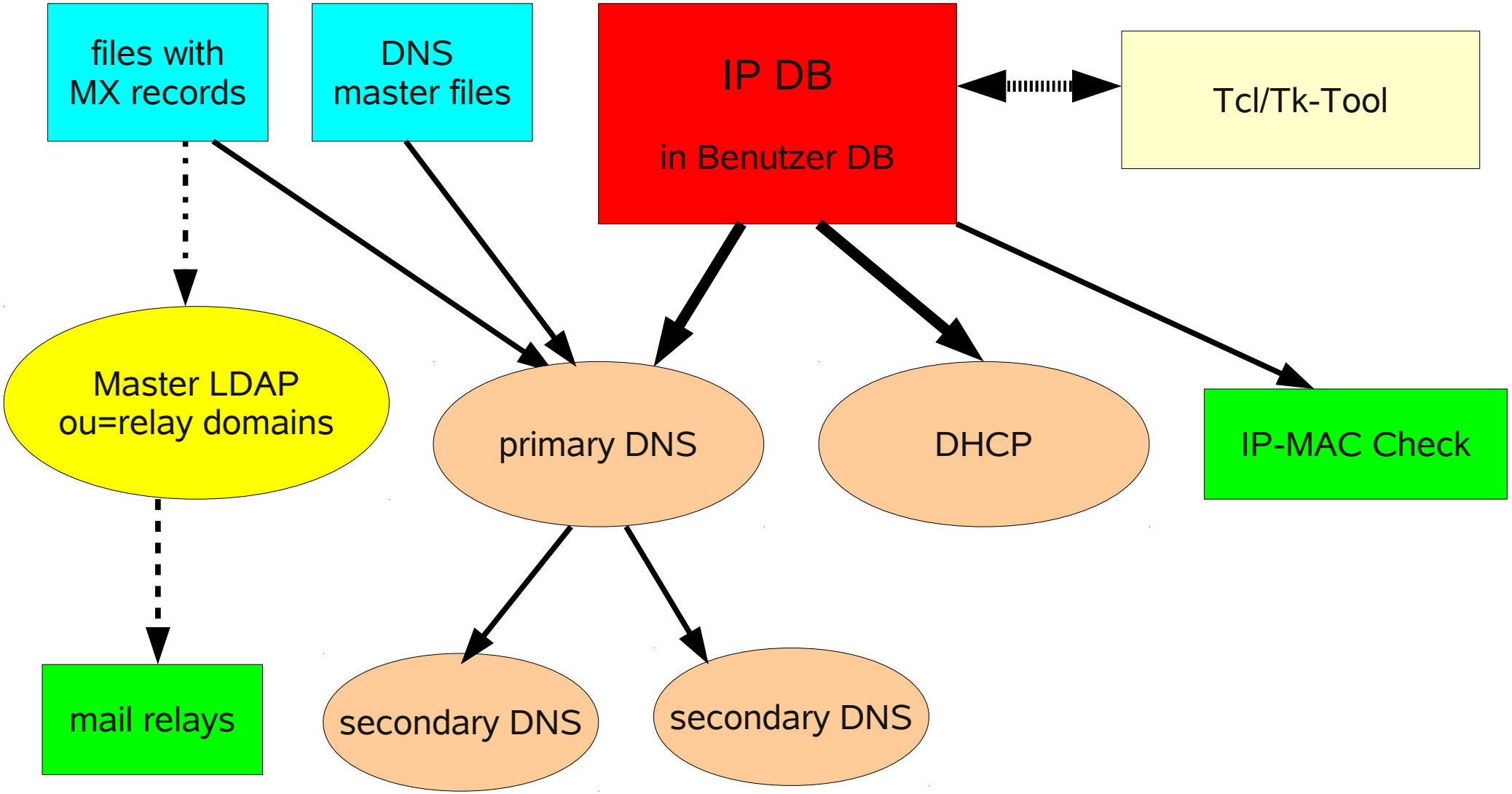
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Bemerkungen (2)

- Aleph zu ADMD über eine Datei mit Kennungs-daten und verschlüsselten Passworten
- LSF zu ADMD via HTTPS oder SSH Zugang
- Radius zu ADMD ist ausser Betrieb
- dotLRN zu LDAP, ADMD via Radius und Kennungen vom AFS

RECHENZENTRUM der UNIVERSITÄT MANNHEIM

DNS und IP DB Überblick



Bemerkungen (3)

- Diagramme zeigen Abhängigkeiten bezüglich der DNS Daten
- IP-DB enthält DNS-Namen, IP-Adressen, MAC-Adressen und Ansprechpartner
- MX records werden (nur?) über Dateien gepflegt
- aus MX records werden für die Mail-Relays Informationen zu relay-domains in den LDAP (von Hand) aufgenommen

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Aufgaben ab 2007/08

- zweiter LDAP-Auth Server
- Überarbeitung der Zugriffsrechte für die LDAPs
- CAS Installation und LDAP Anbindung
- Zugriff zu Diensten über Rollen
  - webmaster, svn-user, compute-user
- dotLRN Umstellung auf LDAP
- LSF und dotLRN Umstellung auf CAS
- Squid-Cache Anbindung an LDAP, oder CAS?
- Migration weiterer LDAP fähiger Anwendungen

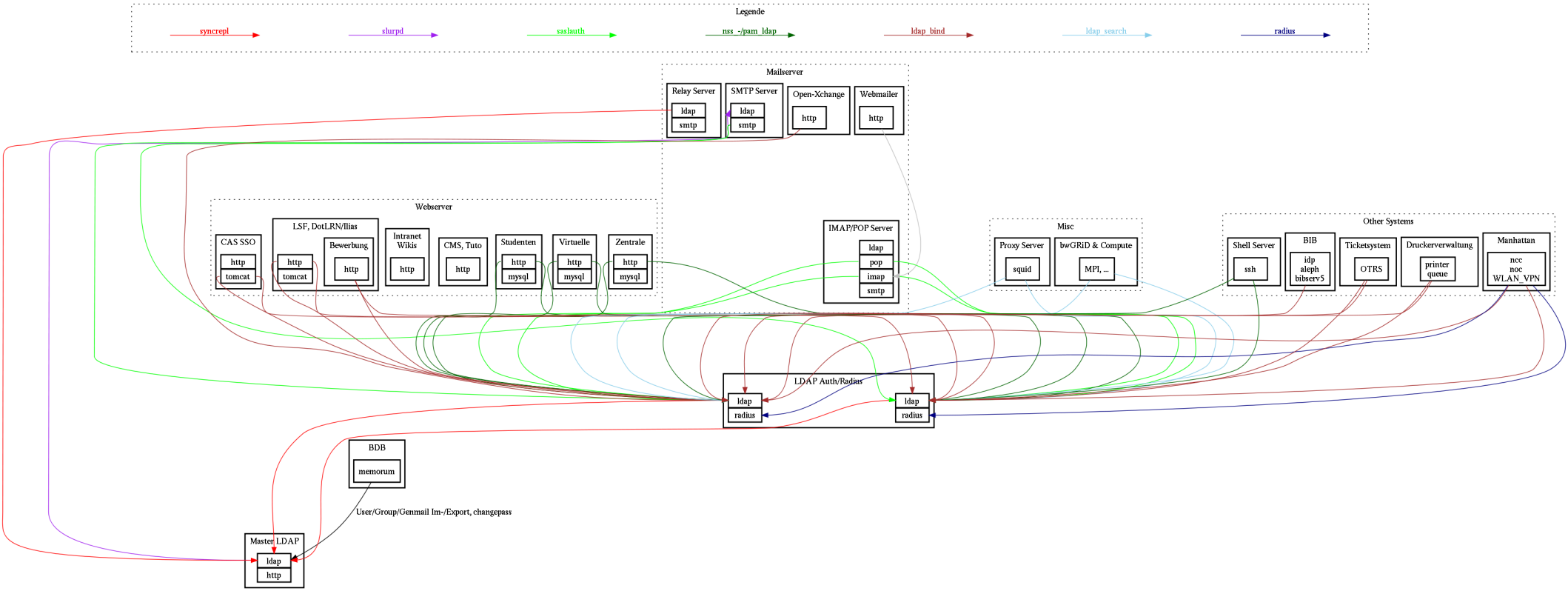
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Inhalt

- Historie
  - Stand und Umfeld in 2006/2007
  - Konzeption von LDAP
- aktuelle Situation in 2010
  - LDAP
  - Provisioning für Windows-Systeme mit AD
  - CAS
- Ausblick

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

LDAP Nutzung 2010



Serverlandschaft RUM, Gruppe Zentrale Systeme, Steffen Hau (steffen.hau@rz.uni-mannheim.de)

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

LDAP 2010 (1)

- Anbindung an LDAP wo möglich
  - ist abgeschlossen
- Umstrukturierung der Replikation von
  - slurp auf syncrepl in Arbeit
  - Master LDAP macht z.Z. beides
- Reduktion der Replikas
- Ausfallsicherheit der Auth-Replikas

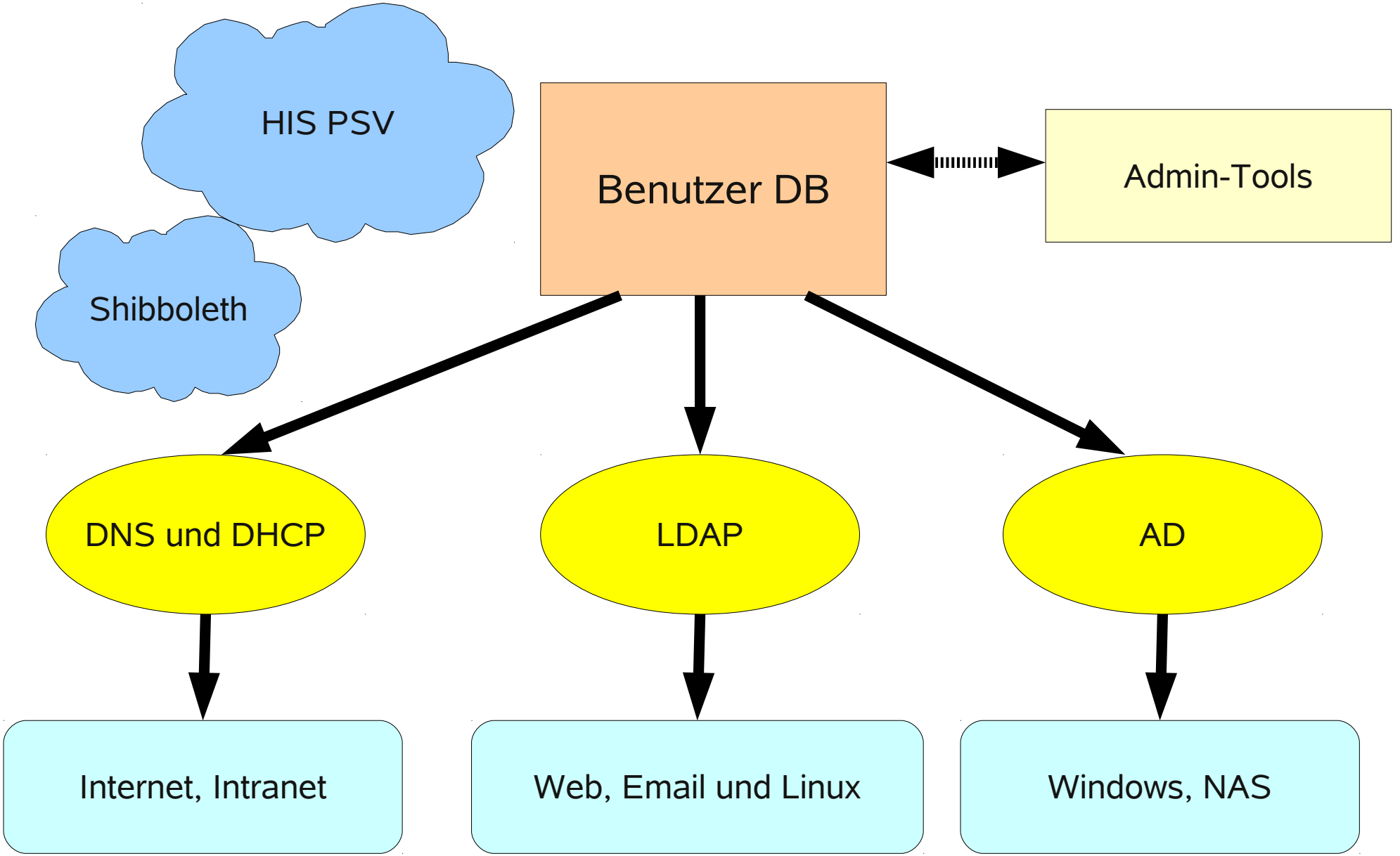
RECHENZENTRUM der UNIVERSITÄT MANNHEIM

LDAP 2010 (2)

- Erweiterung und **Pflege** der Attribute
  - proxyHash für Squid
  - loginShell und homeDirectory für bwGRiD etc.
  - rLMPassword für Adonis, WPA/WPA2 mit EAP
  - rNTPassword für Adonis, WPA/WPA2 mit EAP
  - rGender für ILIAS
- LDAP Search Autorisierung
  - IP-Adressen, viel Pflegeaufwand
  - spezielle Proxy-Kennungen pro Aufgabe/Dienst
  - Einschränkung auf eigene Attribute

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

BDB, LDAP und AD 2010



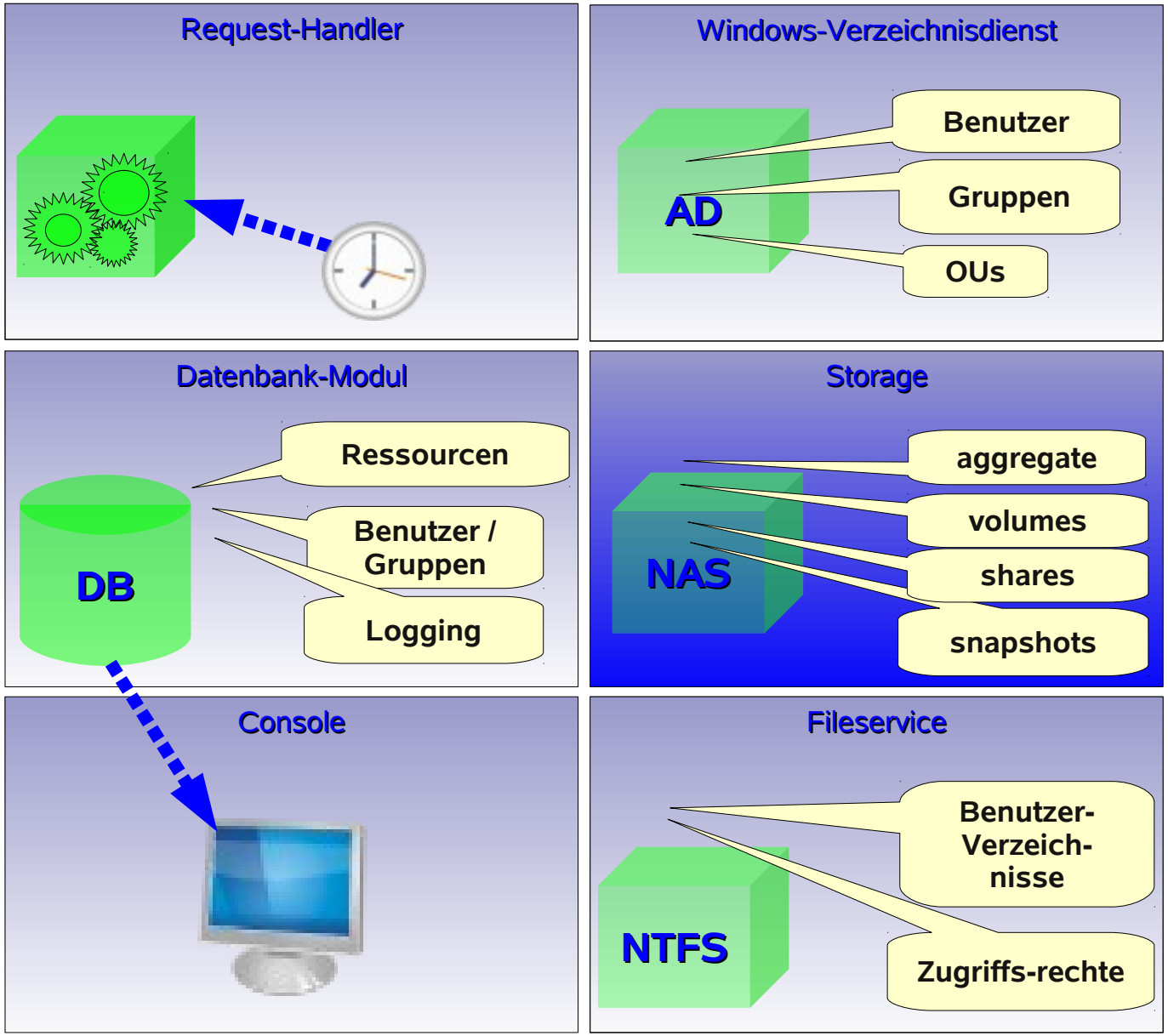
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

AD 2010

- von Werner Aufsattler
- ADMD ist abgelöst
- Provisioning System und ActiveDirectory
  - Eigenentwicklung mit PowerShell
  - Behandlung von Windows-Domänen
  - Fakultäten und Lehrstühle
- zentraler CIFS File-Space im NAS (Netapp)
  - volumes, shares, snapshots
- Windows NTFS
  - Benutzer und Zugriffsrechte

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Provisioning Komponenten



RECHENZENTRUM der UNIVERSITÄT MANNHEIM

Provisioning Bearbeitung

- Pending Request Queue
  - DB Trigger bei Veränderungen
- Anlegen des Benutzers im AD
- File-Space im NAS-Filer anlegen
  - Lst-Volume, private Volumes, public Volumes
- NTFS Verzeichnisse anlegen und Rechte setzen
- Logging: Erfolg oder Fehler
- DB Status Update bei allen Veränderungen
  - bei Erfolg wird der Request entfernt

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

CAS

- Single-Sign-On wird gewünscht
  - jetzt möglich, da (fast) keine Authentifizierungs Inseln mehr
    - nur wenige Anwendungen haben/brauchen eigene Benutzerverwaltung
- Central Authentication Service (CAS)
- Anbindung von HIS-LSF, dotLRN und ILIAS
  - Prüfungsverwaltung
  - e-learning
- eventuell auch an Horde
  - Web-Email

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

Zusammenfasung und Ausblick

- Verlässliche standardisierte Authentifizierung und Autorisierung für beliebige Dienste mit Hilfe von (Open)LDAP realisiert
- nach Ablösung von ADMD ist die Umstellung auf LDAP und AD weitgehend abgeschlossen
- Erweiterung von Single-Sign-On
- Verhältnis zu Shibboleth
- BDB Anbindung an HIS PSV
- Abbildung der PSV Rollen in LDAP und AD