TUBIS-Sphäre
Identitätsmanagement an der TU Berlin

AK Verzeichnisdienste, 27. Februar 2009

Thomas Hildmann und Christopher Ritter
IT Dienstleistungszentrum
der TU Berlin

Vortragsziele

- Darstellung der Arbeiten an der TU Berlin im Bereich Identitätsmanagement und Verzeichnisdiensten.

- Skizzierung unserer Ansätze und Lösungen (Herausstellungsmerkmale des Systems an der TU Berlin)

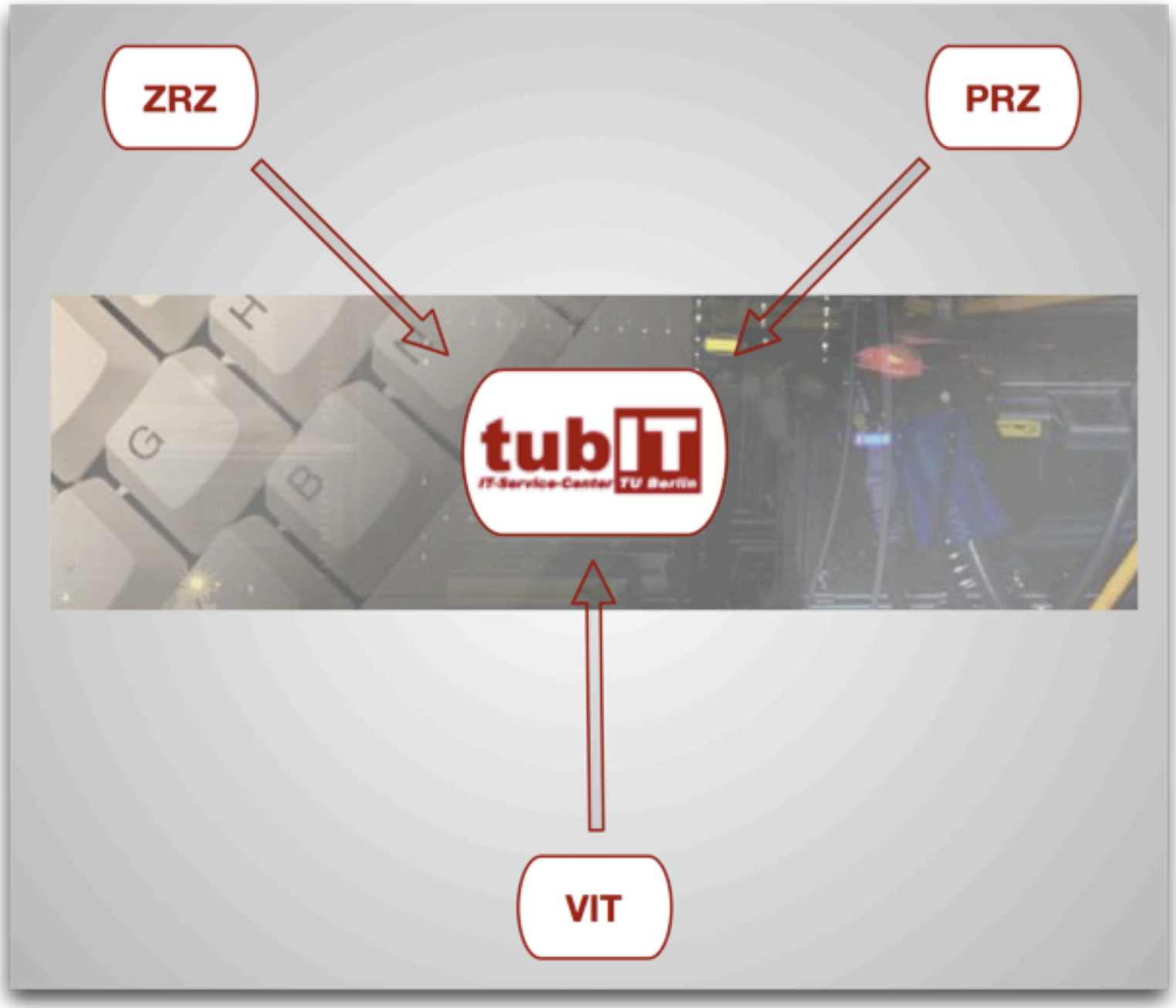
- Vorstellung der Hauptakteure zum Zwecke des Erfahrungsaustauschs, Diskussion und gegenseitiger Unterstützung.

Agenda

- tubIT und Arbeitsgruppe Identity Management
- Das Webportal der TU Berlin (aus Anwendersicht)
- TUBIS - zentrale, verteilte Rollenvewaltung und Metadirectory (aus Technikersicht)
- Verzeichnisdienste (für den AK Verzeichnisdienste)
- Ausblick / Aktuelle Arbeiten
- Zusammenfassung / Kontakte

tubIT
Arbeitsgruppe
Identity Management

Was ist tubIT?



Was ist tubIT?

http://www.tubit.tu-berlin.de/

tubIT: Identitymanagment

- Leiter:
  Christopher Ritter
  (+49 30 314-78614)

- Stellvertreter:
  Thomas Hildmann
  (+49 30 314-23226)

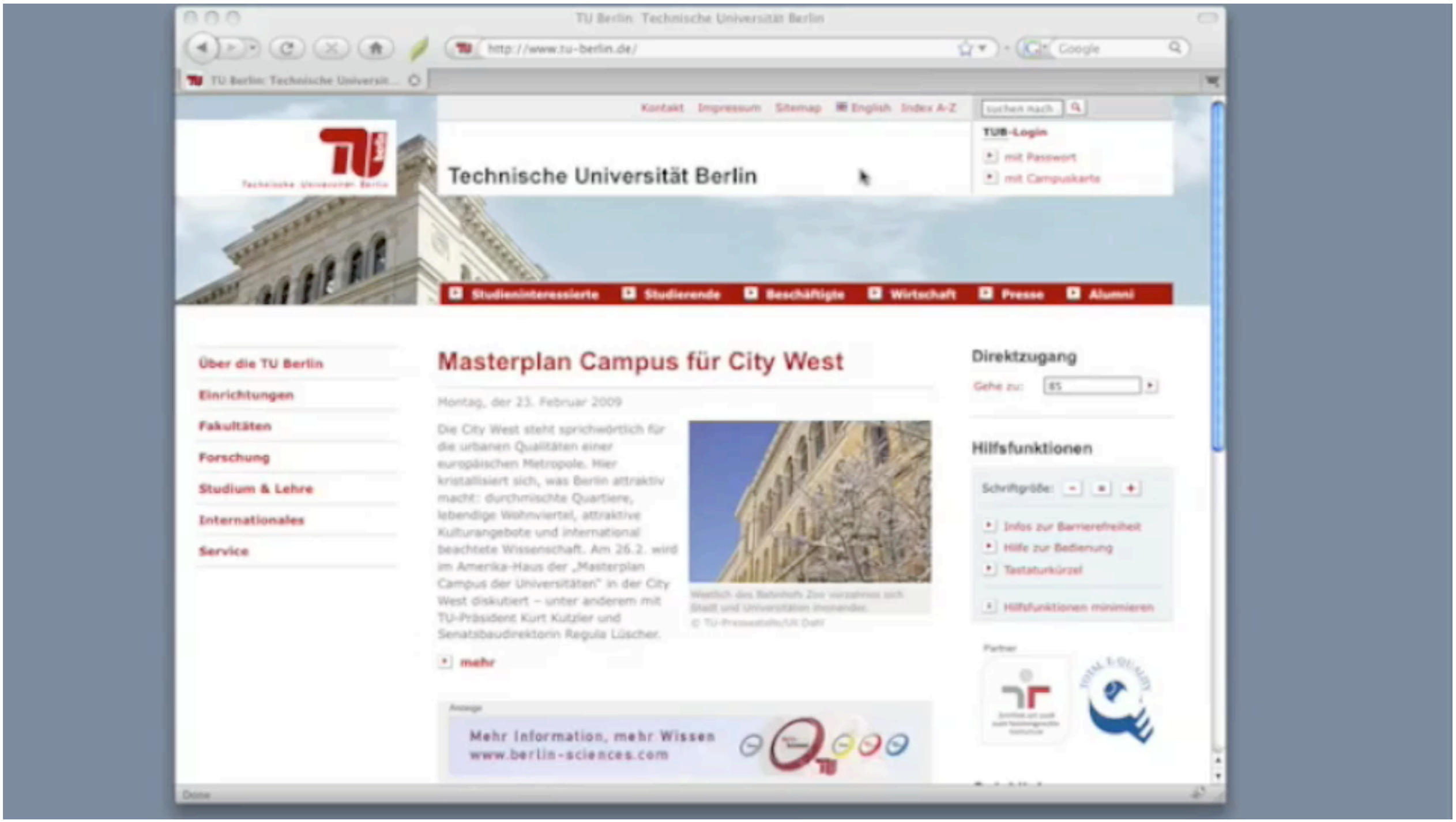
- E-Mail:
  vorname.nachname@tu-berlin.de
  oder
  idm@tubit.tu-berlin.de

- 7 Personen (Festangestellte)
  - Entwicklung
  - Support
  - Tagesgeschäft

- Aufgaben
  - Benutzerverwaltung
  - Verzeichnisdienste (Inhalt)
  - Authentisierung/Autorisierung
  - Anwendungsintegration in das AAI

Das Webportal der TU Berlin und integrierte Anwendungen

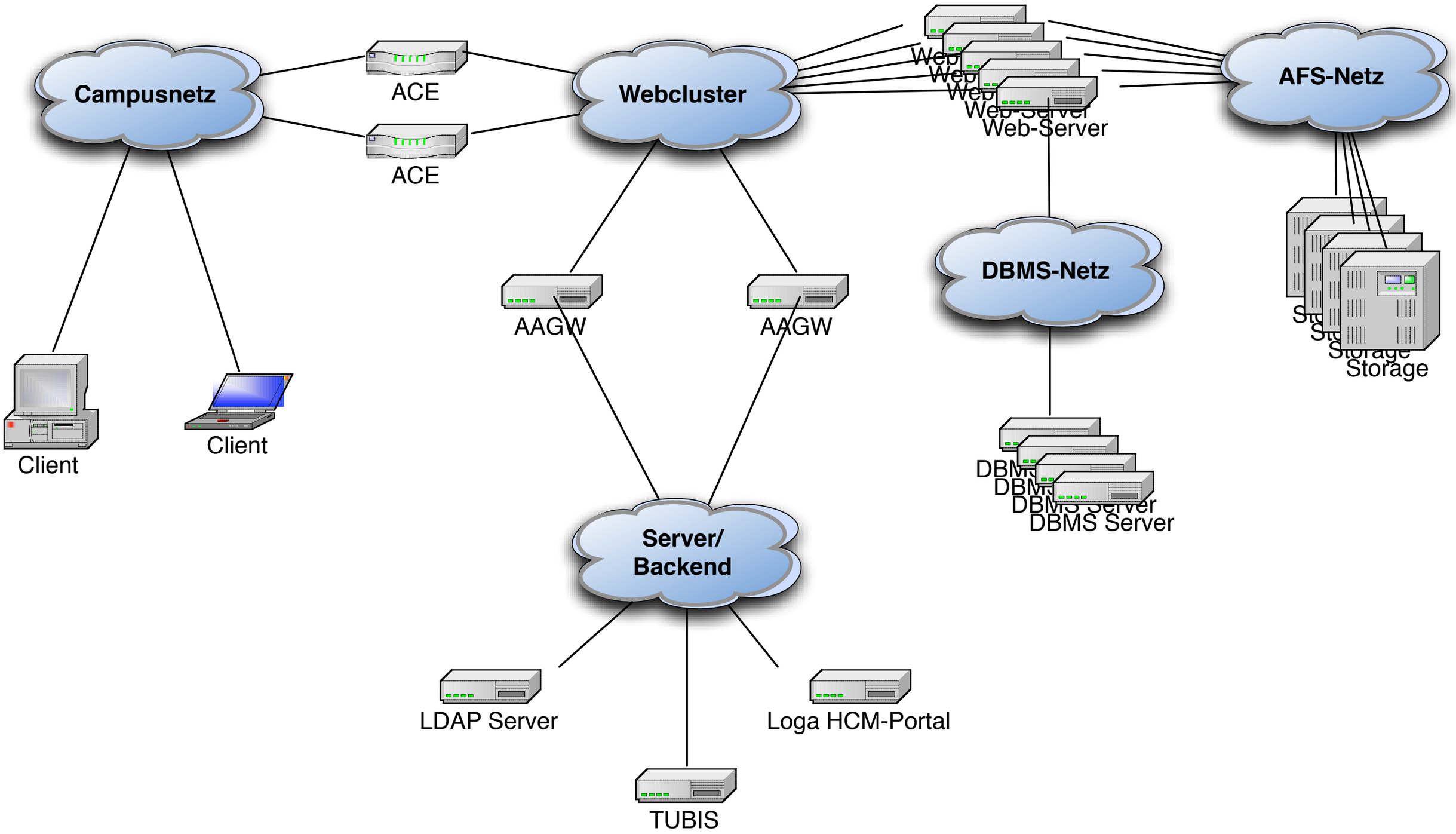
Authentisierung mittels Passwort oder Chipkarte



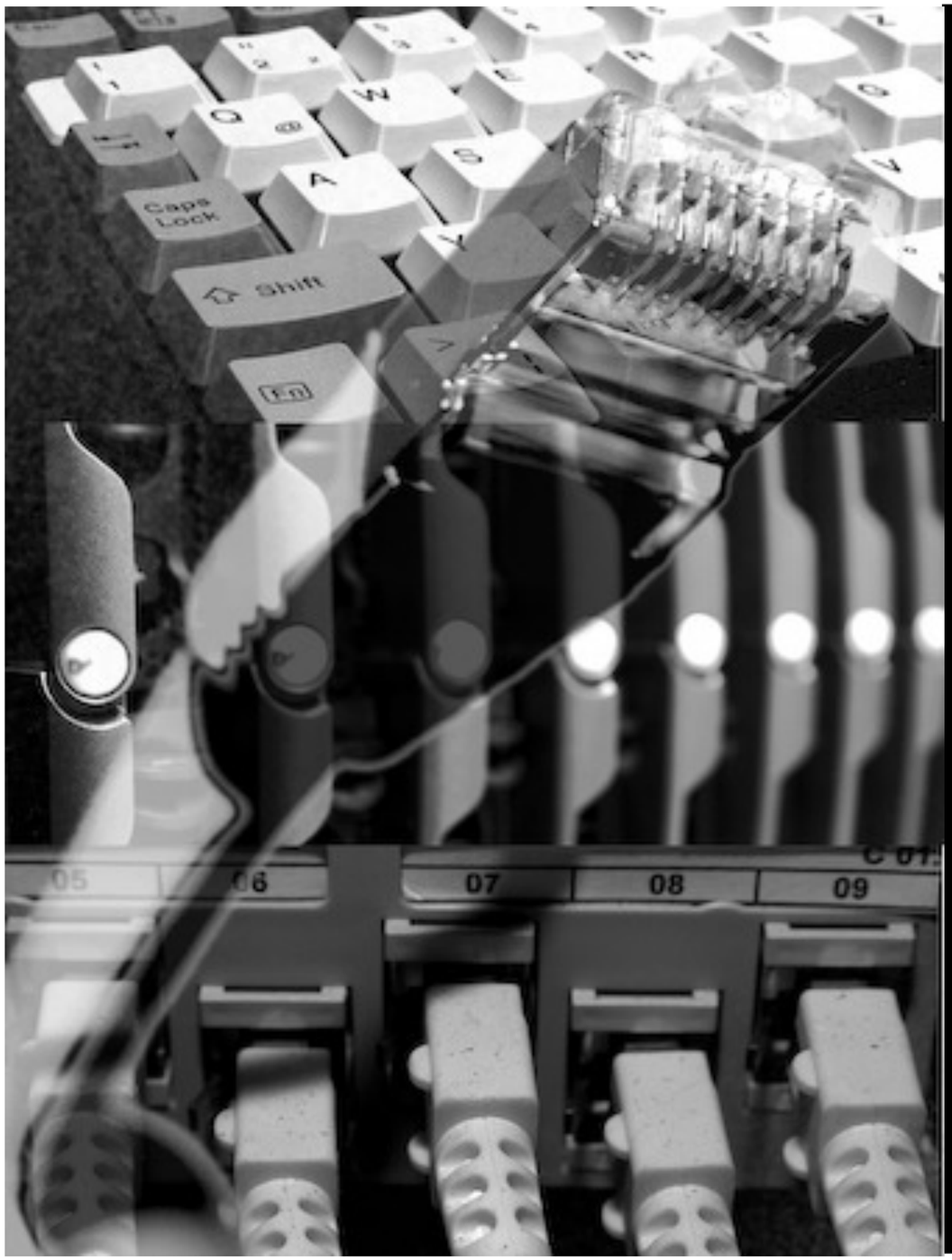
Integrierte Anwendungen

- CMS Typo3 (Webauftritt)
- Loga HCM (Personalverwaltung)
- SuperX (Reportsystem)
- LINF (Leistungsindikatoren in der Forschung)
- QIS/POS (Prüfungsanmeldung)
- asknet-Portal (Software Onlineshop)
- Hardware Onlineshop (TU Eigenentwicklung)
- Online Anträge (z.B. IP, Gäste, Exchangekonten)
- TUBIS Rollenverwaltung
- Schnittstelle zur informationellen Selbstbestimmung
- Selbstverwaltung (Passwörter, TANs etc.)
- weitere in Vorbereitung

Webcluster (vereinfacht)



Technik der Authentisierungs-/ Autorisierungs-Gateways

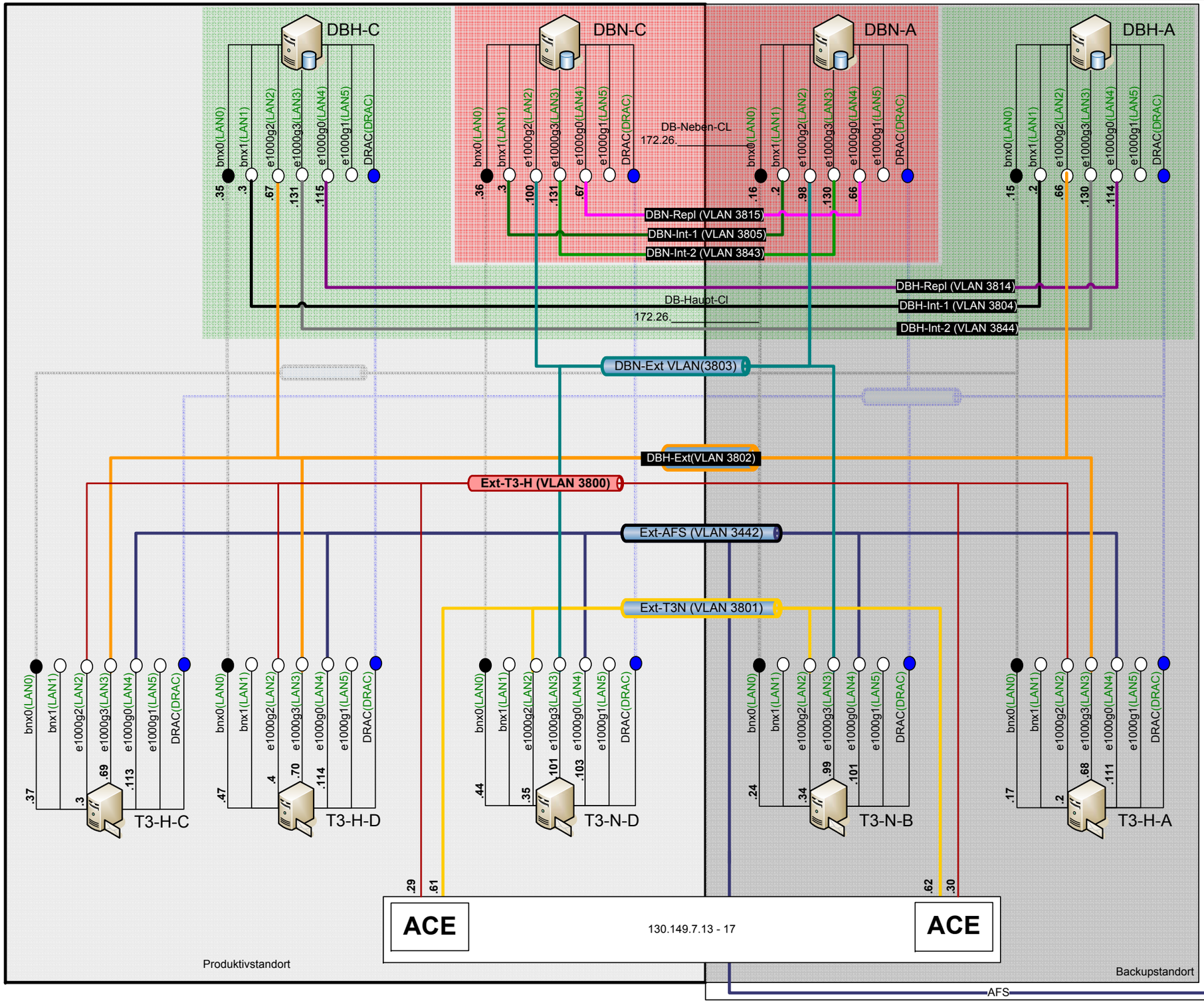


```
aagw2.tubit.tu-berlin.de
Linux Debian 4.0 (Etch)

Dell Blade (Poweredge
1955)
2 DualCore-Xeon a 1,6GHz
3GB Hauptspeicher.

Standort: EN-K033
Rackslot: bs5b6
```

tubIT IT-Service-Center TU Berlin	TITEL: NETZWERKSTRUKTUR TYPO3 / DB CLUSTER			
	BESCHREIBUNG: Netzwerkstruktur des Applikationsclusters in den Teilen Typo3 Haupt und Neben sowie MySQL			
ERSTELLT VON: MICHAEL FLACHSEL	GRÖSSE	FAX-NR.	ZEICHN.NR.: NW T3 / MySQL 1	REV.: 0.5
ÜBERARBEITET AM: 17.06.2008	MASSSTAB: 1:1		BLATT: 1 VON 1	



Netzanfang	Netmask	VLAN
172.26.16.0	255.255.255.224	3800
172.26.16.32	255.255.255.224	3801
172.26.16.64	255.255.255.224	3802
172.26.16.96	255.255.255.224	3803
172.26.23.0	255.255.255.128	3804
172.26.24.0	255.255.255.128	3805
172.26.16.192	255.255.255.240	3806
172.26.16.208	255.255.255.240	3807
172.26.16.224	255.255.255.240	3808
172.26.16.240	255.255.255.240	3809
172.26.17.0	255.255.255.224	3810
172.26.17.32	255.255.255.224	3811
172.26.17.64	255.255.255.192	3812
172.26.17.128	255.255.255.128	3813
172.26.10.0	255.255.254.0	3911
172.26.18.112	255.255.255.240	3814
172.26.18.64	255.255.255.240	3815
172.26.18.80	255.255.255.240	3816
172.26.20.0	255.255.255.128	3839
172.26.20.128	255.255.255.128	3840
172.26.21.0	255.255.255.128	3841
172.26.21.128	255.255.255.128	3842
172.26.23.128	255.255.255.128	3844
172.26.24.128	255.255.255.128	3843
172.26.22.0	255.255.255.128	3845
130.149.205.32	255.255.255.224	3846

- 172.26.8.0/23
- 172.26.10.0/23

http - ACE reicht Ports durch
https - ACE terminiert

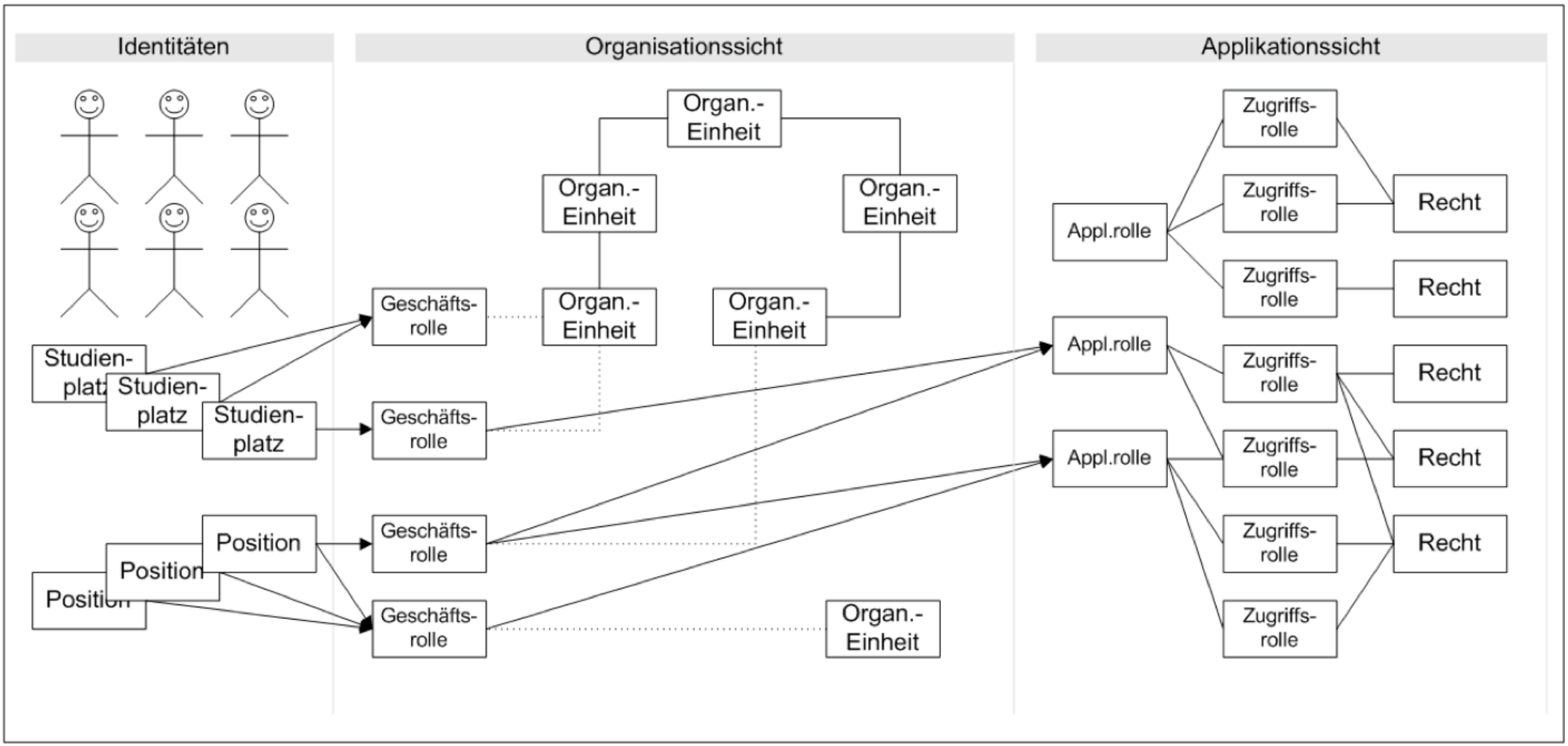
T. Hildmann, C. Ritter AK Verzeichnisdienste, Frühjahr 2009

Durch TUBIS versorgte Dienste, die nicht im Portal sind

- E-Mailkonto
- Radius (ISDN/Modem-Zugang)
- VPN-Zugang
- Windows- / Linux-Account
- AFS-Verzeichnis
- EDUROAM / WLAN
- Exchange

TUBIS
rollenbasiertes Identitätsmanagement und Metadirectory

TUBIS-Modell



Rollenverwaltung

TUBIS-Rollenverwaltung: Zentrales IT-Dienstleistungszentrum der Technischen Universität Berlin (tubIT)
Ihre Rolle: Verwalter TU-Berlin

Organisationseinheit auswählen

Organisationseinheiten

○ 1 Ebene anzeigen ◉ 2 Ebenen anzeigen ○ 3 Ebenen anzeigen

☐ Geschlossene Organisationseinheiten anzeigen

Organisationseinheiten neu aufbauen

47 Zentrales IT-Dienstleistungszentrum der Technischen Universität B ...
4700 Zentrales IT-Dienstleistungszentrum der Technischen Universität ...
47001100 IT-Service-Center TU Berlin (tubIT)
47008100 tubIT-Laden

Selektierte Organisationseinheit auswählen | Eine Ebene höher | Übersicht

Informationen der ausgewählten Organisationseinheit

Name:	Zentrales IT-Dienstleistungszentrum der Technischen Universität Berlin (tubIT)
Kostenstelle:	47
Status:	aktiv
Kategorie:	Zentraleinrichtung
Genehmigte Kurzbezeichnung (OrgName):	tubit
Beantragte Kurzbezeichnung:	tubit
Beschreibung:	Zentrales IT-Dienstleistungszentrum der Technischen Universität Berlin (tubIT)
Adresse:	EN 50 Einsteinufer 17, 10587 Berlin
Telefon:	22703
Fax:	21060
E-mail:	tubit@tu-berlin.de
Homepage:	www.tubit.tu-berlin.de
Rollenverwalter:	Herr Klaus Nagel, Tel: 314-25786

Rollenverwaltung

TUBIS-Rollenverwaltung: IT-Service-Center TU Berlin (tubIT)
Ihre Rolle: Verwalter TU-Berlin

Organisationseinheit auswählen : Organisationseinheit verwalten : Geschäftsrollen-Übersicht

Alle Geschäftsrollen dieser Organisationseinheit

Bestell Tester
DNS-Administrator
DNS-Verwalter
Gast-Verwalter
Leiter/in Bereich - 47001100 (n.v.)
Mitarbeiter/in Zentraleinrichtung - 47001100
Modulverwalter/in
PERS_Büroleitung - 47001100 (nicht delegierbar)
POS Tester
Prüfer/in
PW-Verwalter
t3admin
TUBIS-Master
tubIT-Anwendungsverwalter
tuBV-Verwalter
Typo3 Antrag
Typo3 Chefredakteur
Typo3 Entwickler
Typo3 Redakteur
Typo3 Verwalter

n.v.: (nicht vergeben) - Dieser Rolle wurden noch keine Positionen zugewiesen

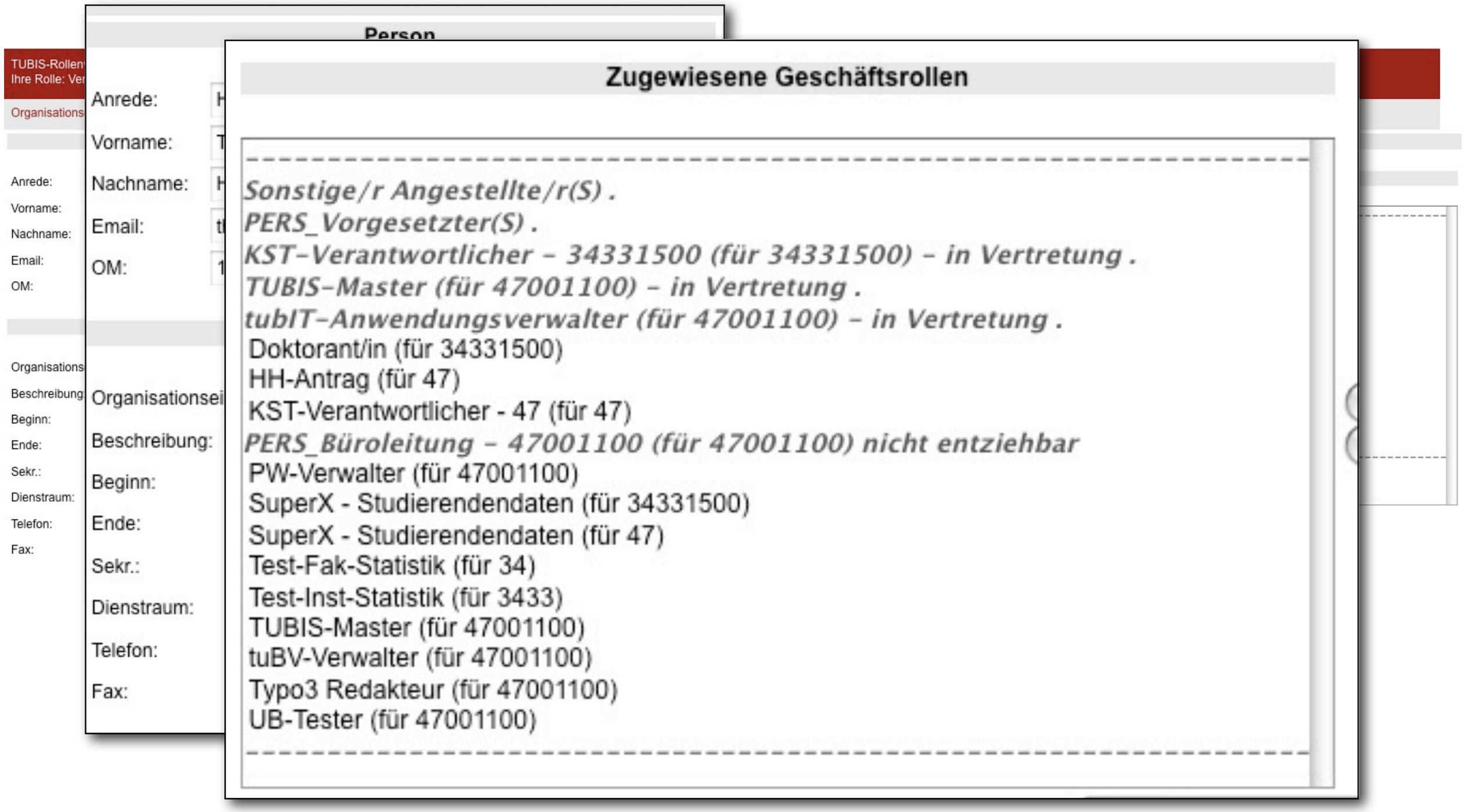
Geschäftsrolle bearbeiten
Geschäftsrolle entfernen
Geschäftsrolle hinzufügen
Mitglieder anzeigen

Mitglieder der ausgewählten Geschäftsrolle

Gehrcke, Hans-Christian Sonstige Angestellte (47001100)
Schmidt, Martin Handw./Facharbeiter/in (47001100)
Kwiatkowski, Manfred Sonstige Angestellte (47001100)
Rieger, Timo Ang. i.d. Maschinenbedienung (Maschinensaal) (47001100)
Nagel, Klaus Wissenschaftliche/r Angestellte/r (47001100)
Gebhardt, Thomas Sonstige Angestellte (47001100)

Mitglied bearbeiten

Rollenverwaltung



Herausstellungsmerkmale

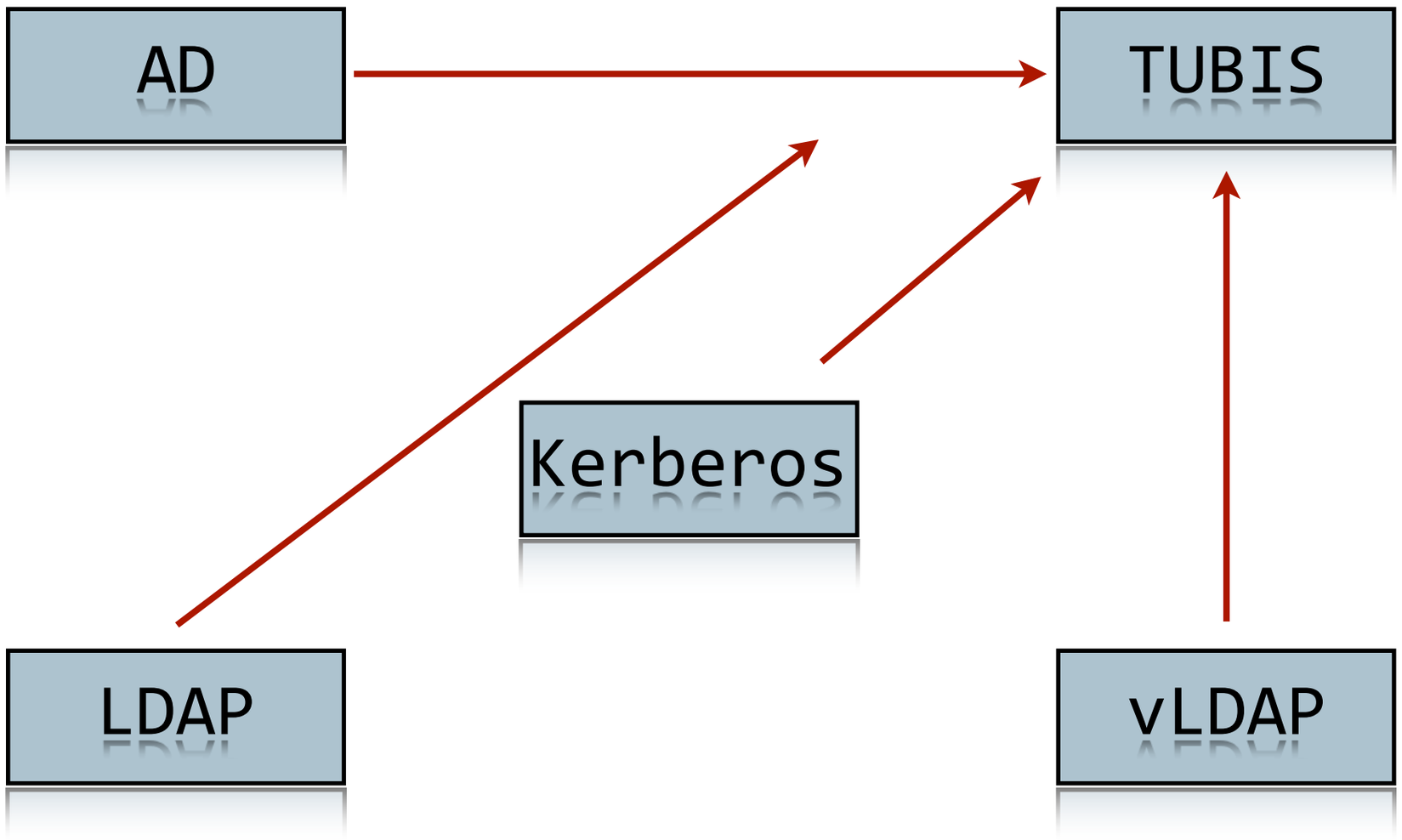
- Drei Typen von Rollen
  - Geschäftsrollen
  - Anwendungsrollen
  - Zugriffsrollen
- Gewaltenteilung auf Modellebene (Sichten)
  - Web-GUI massgeschneidert
  - vollständige Integration ins Webportal
- Unterstützung versch. Authentisierungsmethoden
- Vier Varianten der Rollenzuweisung
  - Standardrollen (automatisch)
  - Strukturverwaltung (dynamische Rollen)
  - Vertretungen / Delegation
  - Teambildung
- Unterstützung von Push- und Pull-Architekturen
- Umfassende Nutzung (viele Dienste)

Benutzte Werkzeuge

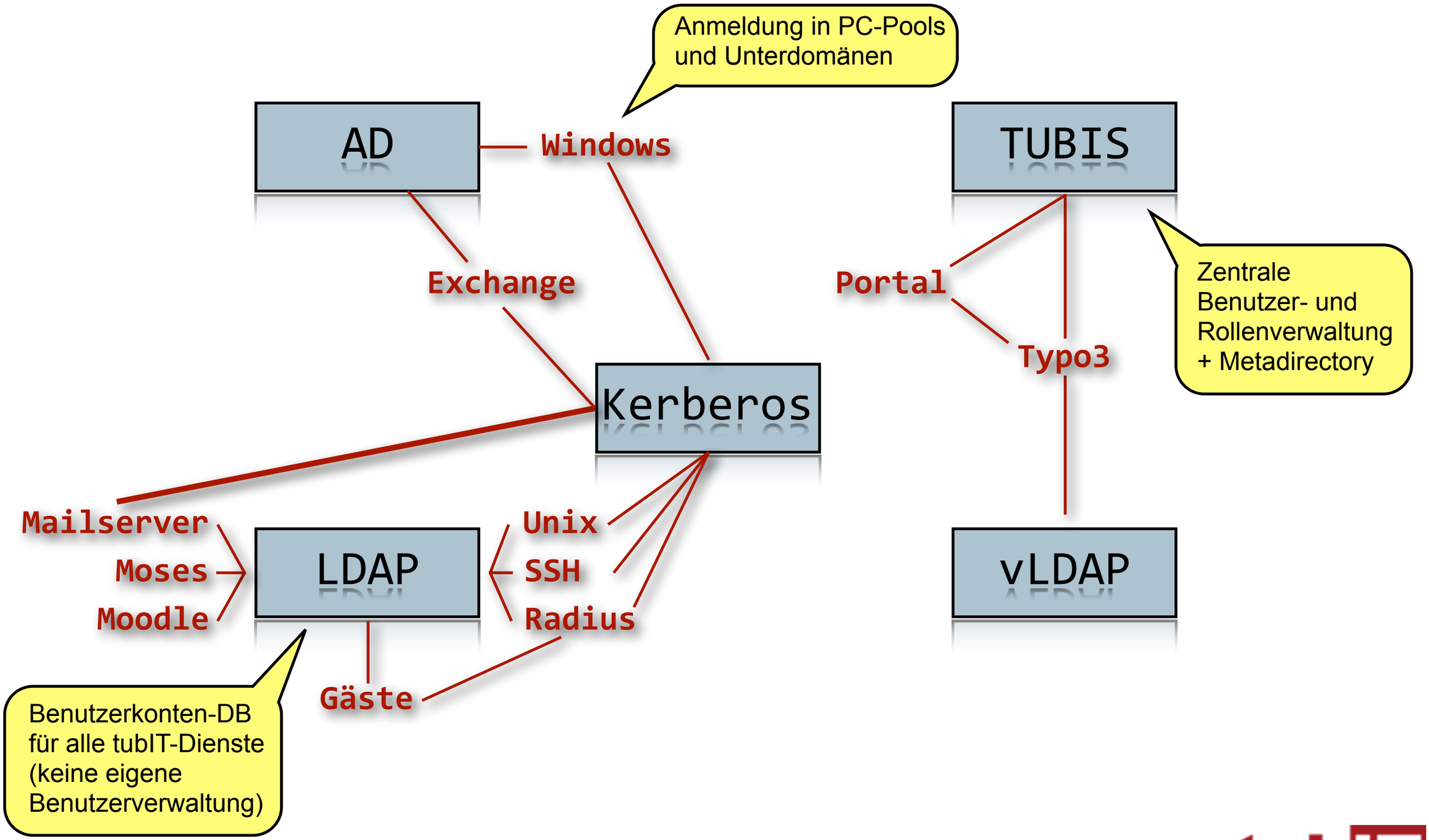
- Entwicklungsumgebung
  - Java / JEE
  - (My)Eclipse
  - Subversion / CVS
  - JPox
- Applicationserver
  - Tomcat
  - Jetty
  - Glasfish
- Scriptsprachen (Glue)
  - Perl
  - Python
  - PHP
- Datenanbindung (Glue)
  - Sequoia
  - Penrose
- Ticketsystem / Support
  - OTRS
- Dokumentation
  - Wordpress
  - OmniGraffle / Visio
  - div. Textverarbeitungen
  - Freemind
- DBMS (relational)
  - PostgreSQL
  - MySQL
- Verzeichnisdienste
  - OpenLDAP
  - ActiveDirectory
  - MIT Kerberos
- PKI
  - OpenSSL
  - Charismatics Middleware
- Webserver / Contentmanagement
  - Apache (mod_rewrite, mod_*)
  - Typo3

Verzeichnisdienste an der TU Berlin

“Benutzt”-Hierarchie unter den Verzeichnissen

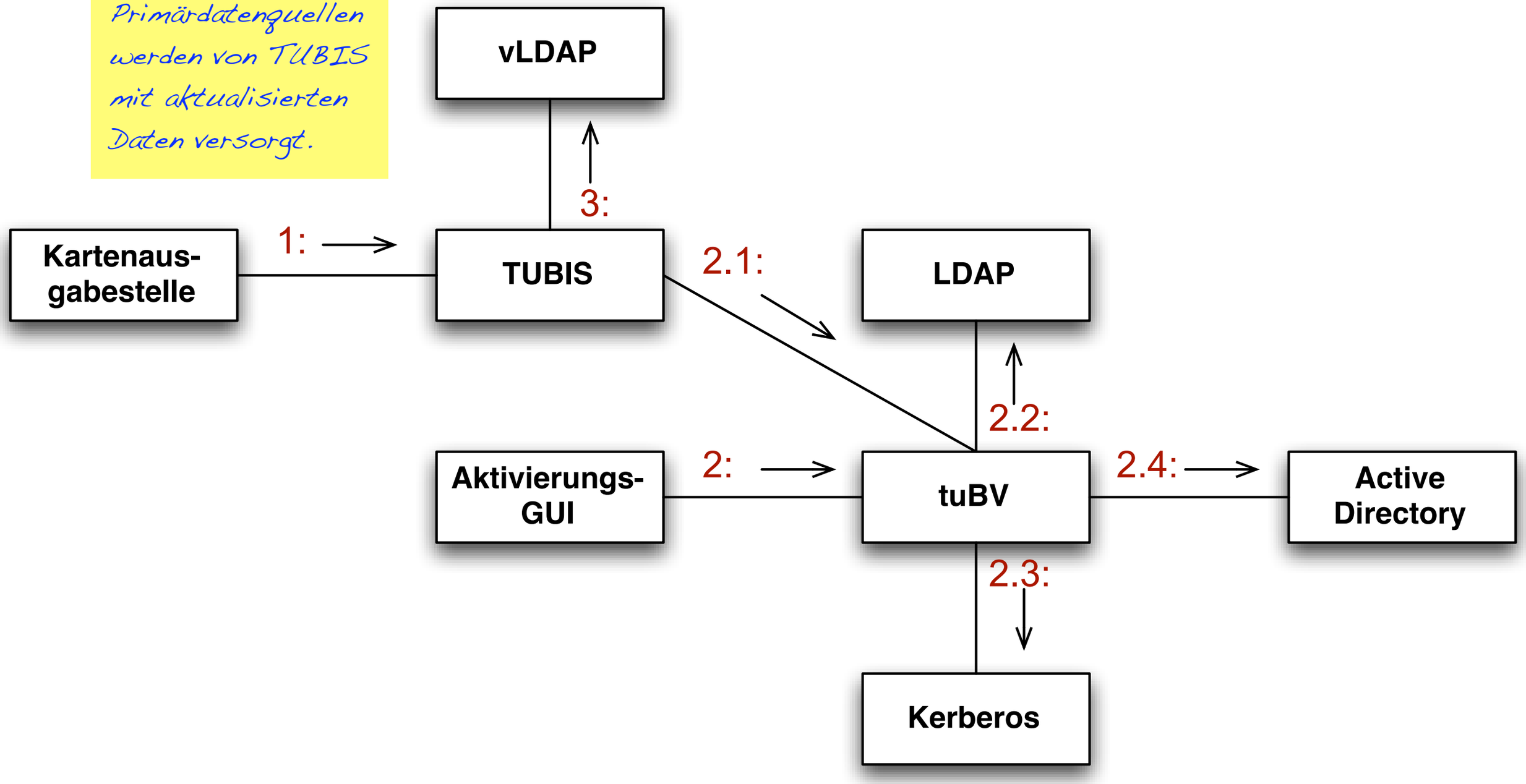


Verzeichnisdienste



Datenfluss: Verzeichnisdienste

Primärdatenquellen werden von TUBIS mit aktualisierten Daten versorgt.

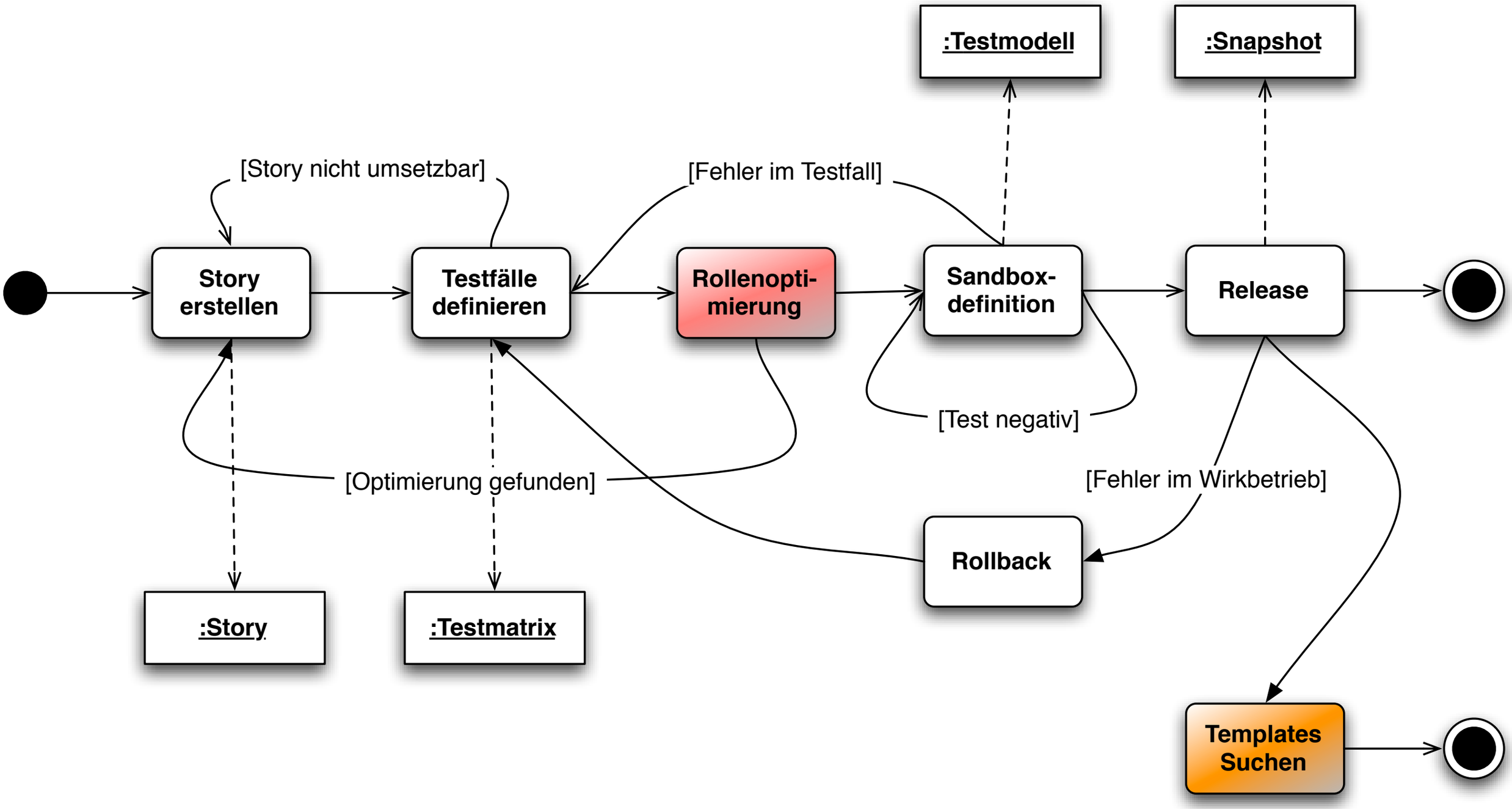


Ausblick:
TUBISx, XRE und Shibboleth

Merkmale der nächsten Version

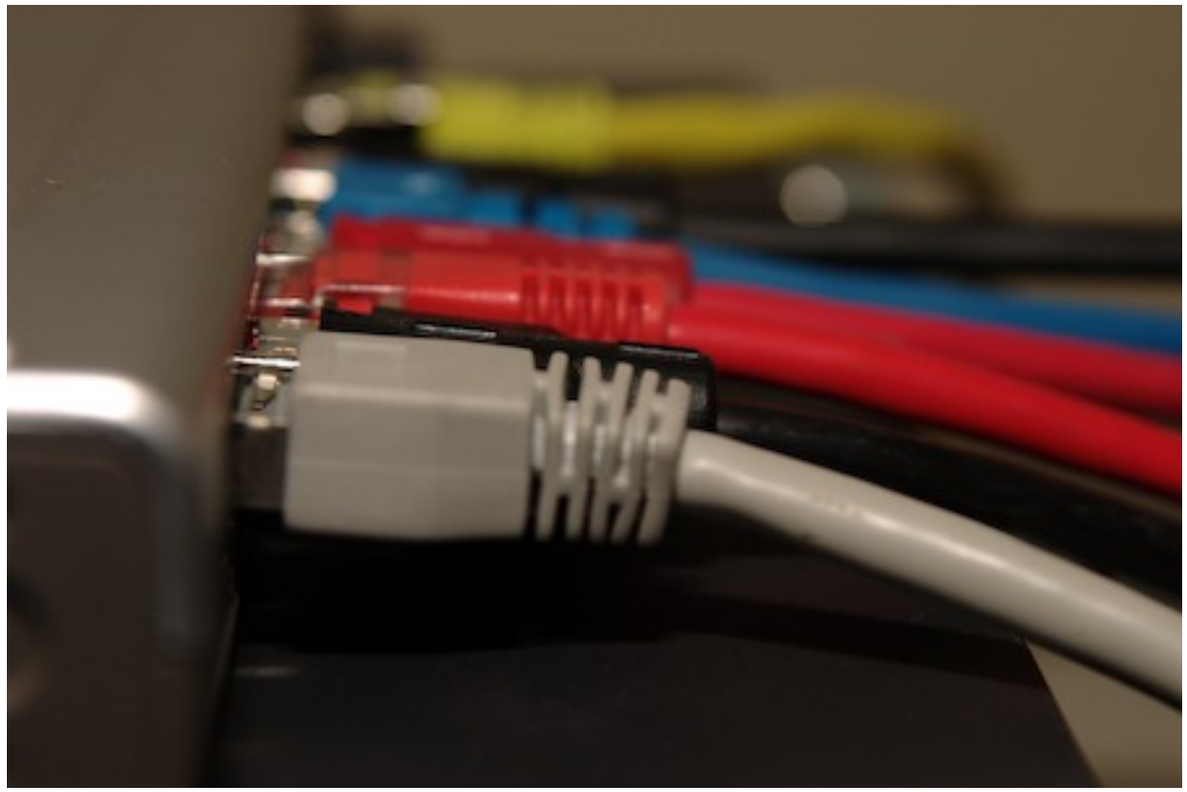
- Existierendes Datenmodell
- Neue Architektur
- Erweiterung der Pull- und Push-Dienste für Verzeichnisse
- Ereignissteuerung (zeitlich, Objektänderung, etc.)
- Neue Benutzungsschnittstelle (Webelemente können in Typo3 genutzt werden, Python-Interface für Scripte)
- Erstes RBAC-System mit xRE-Unterstützung

eXtreme Role Engineering



Shibboleth

- Zur Zeit Testföderation beim DFN
- Aufbau einer Standardinstallation
- Es folgt dann Einbindung in die TUBIS-Sphäre



Zusammenfassung
und
Kontaktdaten

Zusammenfassung

- **Identitätsmanagement an der TU Berlin**
  - Derzeit werden etwa 35000 Identitäten verwaltet.
  - IdM/RBAC-System für alle Dienste
  - Metadirectory für Daten der Universitätsverwaltung

- **Aktuelle Arbeiten**
  - eXtreme Role Engineering
  - TUBISx basierend auf JEE mit Pull- und Push-Architektur
  - Anbindung an Shibboleth
  - Optimierung verschiedener organisatorischer Abläufe

http://www.tubit.tu-berlin.de/

Christopher.Ritter@tu-berlin.de

Thomas.Hildmann@tu-berlin.de

Vielen Dank für die
Aufmerksamkeit!

Fragen, Anmerkungen