

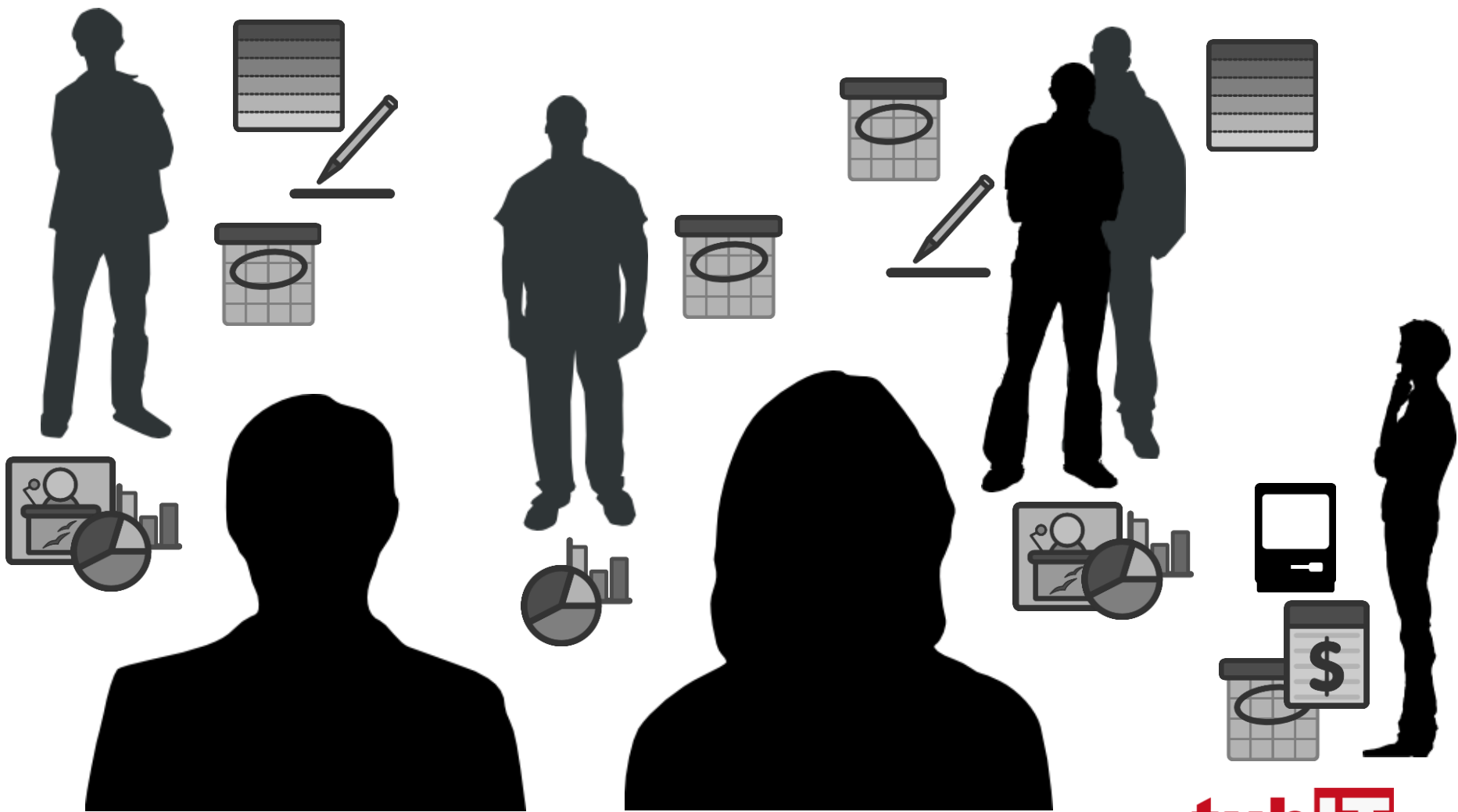
Identity management for the TUB Cloud

T. Hildmann, O. Kao, C. Ritter | tubIT, CIT | EUNIS 2013

Agenda

The path of the TU Berlin towards integrated service provisioning:

- Provisioning: Entering the Cloud
- Role-Management: Authorization
- IDM & TUB Cloud: Technology
- Cloud-Storage: ownCloud @ TU Berlin
- Summary: Lessons learned



Entering the Cloud

Provisioning



E5001564

Technische Universität Berlin



TU Berlin, tubIT IT-Service-Center, Sekr.: E-N 50, Einsteinufer 17, D-10587 Berlin

E-Mail: tubis@tubit.tu-berlin.de / Tel: (030) 314 - 28000

Ms
Erika Mustermann
16905001564
EN 50

tubIT-Account setup for external members to use IT services of the
TU Berlin




Organisational ID : 16905001564



TU smart card (student's version)



activating the account

User Administration ACCOUNT ACTIVATION   

tubIT Account Activation: Login

With your tubIT account you can use many tubIT services, such as WLAN access, online disk, PC pool, E-mail and much more. Within the scope of account activation you will be prompted to choose a name and a password for your account.

Please enter your organisational ID into the following form. You find it on the printout you got for your provisioning or on your Campus Card - it starts with "1690".
As a student you can also enter your matriculation number into the input field "Organisational ID"

You find the initial password in the printout you got for your provisioning.

Organisational ID:

Initial password:

E-mail contact: tubit@tu-berlin.de Page rendered: 11/Jun/2013, 11:12:28 A

provisioning for ...

staff members

- covering letter with employment
- campus smartcard = staff member identity card

students

- covering letter with matriculation
- optionally card with or without chip, TAN list, mTAN

external members of TU Berlin

- extra-professional lecturer, graduate student studying for a doctorate without employment, foundationer, ...
- user account without smart card (with exceptions)

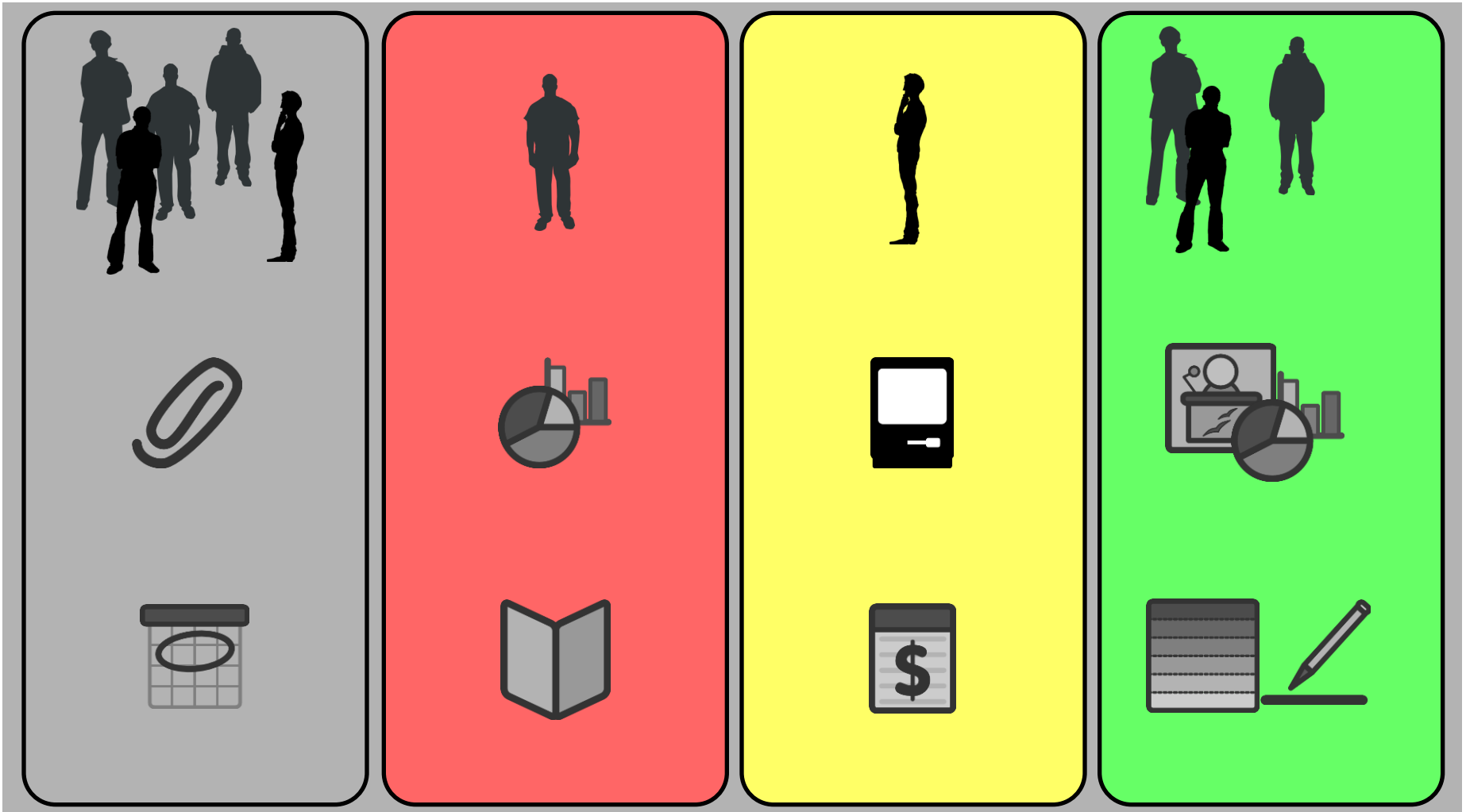
guests

- pseudonymous accounts for WiFi-usage only
- no access to personalized TU portal

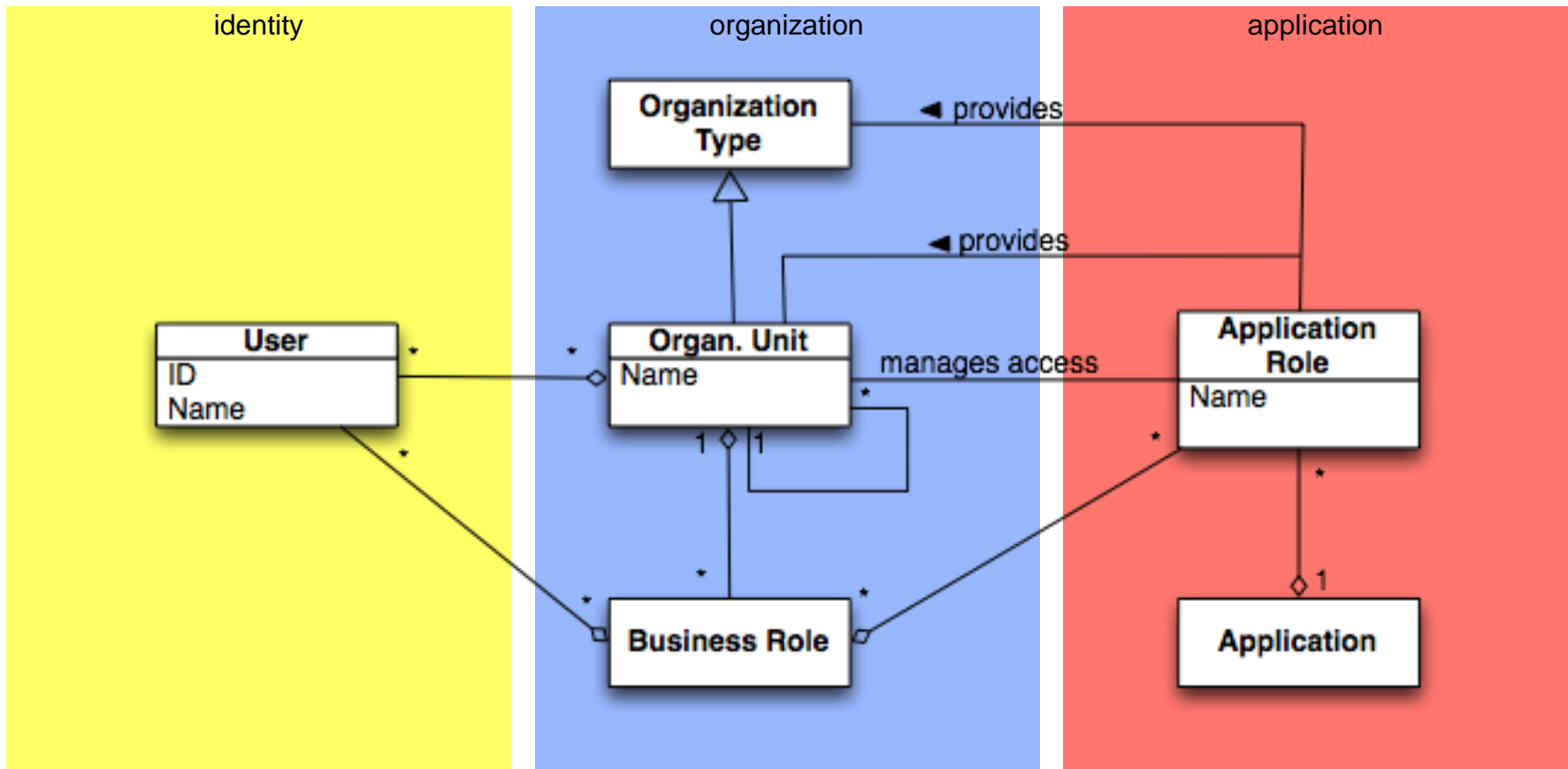
Authorization

Role-management

Roles, Permissions and Members



three layer rbac-model



Person

Zugewiesene Geschäftsrollen

Sonstige/r Angestellte/r(S) .

PERS_Vorgesetzter(S) .

KST-Verantwortlicher - 34331500 (für 34331500) - in Vertretung .

TUBIS-Master (für 47001100) - in Vertretung .

tubIT-Anwendungsverwalter (für 47001100) - in Vertretung .

Doktorant/in (für 34331500)

HH-Antrag (für 47)

KST-Verantwortlicher - 47 (für 47)

PERS_Büroleitung - 47001100 (für 47001100) nicht entziehbar

PW-Verwalter (für 47001100)

SuperX - Studierendendaten (für 34331500)

SuperX - Studierendendaten (für 47)

Test-Fak-Statistik (für 34)

Test-Inst-Statistik (für 3433)

TUBIS-Master (für 47001100)

tuBV-Verwalter (für 47001100)

Typo3 Redakteur (für 47001100)

UB-Tester (für 47001100)

TUBIS-Rollen
Ihre Rolle: Ve
Organisations

Anrede:
Vorname:
Nachname:
Email:
OM:

Organisations
Beschreibung
Beginn:
Ende:
Skr.:
Dienstrraum:
Telefon:
Fax:

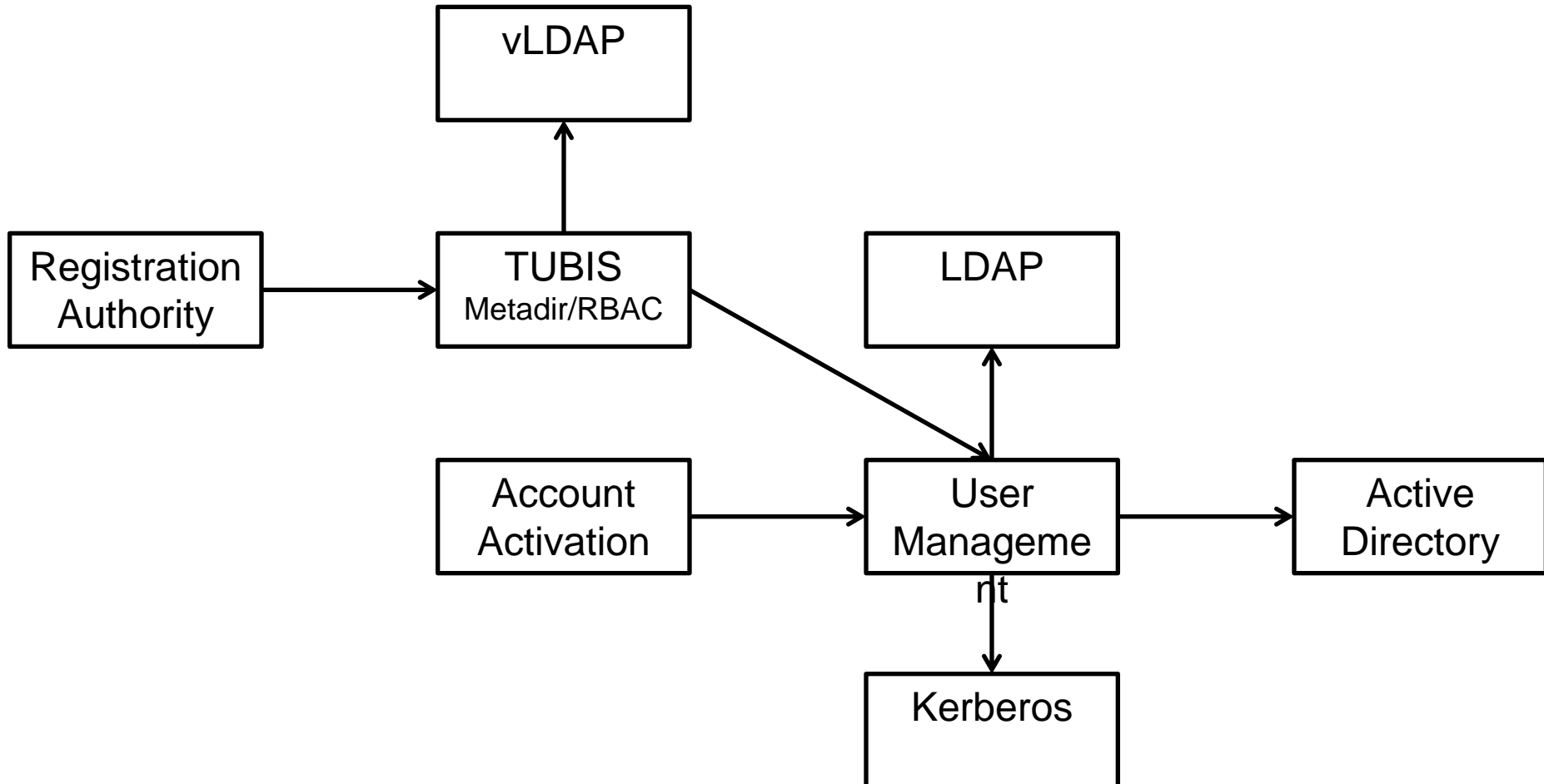
Anrede:
Vorname:
Nachname:
Email:
OM:

Organisationsel
Beschreibung:
Beginn:
Ende:
Skr.:
Dienstrraum:
Telefon:
Fax:

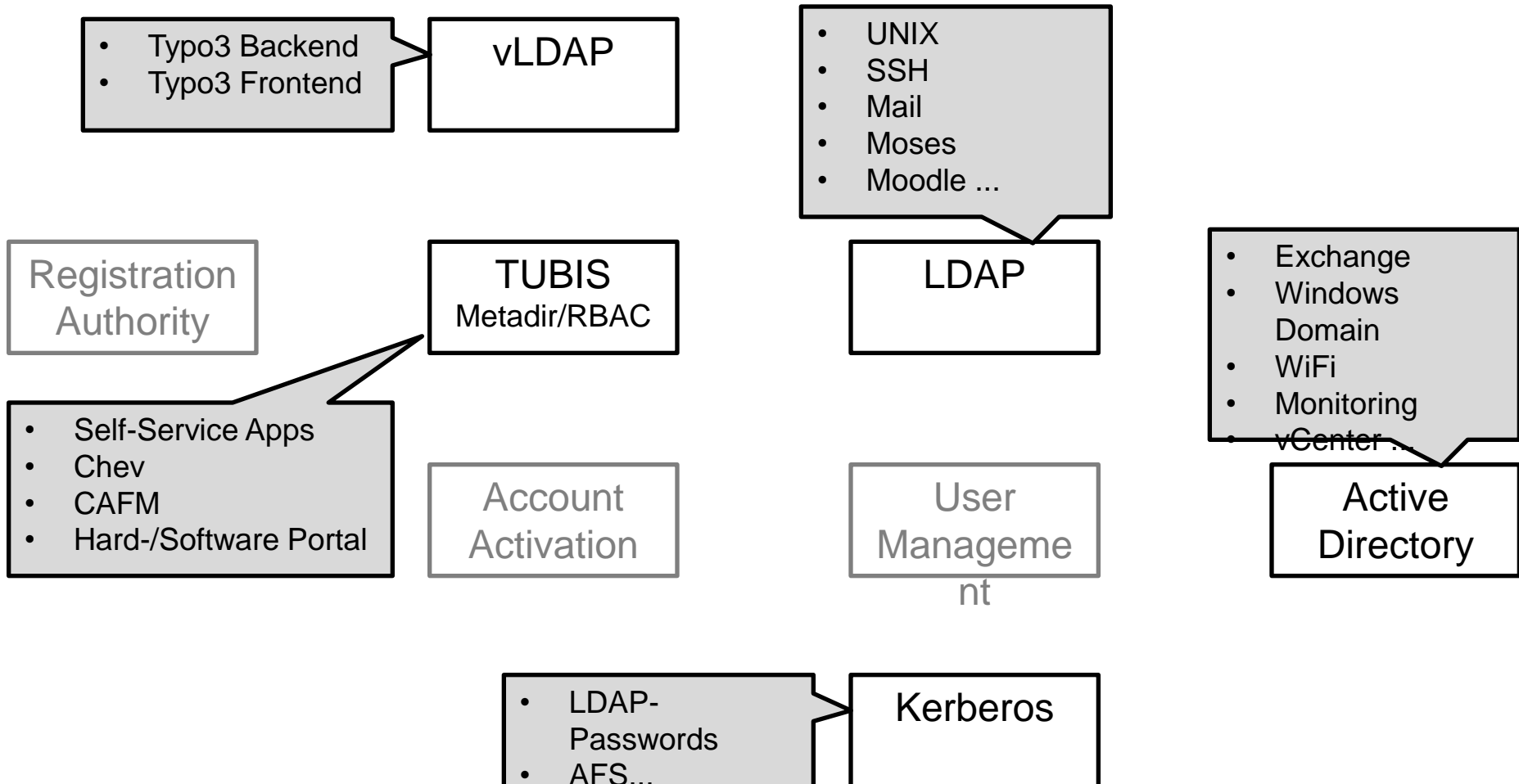
Technology

IDM & tub cloud

data-flow: directory services



usage: directory services



Public & Private Cloud

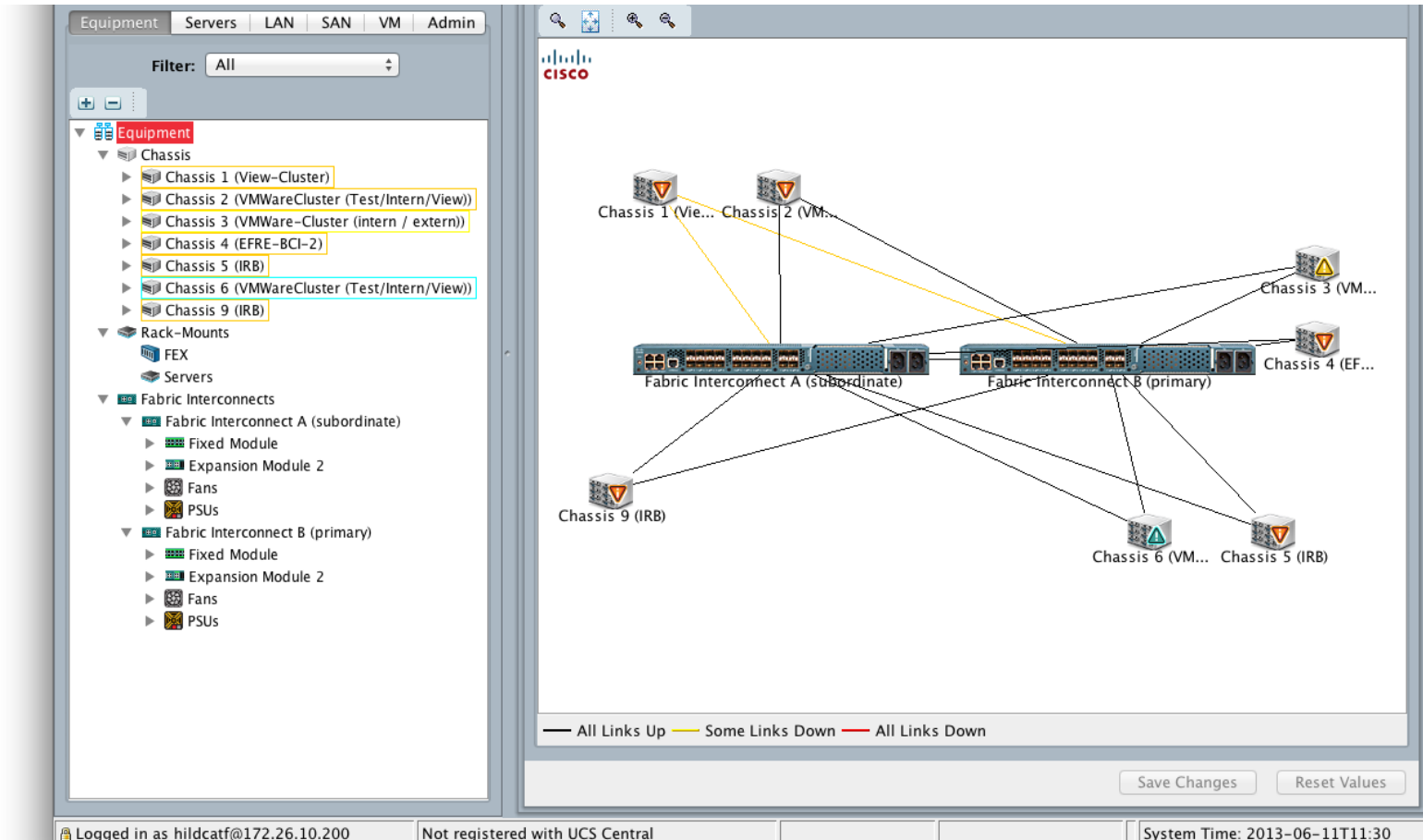
Private Cloud

- based on VMware ESXi and View
- all central services (including IDM) running on private cloud
 - mail / exchange
 - typo3 cms
 - storage (AFS / ownCloud)
 - campus-management and administration application
 - self-services
- role-based access to services for university members
 - automatically
 - delegated

Public Cloud

- based on Zimory
- user authentication based on LDAP
- prototype for RBAC-integration available

UCS technology (“hardware virtualization”)



Hardware - basic

1 UCS Chassis

8 x UCS B200 M1 Blades „half-Size“

- 2x QC Xeon 5540 2.53 GHz
- 48 GB RAM
- No HDD – „boot from SAN“
- 1 Qlogic DualPort CNA

2 x UCS 6120XP

- Incl. 8 Port FC-Expansion Card

VMWare VSphere 4.0 license



Hardware-Expansion

2010:

2 chassis

2011:

2 chassis

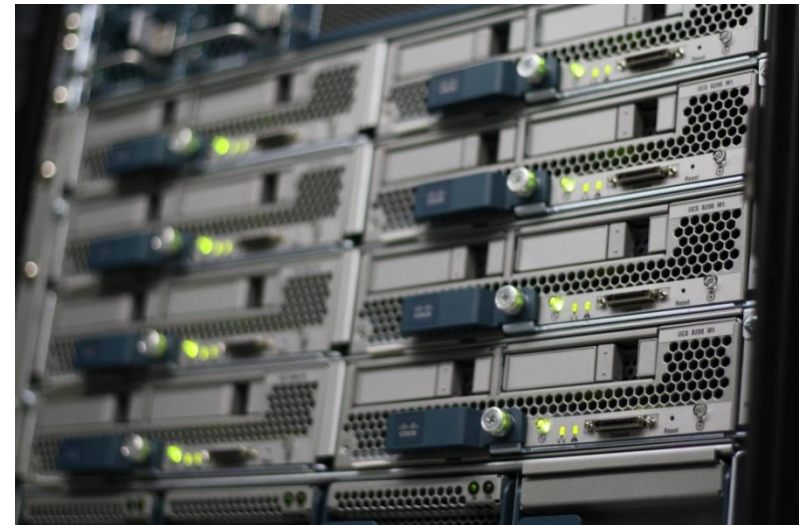
2 fabric inter connects

backup data-center

vSphere 5

2012:

2 chassis



resources for private cloud

Produktiv-Cluster

CPU	256 Cores, 602 GHz
RAM	2,9 TB
SAN	170 TB
Hosts	15
VMs	255

Test-Cluster

CPU	40 Cores, 79 GHz
RAM	384 GB
SAN	32 TB
Hosts	2
VMs	103

Public & Private Cloud

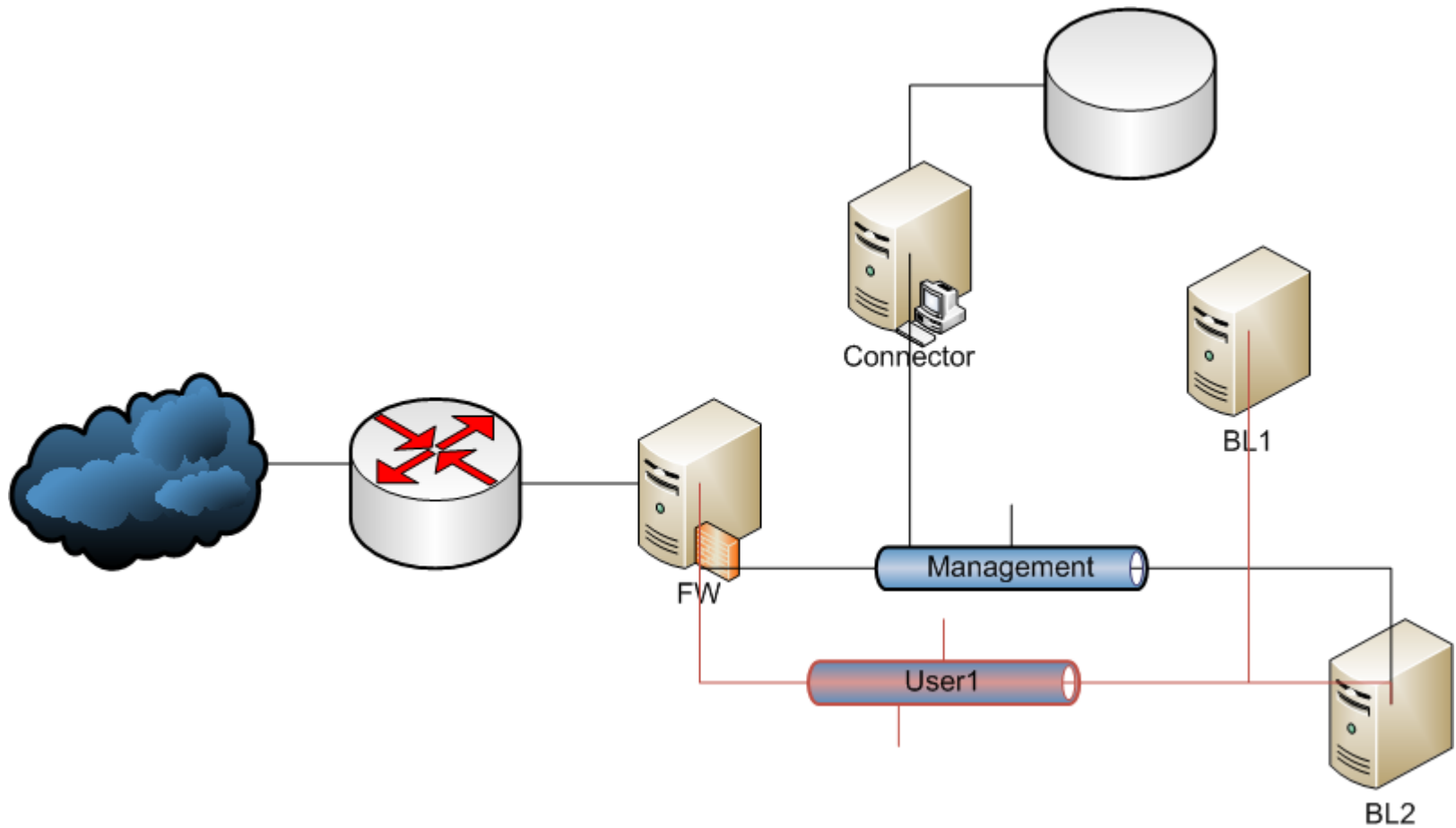
Private Cloud

- based on VMware ESXi and View
- all central services (including IDM) running on private cloud
 - mail / exchange
 - typo3 cms
 - storage (AFS / ownCloud)
 - campus-management and administration application
 - self-services
- role-based access to services for university members
 - automatically
 - delegated

Public Cloud

- based on Zimory
- user authentication based on LDAP
- prototype for RBAC-integration available

BCI / Zimory



ownCloud @ TU Berlin

Cloud-Storage

storage and sharing @ TUB

central storage: Andrew File System (AFS)

- Quota
 - personal (1 GB for students, 5 GB for staff)
 - for organizational units (250 GB)
 - extensible in 1 TB steps
- access via
 - AFS-client (Windows, MacOS X, Linux, ...)
 - WebAFS
 - SFTP via SSH gateway
 - <http://www.user.tu-berlin.de/<nutzernamen>>
 - *Subversion (SVN)*

Sharing: GigaMove using DFN-AAI (shibboleth)

growing number



Server: very good usability via AFS client module



PC/Mac: usability depends on OS system and connectivity



Laptop: some issues with client, alternative: WebAFS



Tablet: WebAFS only. Bad integration!

shrinking usability

ownCloud @ TUB

quota

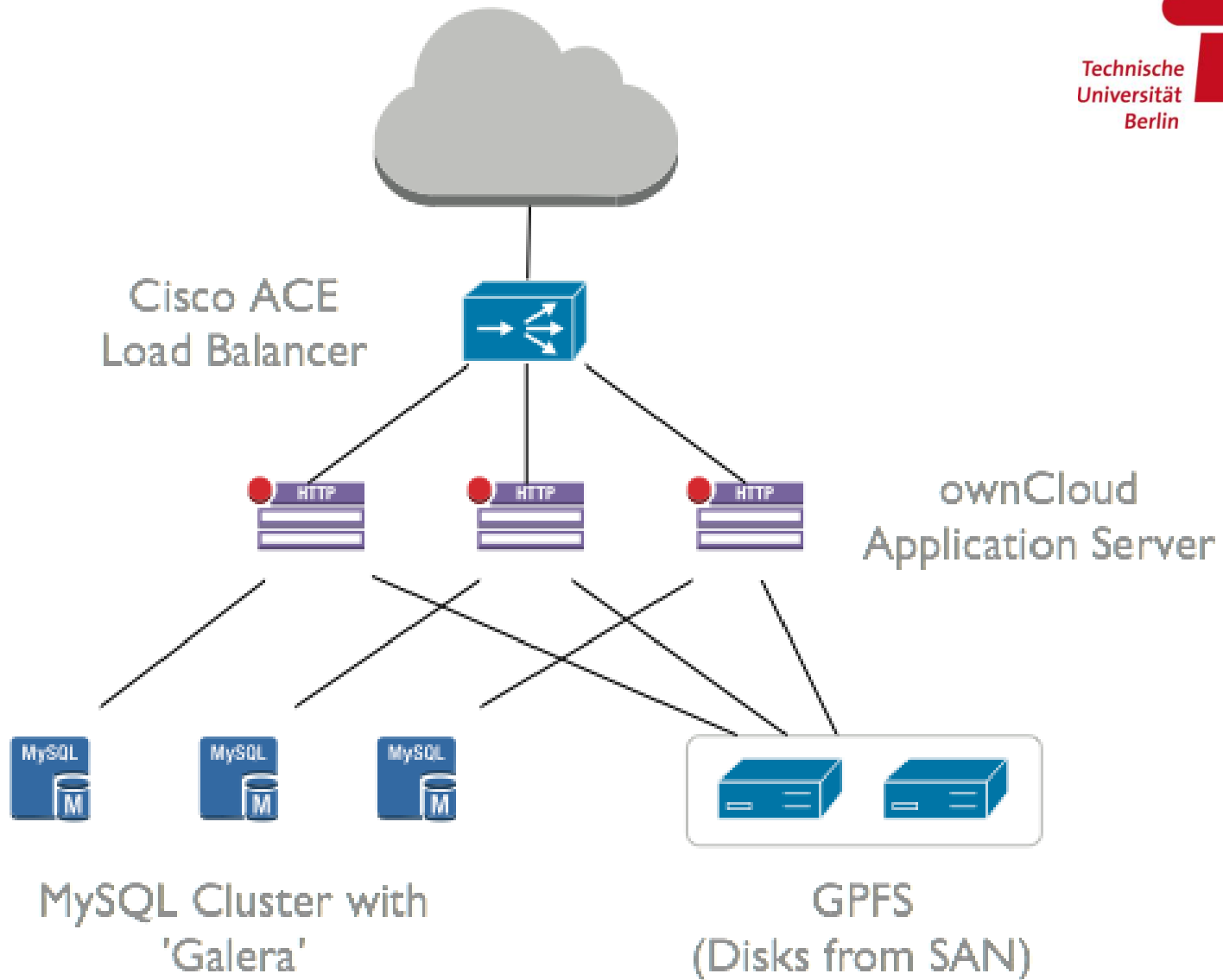
- students 10 GB
- staff members 50 GB
- organizational units will follow

accessibility

- WebDAV for stationary devices
- Sync-Client for Laptops and PCs in remote networks
- iOS / Android-Apps for Smartphones and Tablets
- Web-GUI for independent access from everywhere

share

- sharing of files and folders including corporate work
- simply using e-mail addresses TU Berlin der TU Berlin



Summary

- workflows integrate user provisioning - accounts for all university members
- RBAC based authorization using self-service user interfaces
- IDM pulls data from primary sources and pushes to directory services
- three separated clouds
 - public cloud (user's virtual machines)
 - private cloud (services provided for users and administration)
 - storage cloud (roll-out in March 2013, not mentioned in paper)
- mobile devices raise the need for cloud services
- increasing integration in external cloud services needed