

Identitätsmanagement für Hybrid-Cloud-Umgebungen an Hochschulen

Erfahrungen im Münchner Wissenschaftsnetz

Silvia Knittl, Wolfgang Hommel
{knittl,hommel}@mnm-team.org

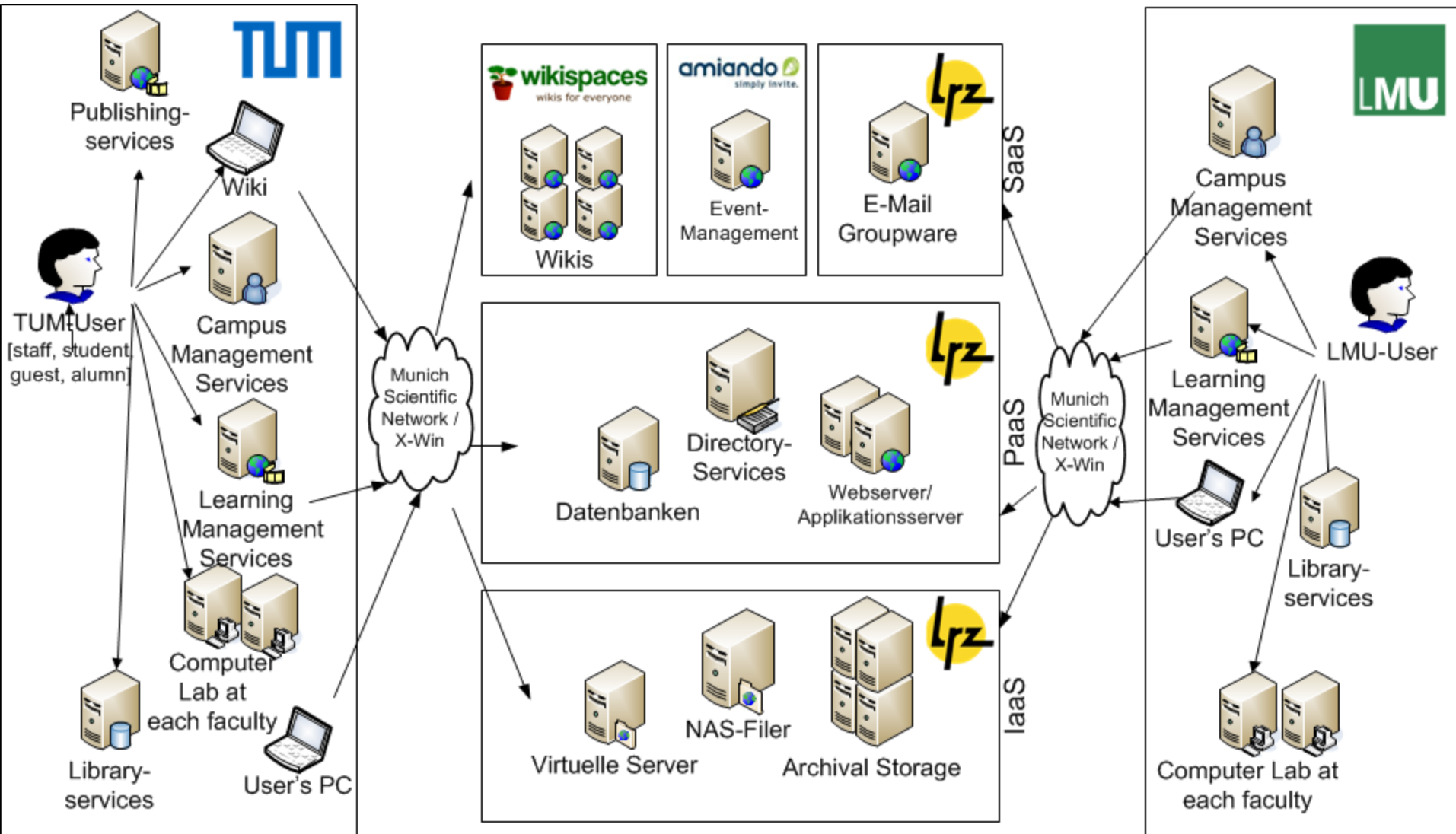
- Hybrid Cloud im Münchner Wissenschaftsnetz (MWN)
- Identity & Access Management (IAM) im MWN
 - IAM für normale User-Accounts
 - IAM für administrative User-Accounts
- Zusammenfassung, Ausblick

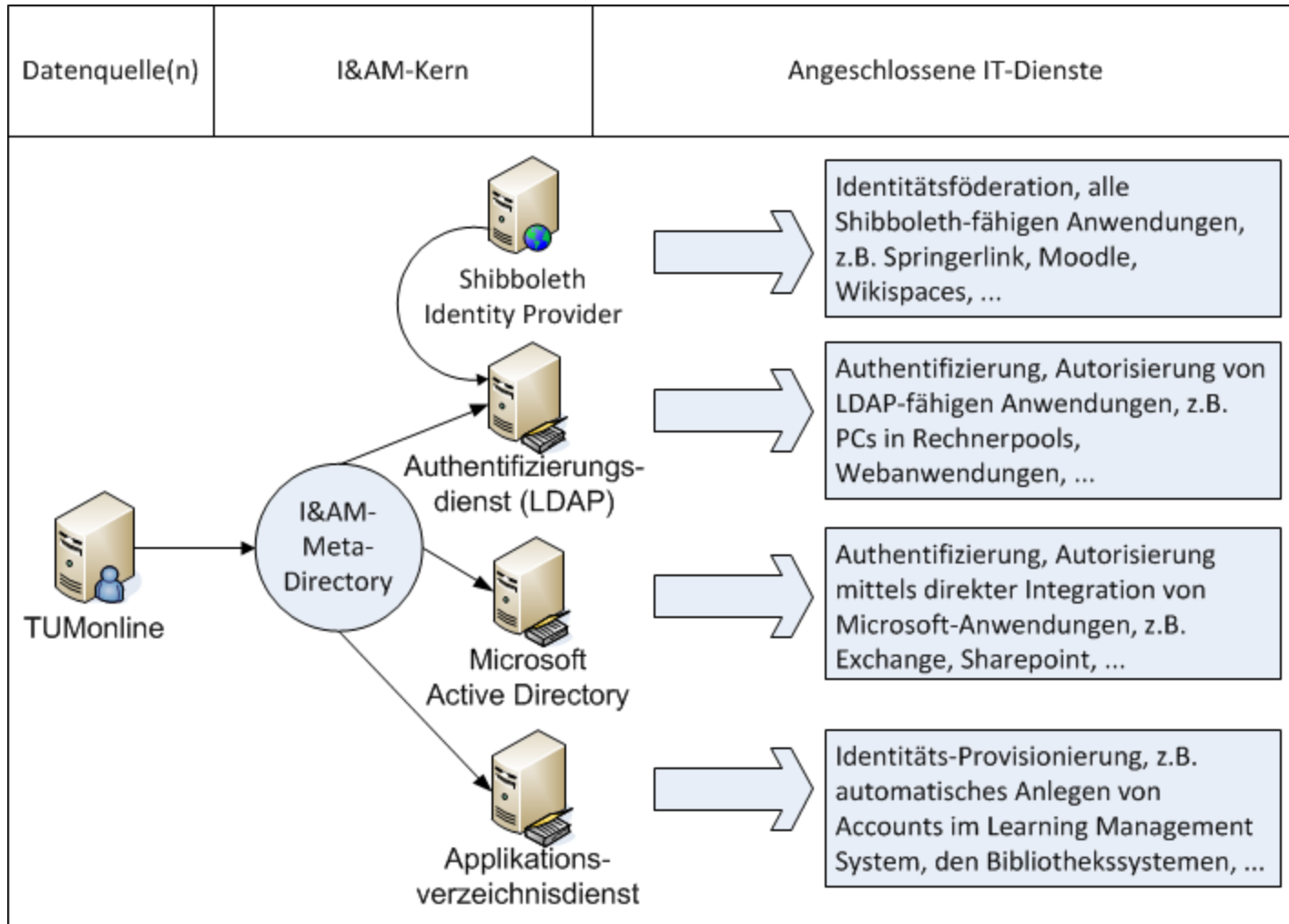
- Einzige TU in Bayern
- 3 Standorte mit je lokaler Verwaltung
- 13 Fakultäten
- 26.302 Studenten
- 461 Professoren
- 5.564 akademische, 3.032 nicht akademische Angestellte [2011]

- TUM- Standorte
- Wissenschaftsnetzwerke

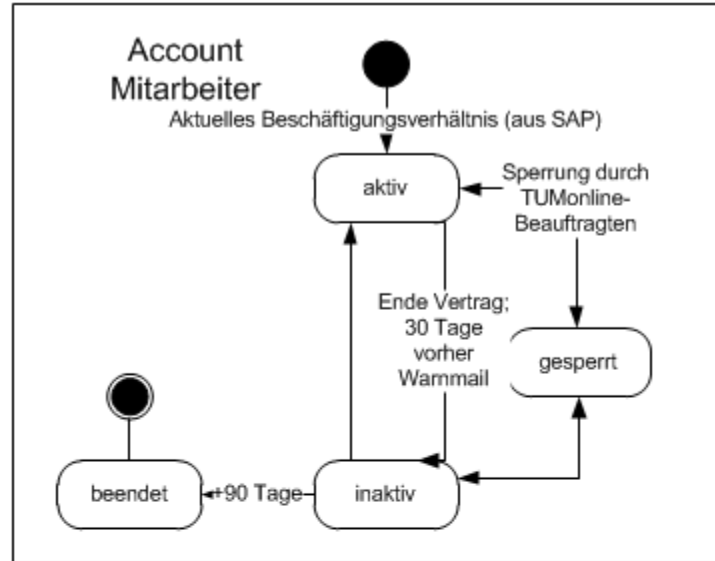


ENISA (11/09)	ENISA (04/10), CSA, NIST	Bitkom
Software, Platform und Infrastructure as Service (SaaS), (PaaS), (IaaS)		
Merkmale: <ul style="list-style-type: none"> - fast sofortige Skalierbarkeit - Flexibilität und Bereitstellung - gemeinsam genutzte Ressourcen - „on demand“ meist mit „pay as you go“ - Nutzung über Internet 		
Public: verfügbar für jede Organisation		
Private: Zugriff nur innerhalb eines privaten Netzes	Private: Cloud Infrastruktur wird für einzelne Organisation betrieben	Private/ Enterprise Cloud: unternehmenseigene, vom Unternehmen selbst betriebene Umgebung; Zugriff i.d.R via Intranet (VPN)
	Community: Infrastruktur wird von versch. Organisationen geteilt	Hybrid: Nutzungskombinationen von Private/Public Clouds und traditioneller IT-Umgebung
Partner: wohldefinierte Anzahl Kunden	Hybrid: Cloud Infrastruktur besteht aus obigen Clouds	

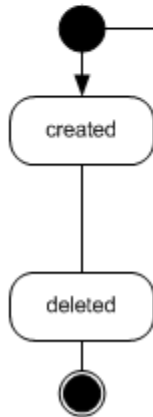




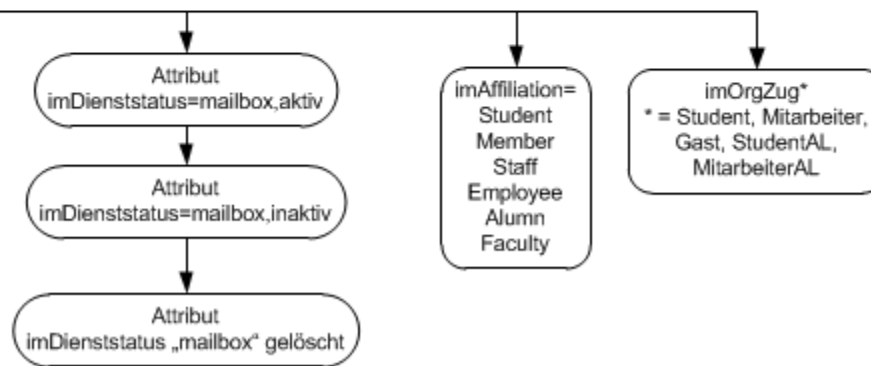
Campus Management System
TUMonline



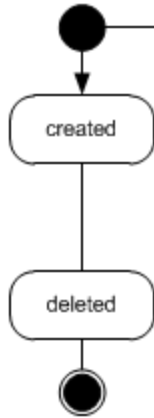
TUM-Verzeichnisse
(vereinfachte Darstellung)



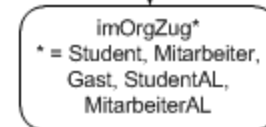
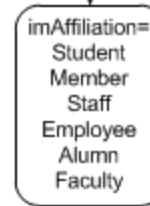
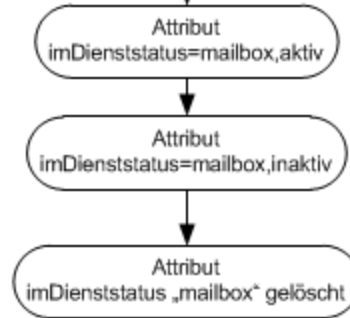
Lebenszyklus Objekt vom
Typ Person



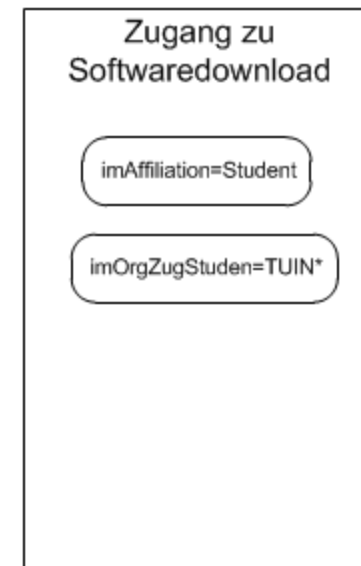
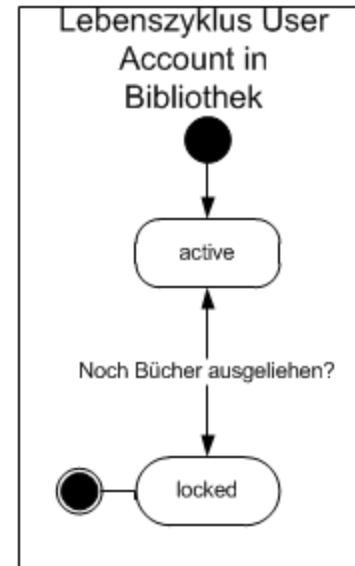
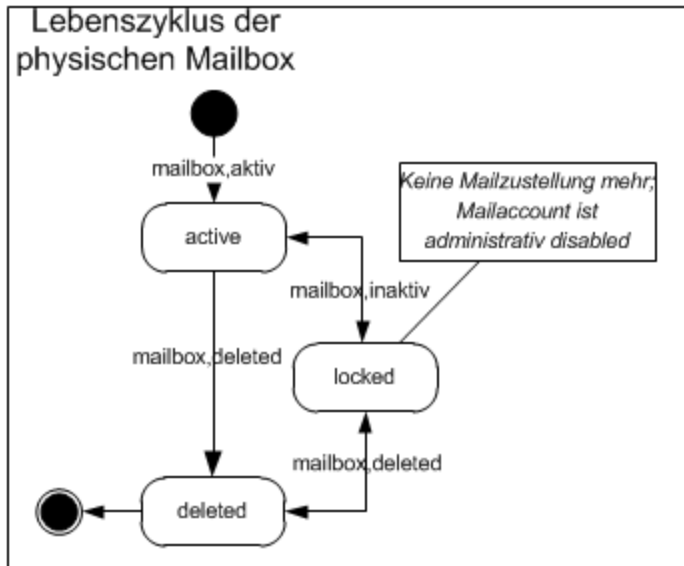
TUM-Verzeichnisse
(vereinfachte Darstellung)



Lebenszyklus Objekt vom
Typ Person



Dienstebene



- Identitätsmanagement normaler User-Accounts
 - Intern: Anbindung an IAM-Komponenten
 - Extern: Föderiertes IAM (Shibboleth)
 - Provisionierung, direkte Integration in AA Infrastruktur
 - User-Lebenszyklus über Rollen/Attribute
 - Student -> Alumni, Mitarbeiter -> Alumni, Guest

- Herausforderungen:
 - Hohe natürliche Fluktuation
 - Kürzere Studienzeiten bei Bachelor/Master
 - Befristete Beschäftigungsverhältnisse
[http://www.his.de/presse/news/ganze_pm?pm_nr=816]

1. IS YOUR USE OF PRIVILEGED ACCOUNTS MONITORED?

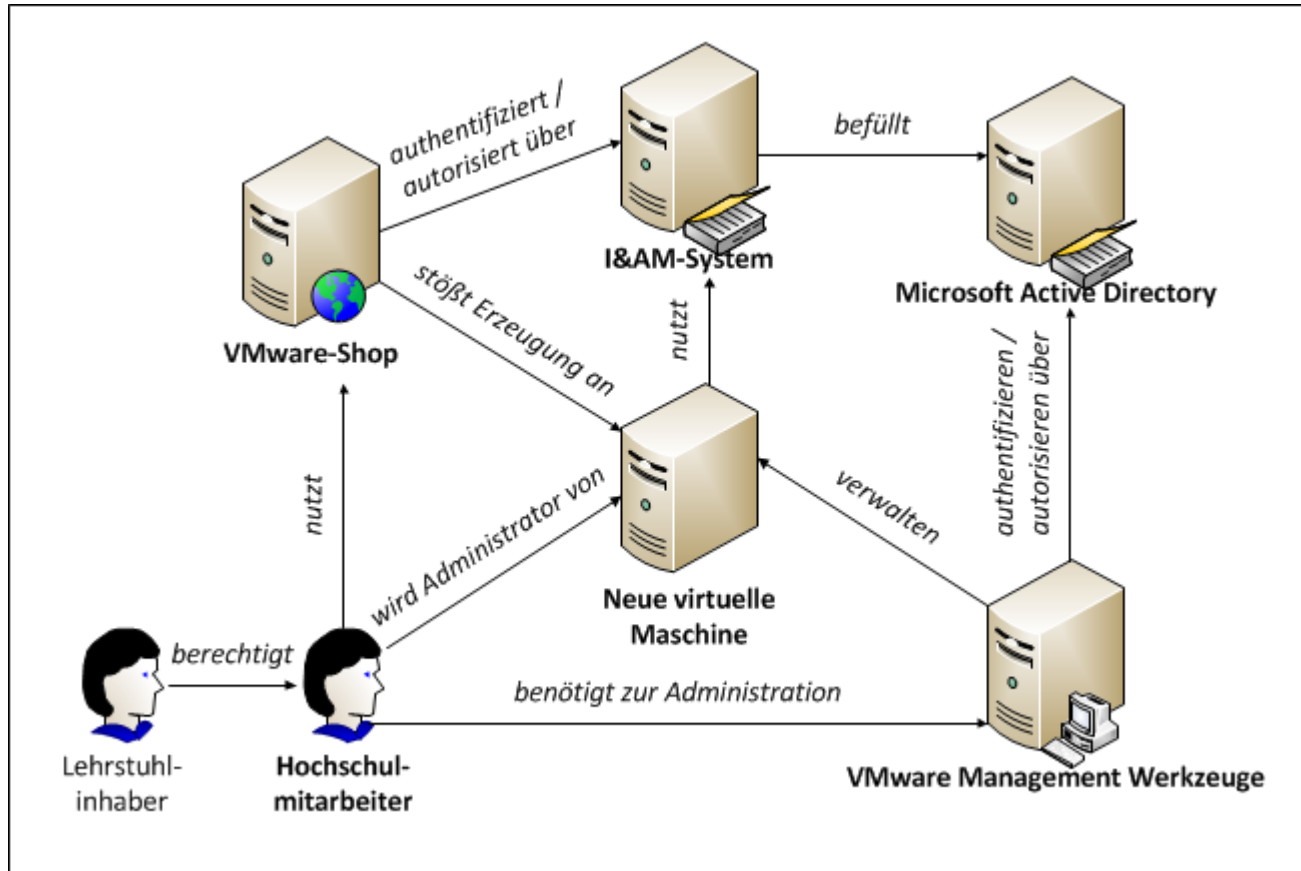
	EMEA	%	US	%	C-Level	%
Yes	331	59%	573	67%	47	66%
No	182	32%	174	20%	22	31%
Don't Know	50	9%	106	13%	2	3%
Grand Total	563	100%	853	100%	71	100%

[<http://www.it-cube.net/fileadmin/itcube/images/it-infrastructure/2011-Snooping-Survey-data.pdf>]

- Status Quo: manuelle Administration

- LRZ: VM-Shop; Anforderungen an IAM
 - (De-)Provisionierung
 - Mehr als reines Anlegen und Löschen
 - Berechtigungsverfahren in mehreren Schritten
 - Authentifizierung, Single Sign-On, Föderation
 - Passwortmanagement (keine identischen Startpasswörter), Benutzerpasswort <> root-Passwort
 - Kopplung an bestehende IAM-Infrastruktur
 - Zugriffskontrolle, Benutzerprofilmanagement
 - Monitoring komplexer
 - Compliance

- Provisionierung, dedizierte Verzeichnisse
 - 👍 keine Anpassung bei Legacy-Systemen
 - 👍 für längerfristig betriebene IT-Dienste
 - 🙅 Teils aufwändige Implementierung
 - 🙅 Dezentrale Datenpools
- LDAP-basierte Authentifizierung, Autorisierung
 - 👍 Hohe Performanz, Skalierbarkeit
 - 👍 Einfache Konfiguration
 - 🙅 Nur für interne User
- AD-Integration
 - 👍 Zentrales Management von Windows-basierten Services
 - (LDAP für Linux-Systeme)
 - (Single Sign-On (Kerberos))
 - 🙅 Wenig Support für Nicht-Microsoftsysteme
- Shibboleth (o.ä.)
 - 👍 Single Sign-On auch für externe Benutzer
 - 👍 Benutzer stimmt Datentransfer explizit zu
 - 👍 Anzahl Anwendungen steigt ständig
 - 🙅 Anpassung von Services aufwändig



- Modulares IAM
 - Provisionierung, Authentifizierung, AD, FIM
- Automatismen für normale User-Accounts
- Gesonderte Betrachtung privilegierter Accounts
 - Konzept von Dienstleister LRZ für Berechtigungsvergabe
 - Idee: Automatische Bereitstellung von Plattformen (virtualisierter Server as a Service)
 - Vision:
 - Berechtigungsvergabe integriert in TUMonline
 - Auch für weitere Plattformen, z.B. Authentifizierungsserver, AD

- Cloud Services auf verschiedenen Ebenen
 - IaaS, PaaS, SaaS
 - Vorteile:
 - Kosteneinsparung
 - Flexibilitätsgewinn
 - Professionell gemanagte IT-Services
 - Konzentration auf Kernkompetenz
 - Vielfältige Herausforderungen an das Management
 - IT Service Management, ITIL-Orientierung
 - Risikomanagement, SLA-Gestaltung

