

# **IDMone**

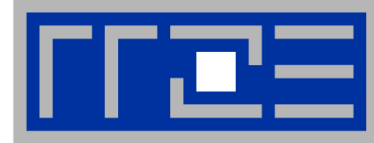
**09.05.2007**

**Sitzung BRZL AK MetaDir, Erlangen**

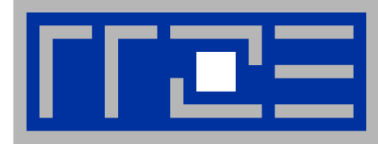
**Hendrik Eggers**



- **Projektkontext**
- **IDMone im Detail**
- **Das IDMone Fachkonzept im Überblick**
- **IDMone Feinkonzept**
- **Novell.IDM@Bayern**

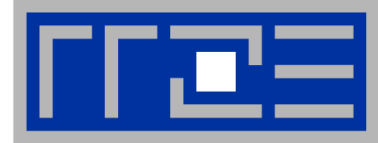


- **Verstärkter Wettbewerb zwischen Universitäten**
  - **Stärkung der Eigenverantwortung der Hochschulen**
  
  - **Steigende Anforderungen an Verwaltung:**
    - **Studentenmanagement (Bologna)**
    - **Kosten-Leistungs-Rechnung**
  
  - **Neue, zusätzliche Aufgaben müssen mit bestehendem Personal erledigt werden**
- ➔ Effizienzsteigerung ist nötig**



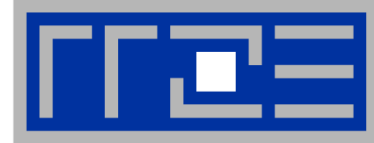
## Unter anderem:

- **Zusammenführung von Verwaltungsdatenverarbeitung und Rechenzentrum im März 2005**
- **Gründung einer Bologna-Gruppe im Juli 2005**
- **Start von „ProFAU“ 2005**
- **Erstmaliger Abschluss von Zielvereinbarungen mit dem Ministerium im Sommer 2006**
- **Planung von flächendeckenden Selbstbedienungsfunktionen für Studierende zum WS 07/08**



- **Unterstützung des Bologna-Prozesses**
- **Entlastung der Mitarbeiter von Routine-Aufgaben**
- **Aufbau einer integrierten Datenhaltung**
- **Einführung umfassender eGovernment-Funktionen**
- **Schaffung von Flexibilität für zukünftige Entwicklungen**

**Der Aufbau einer Identity-Management-Infrastruktur ist die Grundlage für all diese Punkte**



**Friedrich-Alexander-Universität  
Erlangen-Nürnberg**



## **ZIELVEREINBARUNG**

zwischen der  
Friedrich-Alexander-Universität Erlangen-Nürnberg,  
vertreten durch den Rektor  
Prof. Dr. Karl-Dieter Gröske,

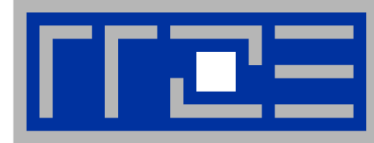
und dem  
Bayerischen Staatsministerium  
für Wissenschaft, Forschung und Kunst,  
vertreten durch den Staatsminister  
für Wissenschaft, Forschung und Kunst  
Dr. Thomas Goppel



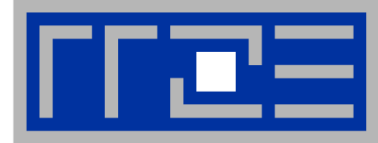
## 3.8.3 Erweiterung des Einsatzes von eGovernment-Funktionen in der Hochschulverwaltung

**Der Aufbau einer zentralen Identity-Management-Infrastruktur bis Ende 2008 ist die Grundlage für eine effiziente Nutzung der universitären IT-Dienste.**

**Die Integration der bisherigen parallelen Datensysteme in eine zentrale Infrastruktur führt zu erhöhter Benutzerfreundlichkeit, Arbeitserleichterungen für die Administratoren sowie einer erhöhten Datenqualität und –sicherheit und unterstützt den Ausbau der von der Staatsregierung gewünschten eGovernment-Funktionen**



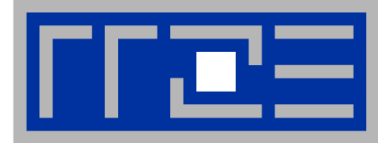
- **26.000 Studierende, 6.000 Beschäftigte, 10.000 Gäste pro Jahr**
- **Seit 1991 selbst entwickelte, gewachsene Benutzerverwaltung am RRZE**
- **Ca. 15 zentrale und x dezentrale Systeme, die mit Stammdaten arbeiten**
- **Keine globale Sicht auf Identitäten**
- **Manuelle Erfassung inhaltsgleicher Daten in verschiedenen Systemen (z.B. Adressen, Telefonnummern)**
- **Teilautomatisierter Datenaustausch bereits für Studierende, nicht für Beschäftigte und Gäste**
- **Eingeschränkte Anbindung dezentraler Systeme, d.h. oft kein Zugriff auf die zentrale Benutzerverwaltung**
- **Dezentrale Administratoren können zentrale Daten nicht bearbeiten**



1. zeitintensive Verfahren für Admins und Kunden, lange Wege
2. erhöhte Fehleranfälligkeit führt zu Nachfragen und Nacharbeiten
3. wiederholtes Abfragen der Stammdaten bei Kunden

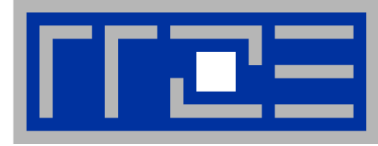


- **1990 Projektidee Kanzler: „eine Karte für alles“**
- **03/2005 Initialer IDM Workshop FAU**
- **05/2006 Entscheidung Software + Dienstleister (Novell)**
- **06/2006 Beschlussvorlage Hochschulleitung**
- **07/2006 Zielvereinbarung FAU / Staatsministerium**
- **09/2006 Projektfreigabe durch Kanzler**
- **10/2006 Projektinitiierung**
  
- **7. November 2006: Projekt Kickoff-Veranstaltung**

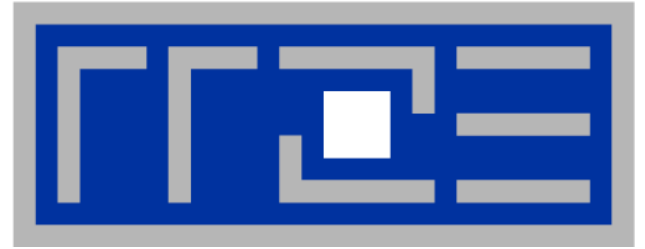


**Mit einer zentralen Identitätsverwaltung die Grundlage für eine effiziente Nutzung universitärer IT-Dienste schaffen**

- **Steigende Verwaltungsanforderungen (z.B. durch *Bologna*) bewältigen**
- **Benutzerfreundlichkeit für Kunden und Administratoren erhöhen: Webseite statt Formular, jederzeit & überall**
- **Entlastung für Sachbearbeiter und Admins schaffen: Datenpflege wird erleichtert**
- **Datenqualität und -validität erhöhen: Stammdaten sind aktuell, eindeutig und einheitlich**
- **Sicherheit erhöhen: Reduzierung anonymer Accounts**
- **Wirtschaftlichkeit:**
  - **Vermeidung von Doppelarbeit**
  - **Keine Medienbrüche**

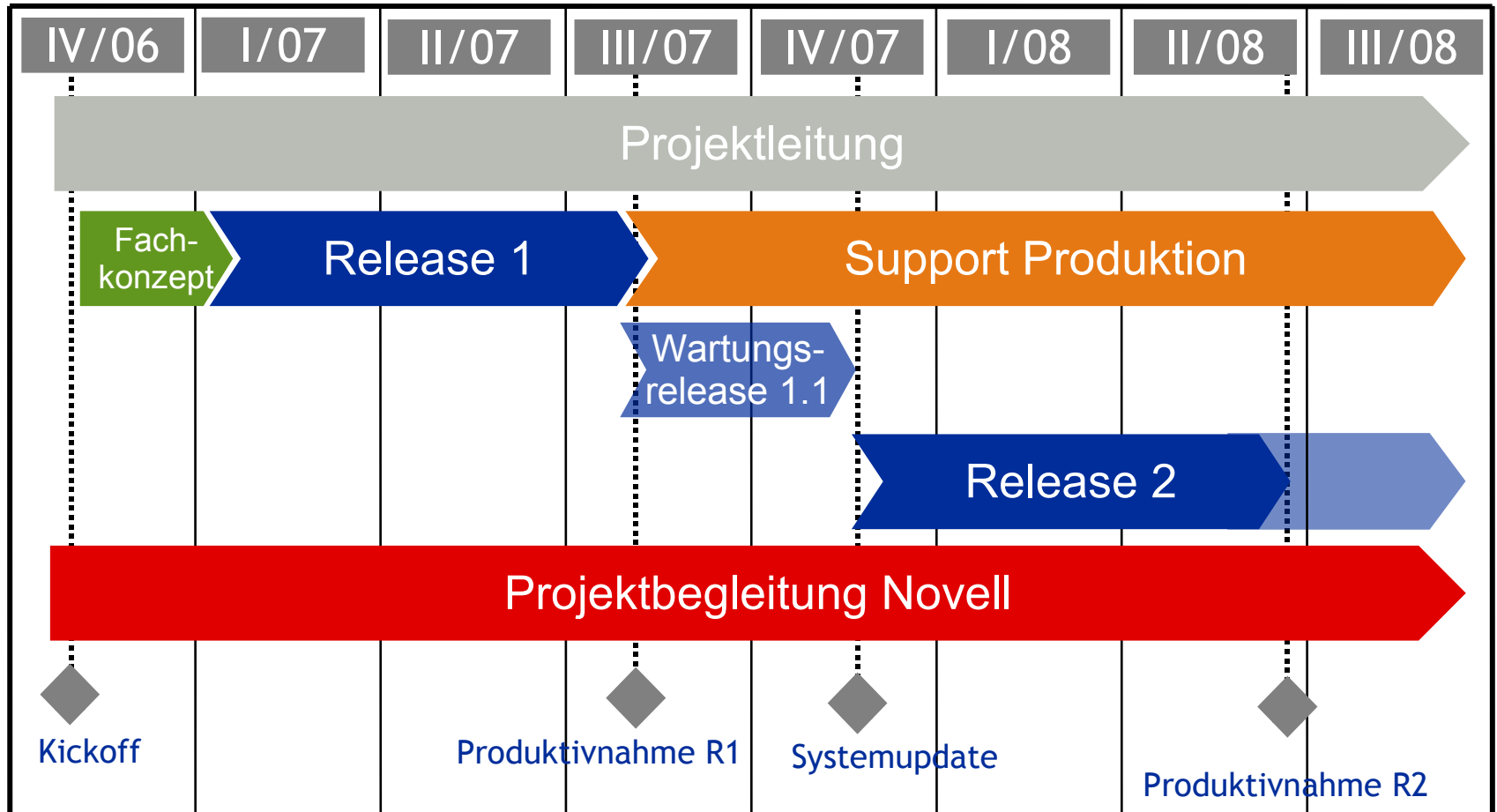
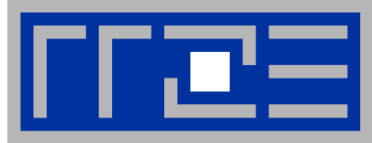


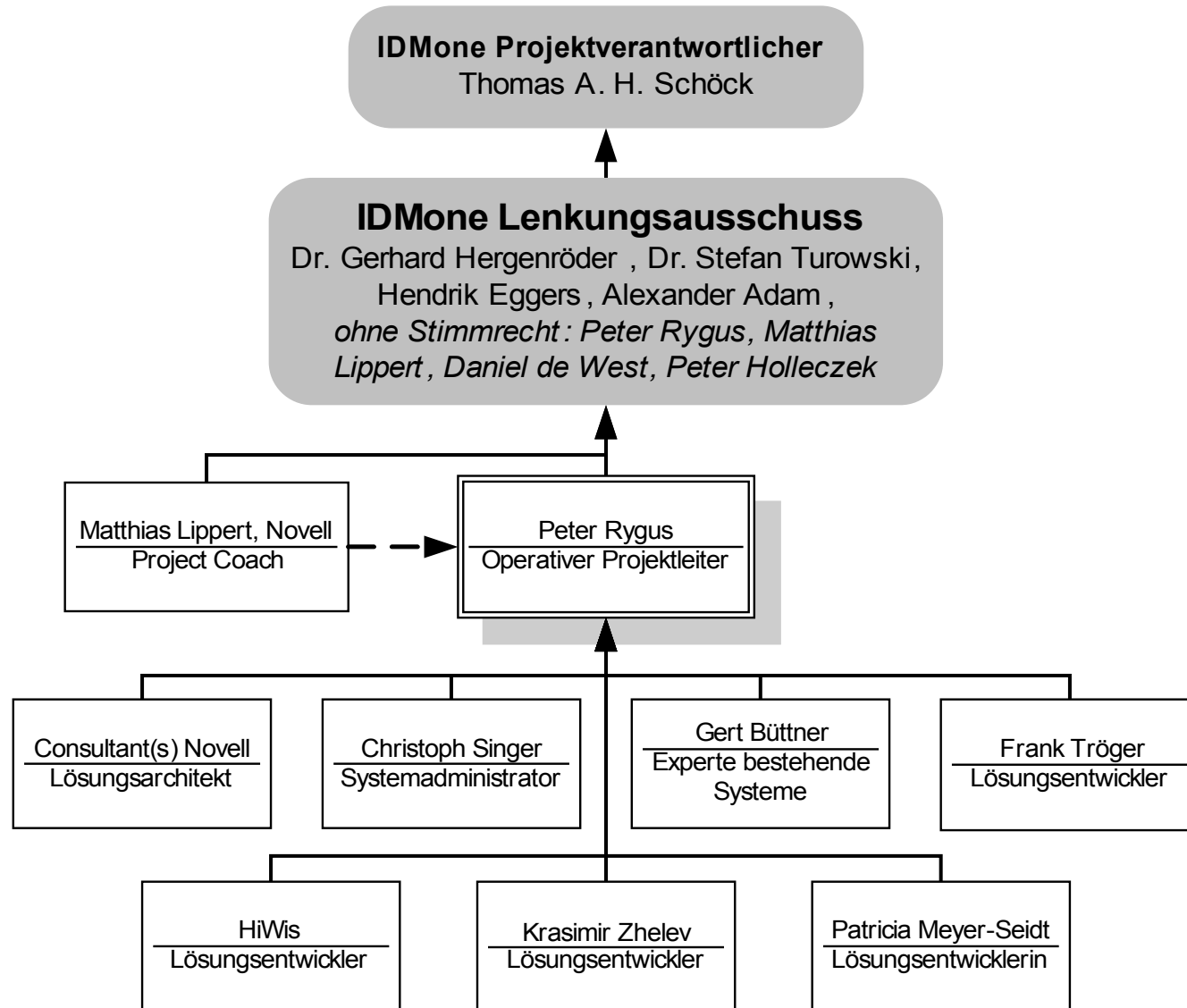
- **Inbetriebnahme einer zentralen Identitätsverwaltung**
- **Automatisierte Vergabe von Benutzerkennungen für Studierende und Beschäftigte zur Nutzung der kostenfreien Basisdienste (WLAN, VPN, E-Mail)**
- **Dezentrale web-basierende Erfassung von Gästen**
- **Vorraussetzungen schaffen für die Einführung der Online-Prüfungsverwaltung (Projektschnittstelle)**
- **Provisionierung der Systeme:**
  - **Zutrittskontrolle (FAU-PORT / FAMOS)**
  - **Zeiterfassung**
  - **...**
- **Bereitstellung einer Schnittstelle für dezentrale Systeme (Authentifizierung / Datenaustausch)**

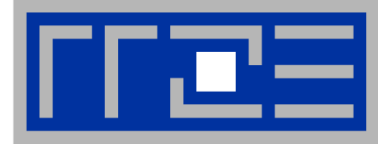


## **IDMone im Detail**

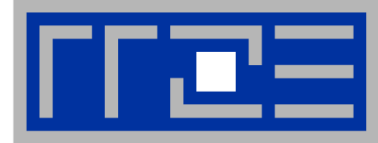
# Initialer Zeitplan





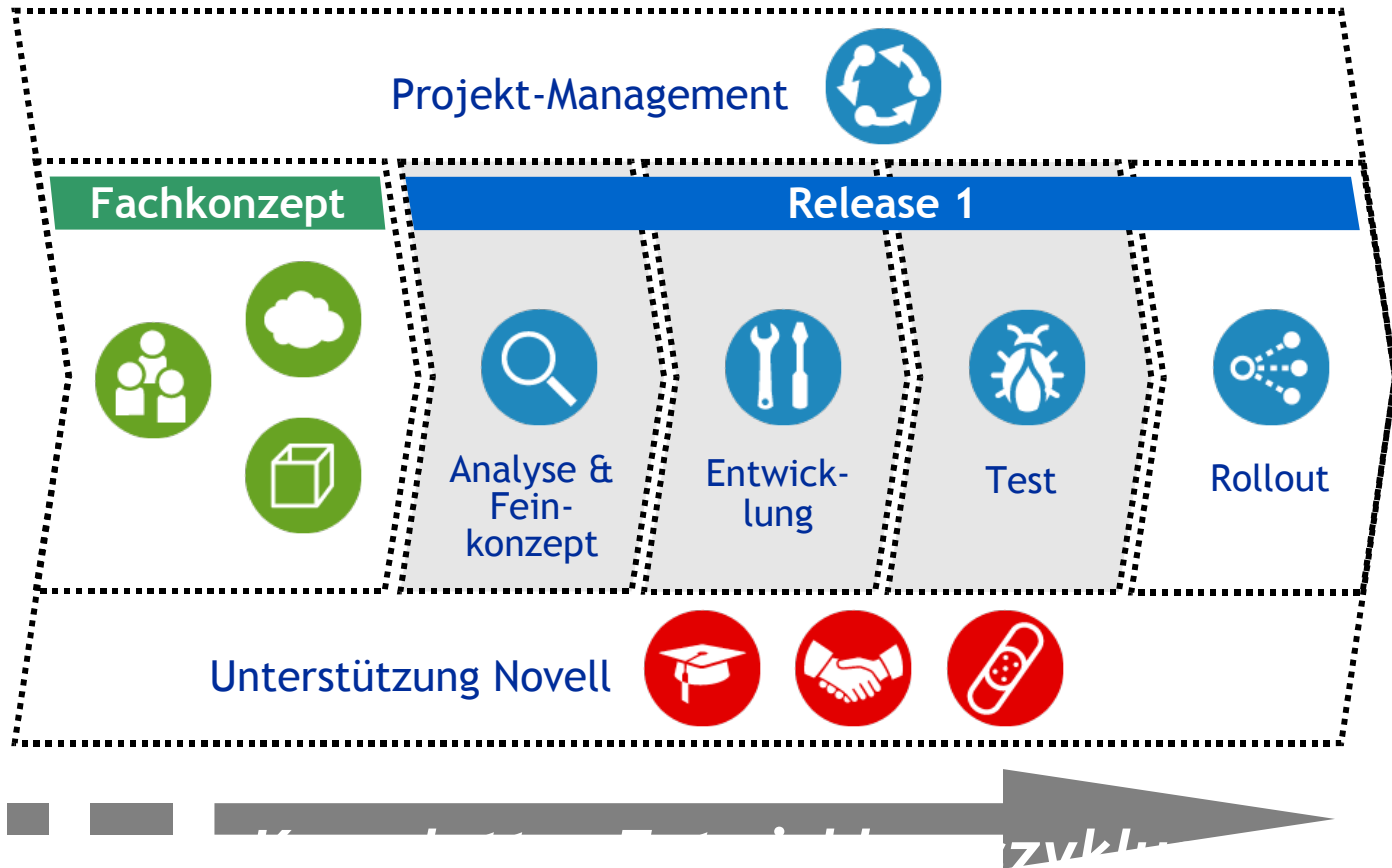


- **Bereitschaft aller Beteiligten, notwendige Veränderungen an Arbeitsabläufen mit zu tragen**
- **Technologie ist kein Allheilmittel => Abläufe müssen sauber definiert und implementiert sein**
- **Release 1 muss bereits spürbaren Nutzen für Endkunden und Administratoren zeigen**



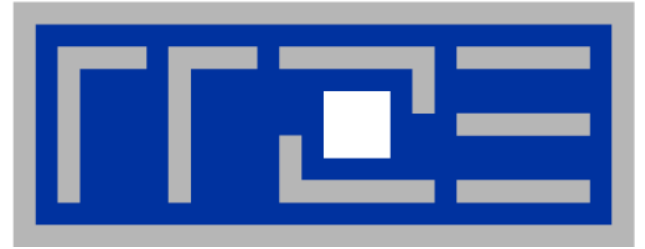
# Risiken

- **Personelle Ausstattung**
- **Barrierefreie Weboberfläche mit Novell Front-End**
- **Konsensverfahren**
- **Abbildung der Organisationsstruktur**
- **DIT -Struktur**
- **Neueinführung Novell IDM**
- **Anbindung RRZE-Abrechnung**

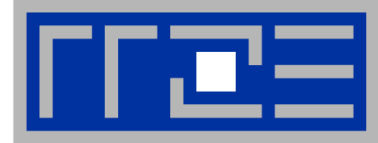




- **Quartalsweise Projektstatusbericht**
- **Verwertung der Erfahrungen**
  - **studentische Arbeiten**
  - **diverse wissenschaftliche Artikel**
  - **zwei Promotionen**
  - **Erfahrungsaustausch**
    - **BRZL**
    - **ZKI + ZKI Arbeitskreis Verzeichnisdienste**
    - **EUNIS**
    - **sowie bilaterale Kommunikation mit anderen Identity Management Projekten im In- und Ausland**
  - **aktive Pressearbeit (BI, Uni-Kurier, ...)**

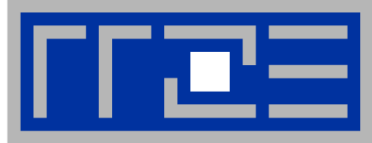


## **Das IDMone Fachkonzept im Überblick**



# Benutzergruppen

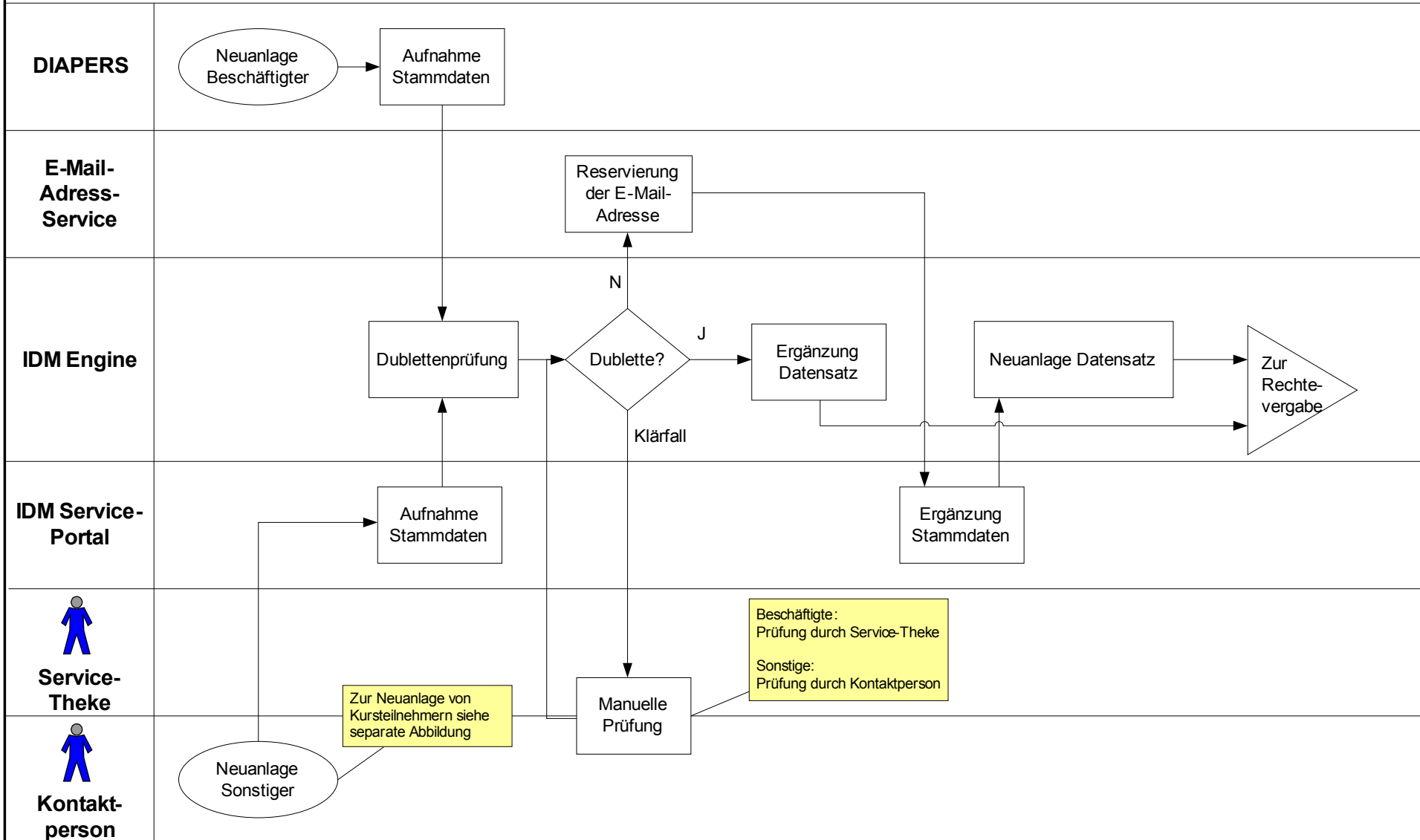
- **Studierende**
- **Beschäftigte**
- **Sonstige**
  - **Gäste aller Art**
  - **Externe**
  - ...
- **Organisationen und Organisationseinheiten**



# Prozesse

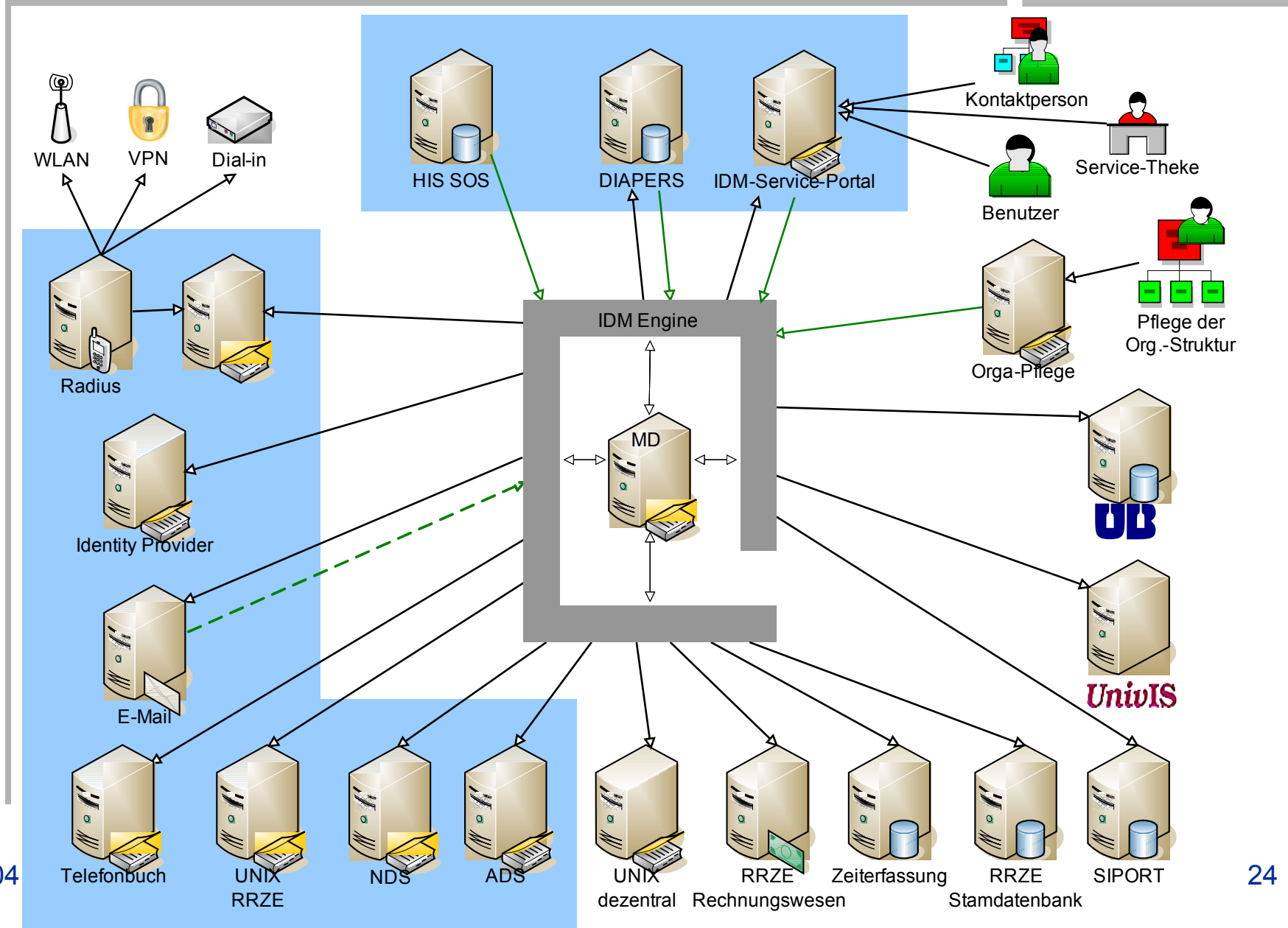
- **Übersicht über die wesentlichen Prozesse der Benutzerverwaltung nach Benutzergruppen dargestellt**
  - **Neuanlage**
  - **Ändern**
  - **Archivieren (kein Löschen im IDM nur ggf. in den Zielsystemen)**
    - **Ermöglichen der Rückkehr an die Universität**
    - **Vermeidung von Kollisionen z.B. bei E-Mail-Adressen**
- **Exakte Prozessgestaltung erfolgt im Feinkonzept auf die jeweiligen Zielsysteme bezogen**
- **systemübergreifende Modellierung**

## Neuanlage eines Personeneintrages für Beschäftigte und Sonstige

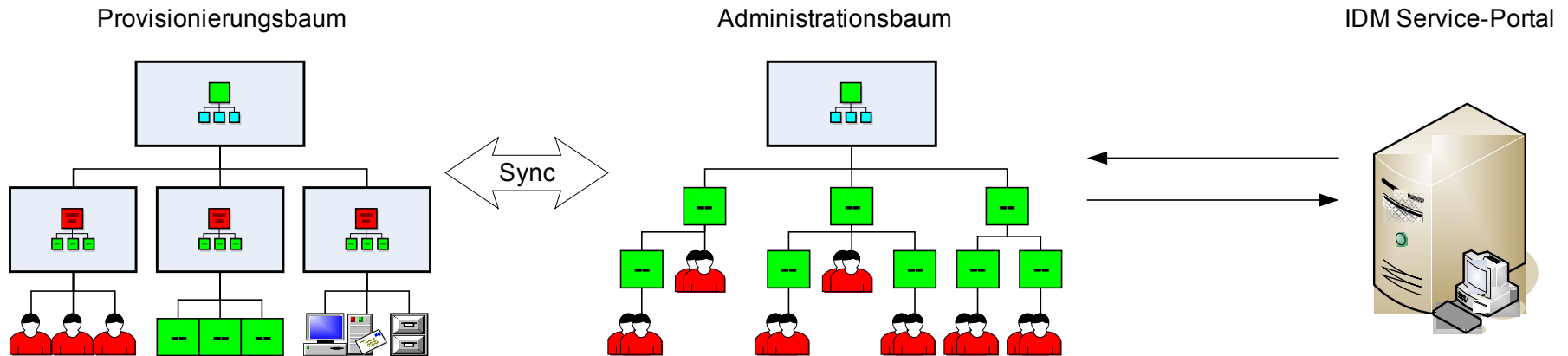




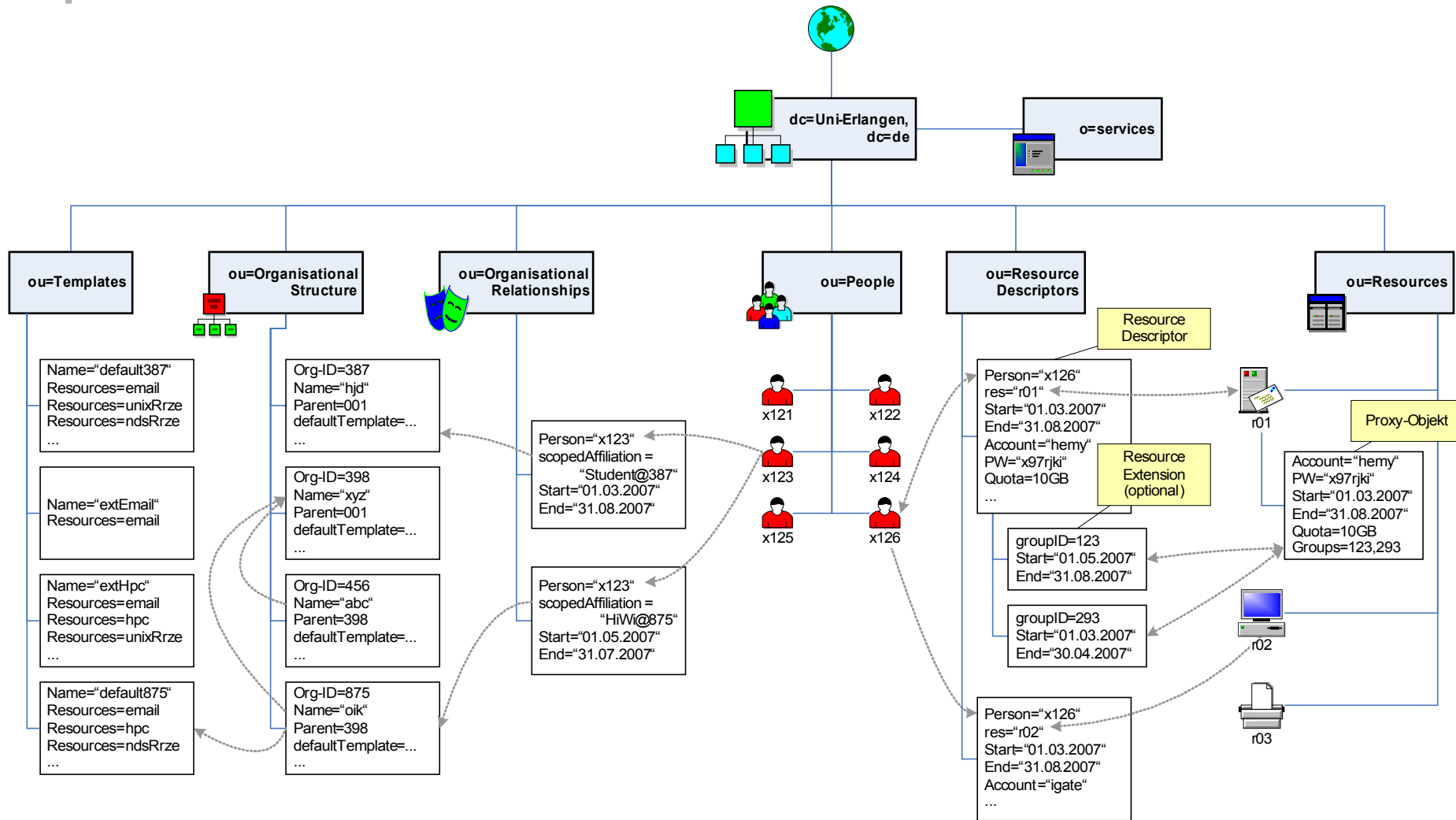
# Zielarchitektur



# Das hybride Modell



# Der Provisionierungsbaum





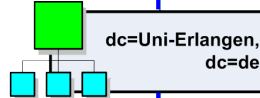
Admin

1

13

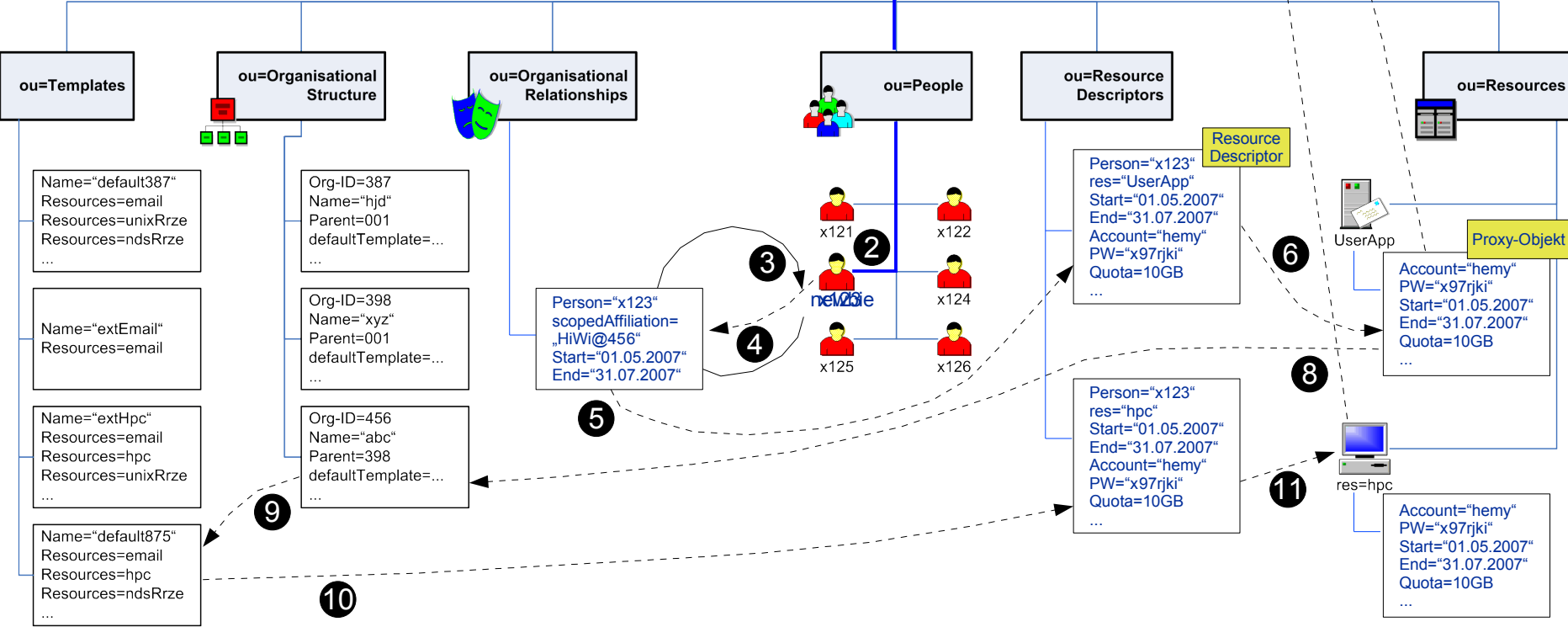


2



7

12



3

2

4

5

6

8

11

9

10

ou=Templates

ou=Organisational Structure

ou=Organisational Relationships

ou=People

ou=Resource Descriptors

ou=Resources

Name="default387"  
Resources=email  
Resources=unixRrze  
Resources=ndsRrze  
...

Name="extEmail"  
Resources=email

Name="extHpc"  
Resources=email  
Resources=hpc  
Resources=unixRrze  
...

Name="default875"  
Resources=email  
Resources=hpc  
Resources=ndsRrze  
...

Org-ID=387  
Name="hjd"  
Parent=001  
defaultTemplate=...

Org-ID=398  
Name="xyz"  
Parent=001  
defaultTemplate=...

Org-ID=456  
Name="abc"  
Parent=398  
defaultTemplate=...

Person="x123"  
scopedAffiliation=  
„HiWi@456"  
Start="01.05.2007"  
End="31.07.2007"

Person="x123"  
res="UserApp"  
Start="01.05.2007"  
End="31.07.2007"  
Account="hemy"  
PW="x97rjki"  
Quota=10GB  
...

Person="x123"  
res="hpc"  
Start="01.05.2007"  
End="31.07.2007"  
Account="hemy"  
PW="x97rjki"  
Quota=10GB  
...

Account="hemy"  
PW="x97rjki"  
Start="01.05.2007"  
End="31.07.2007"  
Quota=10GB  
...

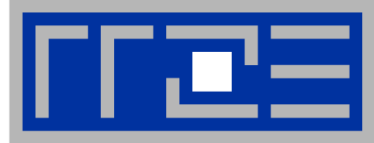
Account="hemy"  
PW="x97rjki"  
Start="01.05.2007"  
End="31.07.2007"  
Quota=10GB  
...

Resource Descriptor

Proxy-Objekt

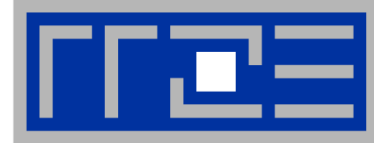
UserApp

res=hpc



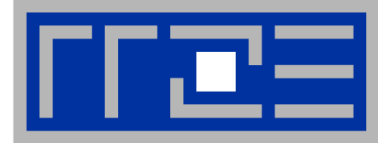
# Das Problem mit der Organisationsstruktur

- **Zugehörigkeit einer Person zu einer Organisationseinheit ist wesentliche Basis für die Berechtigungsvergabe**
- **unterschiedliche Nutzer benötigen jeweils unterschiedliche Sichten auf die Organisation**
- **Ausgangsbasis: Gliederungsbescheid**
  - **Nicht ausreichend, da wesentliche Informationen nicht enthalten, wie z.B.:**
    - **temporäre Strukturen (z.B. Drittmittelprojekte)**
    - **Sonderforschungsbereiche oder andere Forschungsverbünde**
    - **Organisationseinheiten aufgrund von Einzelbescheiden (z.B. interdisziplinäre Einrichtungen)**
    - **Strukturen, die nicht Teil der FAU sind, aber aufgrund unterschiedlicher Beziehungen Ressourcen an der FAU bzw. dem RRZE nutzen (Beispiel: An-Institute)**
    - **Untergliederungen großer Organisationseinheiten aufgrund von Geschäftsverteilungsplänen**



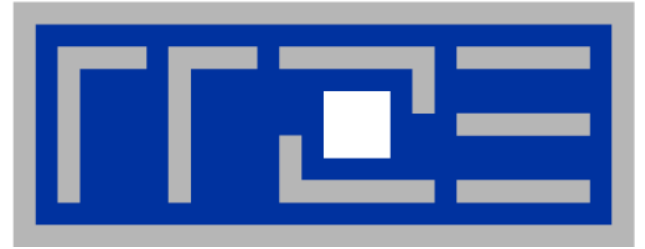
# Das IDM-Service-Portal

- **Zentrale web-basierte Anlaufstelle i.S. IDM für**
  - Benutzer,
  - dezentrale und
  - zentrale Administration
- **Datenquelle für die Sonstigen (Gästeverwaltung)**
- **Selbstbedienungsfunktion für Benutzer**
  - Datenschutzselbstauskunft
  - Passwortänderung
  - Beantragung von Dienstleistungen
  - Adressänderung???
- **Administrative Funktionen**
  - Passwort setzen
  - Konten sperren / entsperren
- **Modelliert mittels UseCases**

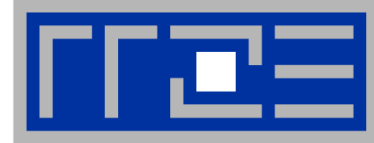


# Die neuen Benutzerkennungen

- **semantikkfrei**
- **aussprechbar**
- **8 stellig**
  
- **Muster {kv|vk}zz{kvkv|vkvk}**
  - **k = Konsonant**
  - **v = Vokal**
  - **zz = Ziffer+andere Ziffer**
  
- **Beispiele:**  
**ba23cedi, mi49hopa, hu63pola, no35daxe, ik87napu, um95kite**

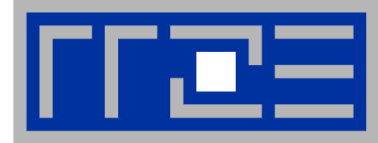


## **IDMone Feinkonzept**

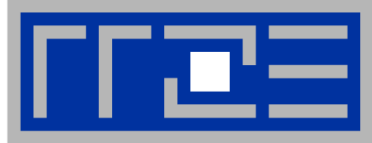


# Woraus besteht ein Arbeitspaket?

- **Kundengespräch + Gesprächsprotokoll**
- **Umfangsdefinition - Was soll laufen?**
  - Was wurde diskutiert?
  - Zu welchen Ergebnissen ist man gekommen und warum?
- **Konzept gemäß Novell-Vorlage im Wiki**
- **Treiber-Konfiguration**
  - Pilotierung
  - Umsetzung im Entwicklungssystem
- **Beispiel System (Quelle- oder Ziel-)**
- **Geschäftsprozessmodell (Swimmlane-Diagramm)**
- **Qualitätssicherung / Test gemäß Konzept Frank Tröger**
- **Review durch System Engineer**
- **evtl. System-Konfiguration**
- **Feedback mit Kunden + Gesprächsprotokoll**

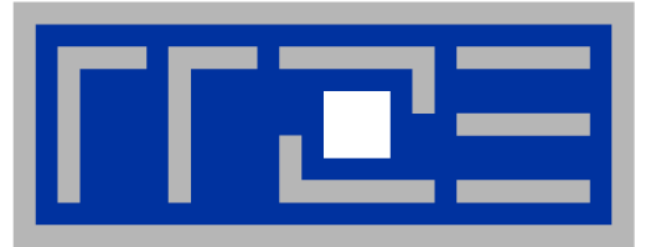


- **01.08.2007**                      **Roll-Out erster Systeme**
- **30.09.2007**                      **Zwischenbericht an Staatsministerium**
- **08/2007 – 02/2008**              **Phase II**
- **03/2008 – 09/2008**              **Phase III**
- **30.09.2008**                      **Projektabschlußbericht**

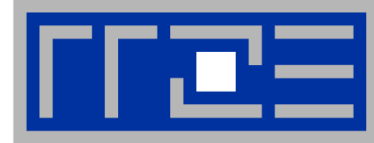


# AG IDMone

- **Ende des „Brütens“**
- **Beteiligung der maßgeblichen Akteure / Fachanwendungsbetreuer**
- **Beobachter des studentischen Konvents**
- **Berichte über den aktuellen Stand**
- **Anregungen für die laufende und zukünftige Arbeit**
  
- **Monatlich immer Dienstags sofort nach der DB**
  
- **seit 08.05.2007**



**Novell.IDM@Bayern**

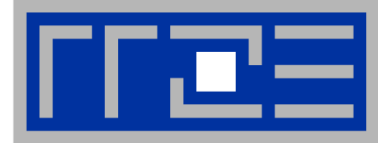


- **Gemeinsames IDM-Konzept**
  - ITS Uni Augsburg
  - KH Eichstätt
  - RRZE
  - Uni Passau
  - RZUW
  - LRZ
- **Entwickelt in regelmäßigen Videokonferenzen**
- **Weitere Teilnehmerinnen willkommen**
- **Ausgangslage**
  - **Generell und flexibel adaptierbar**
    - Modular
    - Inkl. IDM-Service-Portal
  - **Prototypische Umsetzung mittels Novell**
    - Kommunikation ggü. Novell durch RRZE
    - IDMonе als Ausgangsbasis für Konzept



# Was fehlt noch?

- **Lasttests**
  - **Welcher Kollege möchte das System testen?**
- **Ausführliche Beschreibung der Abläufe im IDM-System**
  - **aka Feinkonzept / Dokumentation**
  - **Animation geplant**
- **Kooperationsplattform für Novell.IDM@Bayern**
- **Beschreibung der Projektmanagement-Standards**
  - **Bereits heute auf Anfrage**
- **Publikation von schema-Vergleich und Hilfsmittel zur  
Attribut-Wahl**

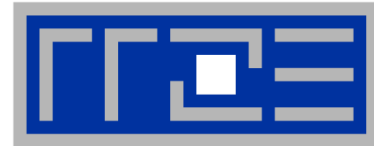


# Links

- **Webseite von IDMone**
  - **Fachkonzept IDMone**
  - **Vortrags-Stream zu IDMone**
  - **Novell Identity Manager**
    - **Novell User Application**



**Vielen Dank für Ihre  
Aufmerksamkeit!**



Dipl.-Kfm.

## **Hendrik Eggers**

Projektleiter Identity Management

RRZE ▪ Martensstraße 1

D-91058 Erlangen

Tel.: +49 9131 85-27819

Mobil: +49 170 6219877

Fax: +49 9131 302941

[hendrik.eggers@rrze.uni-erlangen.de](mailto:hendrik.eggers@rrze.uni-erlangen.de)



**Regionales  
Rechenzentrum  
Erlangen**

**Der IT-Dienstleister der FAU**

<http://www.rrze.uni-erlangen.de>

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)