

IFB IDMone

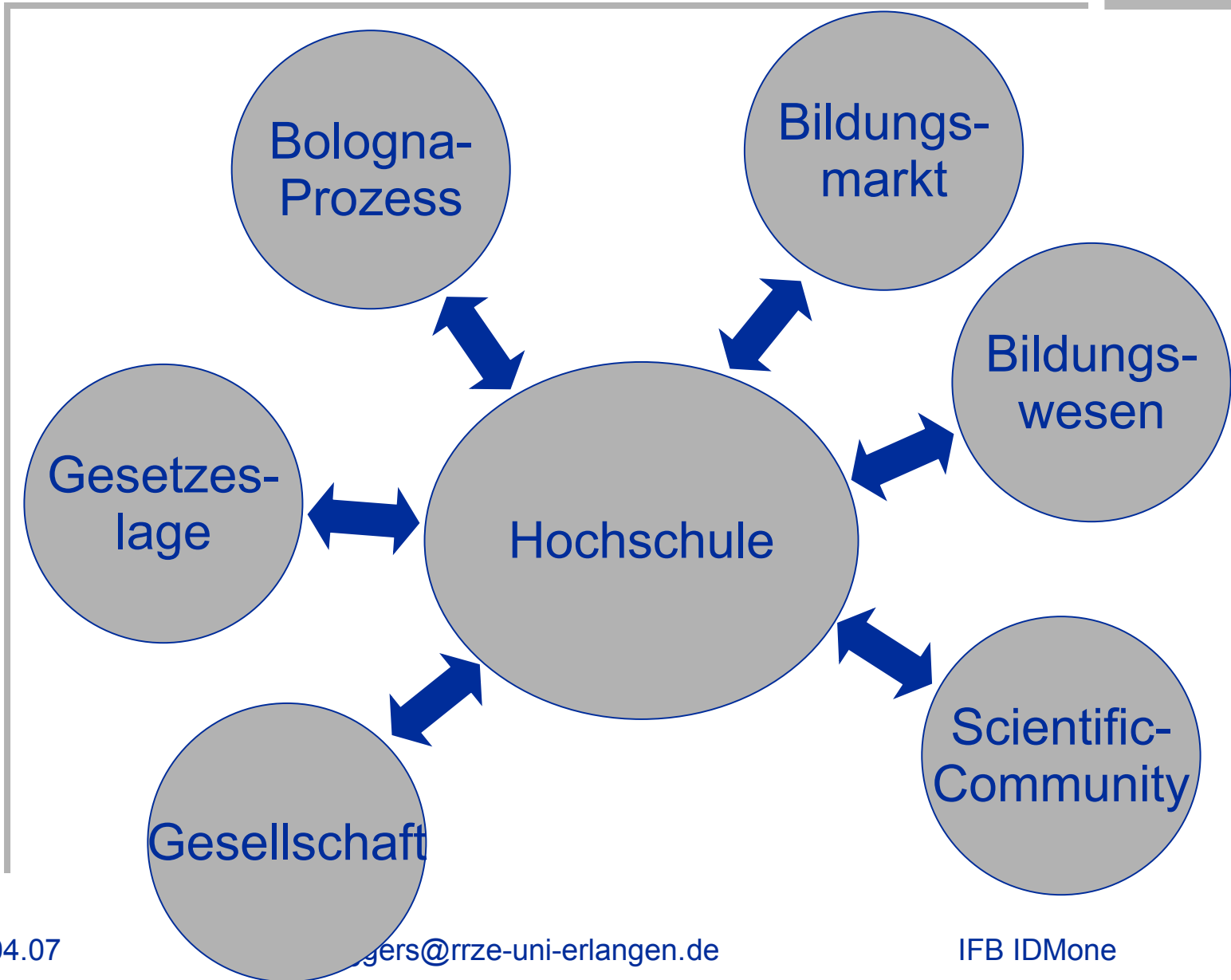
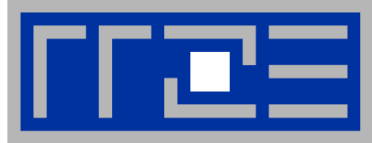
03.04.2007

RRZE

Hendrik Eggers



- **Einführung**
- **Projektkontext**
- **Thematische Einführung „Identity Management“**
- **IDMone im Detail**
- **Das IDMone Fachkonzept im Überblick**
- **Was kommt im Feinkonzept?**

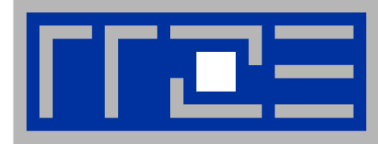




- **Verstärkter Wettbewerb zwischen Universitäten**
 - **Stärkung der Eigenverantwortung der Hochschulen**

 - **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



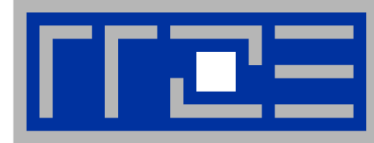
**Friedrich-Alexander-Universität
Erlangen-Nürnberg**



ZIELVEREINBARUNG

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

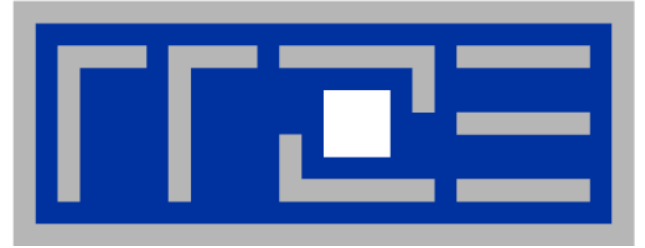
und dem
Bayerischen Staatsministerium
für Wissenschaft, Forschung und Kunst,
vertreten durch den Staatsminister
für Wissenschaft, Forschung und Kunst
Dr. Thomas Goppel



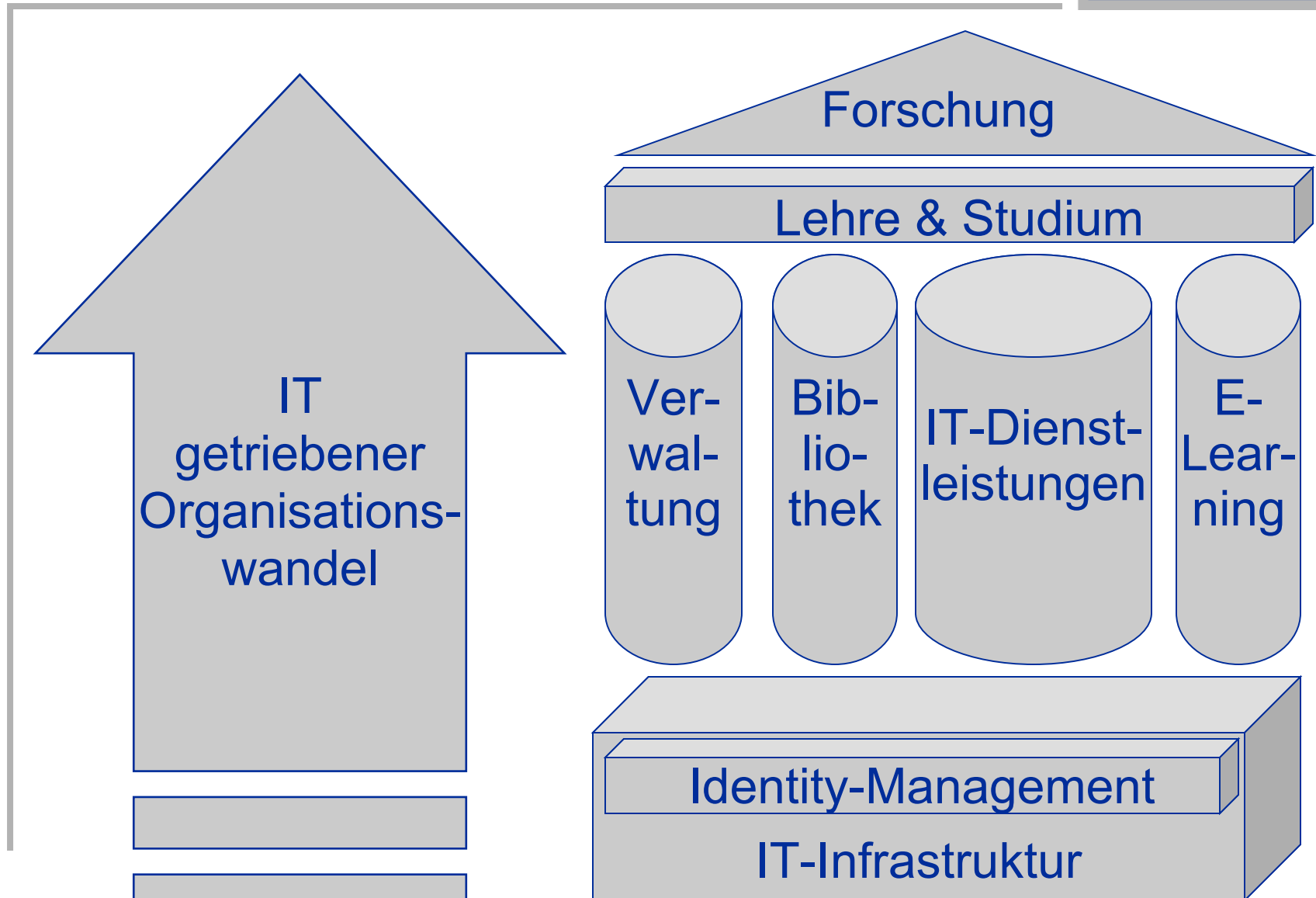
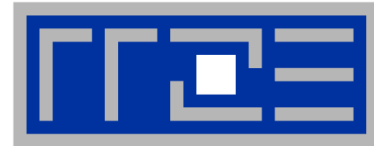
3.8.3 Erweiterung des Einsatzes von eGovernment-Funktionen in der Hochschulverwaltung

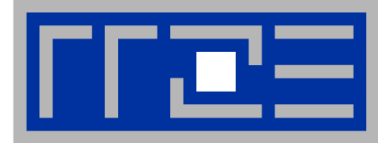
Der Aufbau einer zentralen Identity-Management-Infrastruktur bis Ende 2008 ist die Grundlage für eine effiziente Nutzung der universitären IT-Dienste.

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



Eine Sicht auf die Hochschule aus IT-Perspektive

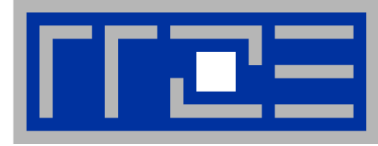




- **26.000 Studierende, 6.000 Beschäftigte, 10.000 Gäste pro Jahr**
- **Seit 1991 selbst entwickelte, gewachsene Benutzerverwaltung am RRZE**
- **Ca. 15 zentrale und x dezentrale Systeme, die mit Stammdaten arbeiten**
- **Keine globale Sicht auf Identitäten**
- **Manuelle Erfassung inhaltsgleicher Daten 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**

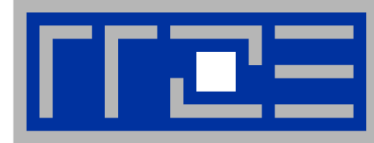


1. zeitintensive Verfahren für Admins und Kunden, lange Wege
2. erhöhte Fehleranfälligkeit führt zu Nachfragen und Nacharbeiten
3. wiederholtes Abfragen der Stammdaten bei Kunden



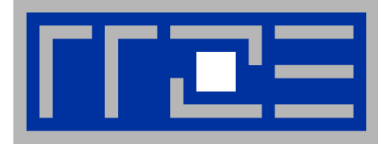
- **1990** Projektidee Kanzler: „eine Karte für alles“
- **03/2005** Initialer IDM Workshop FAU
- **05/2006** Entscheidung Software + Dienstleister (Novell)
- **06/2006** Beschlussvorlage Hochschulleitung
- **07/2006** Zielvereinbarung FAU / Staatsministerium
- **09/2006** Projektfreigabe durch Kanzler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

- **7. November 2006: Projekt Kickoff-Veranstaltung**

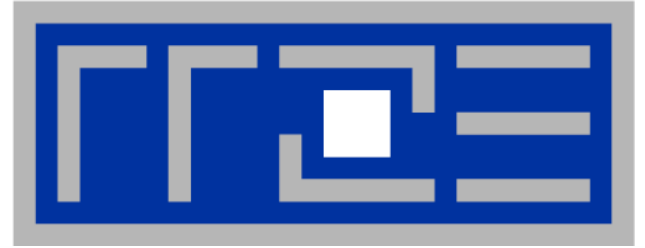


Mit einer zentralen Identitätsverwaltung die Grundlage für eine effiziente Nutzung universitärer IT-Dienste schaffen

- **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 Datenbrüche**

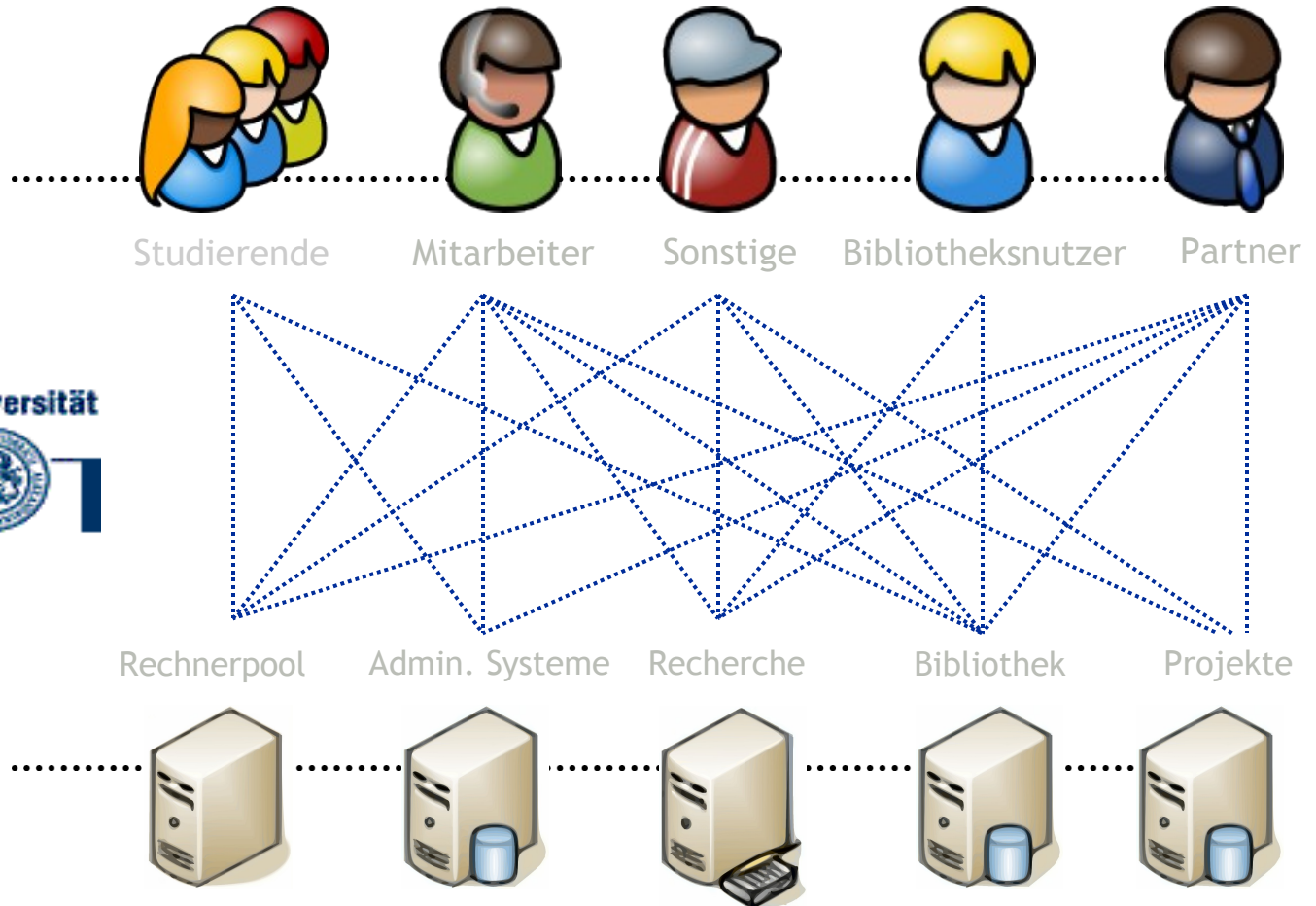
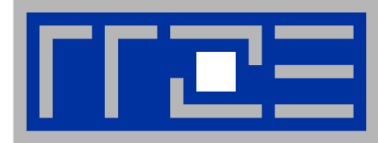


- **Inbetriebnahme einer zentralen Identitätsverwaltung**
- **Automatisierte Vergabe von Benutzerkennungen für Studierende und Beschäftigte zur Nutzung der kostenfreien Basisdienste (WLAN, VPN, E-Mail)**
- **Dezentrale web-basierende Erfassung von Gästen**
- **Vorraussetzungen schaffen für die Einführung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



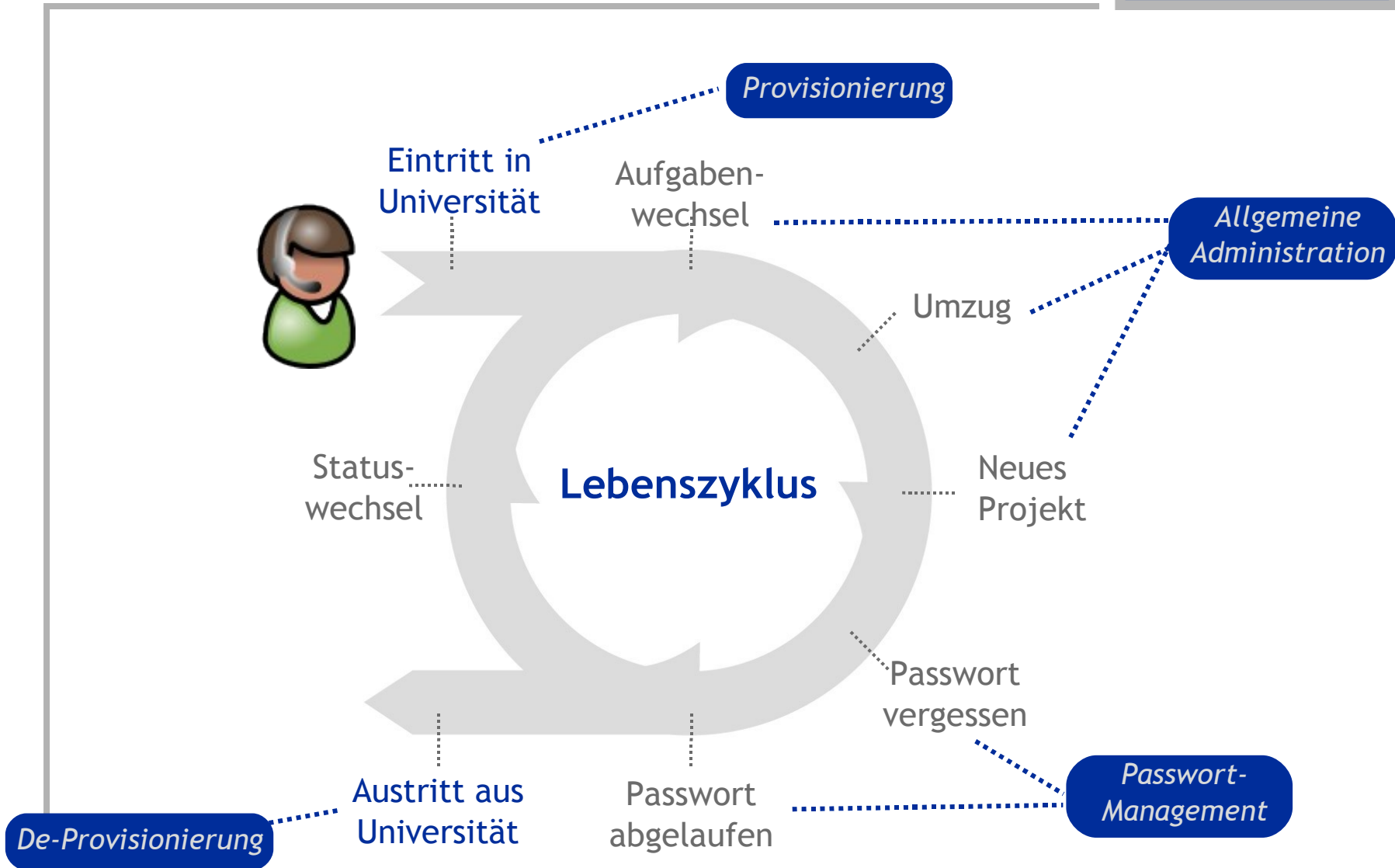
Thematische Einführung „Identity Management“

Zugriffskontrolle ist komplex

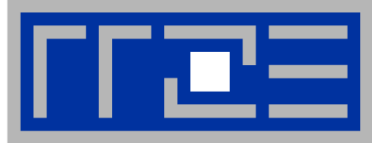


Friedrich-Alexander-Universität
Erlangen-Nürnberg

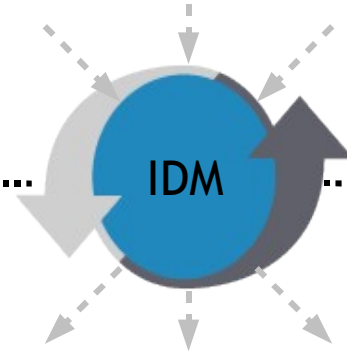
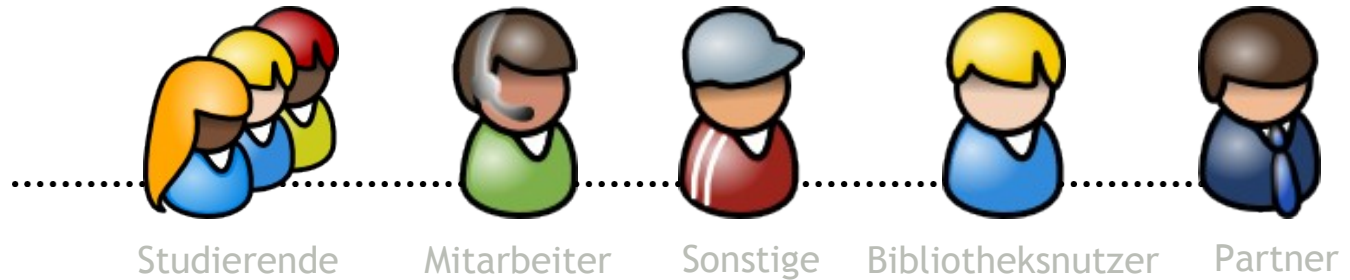




Lösung: Zentrales Identitätsmanagement

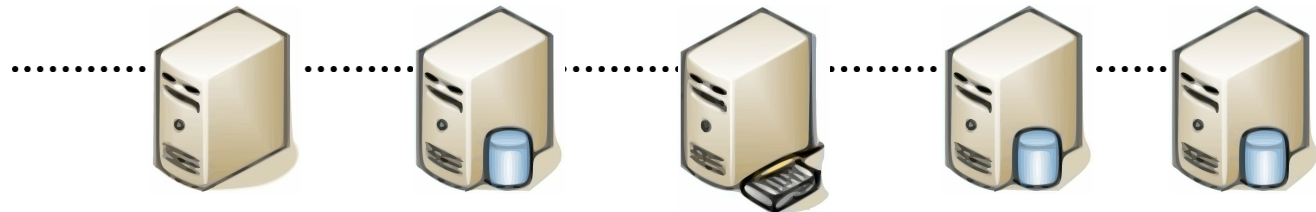


Friedrich-Alexander-Universität
Erlangen-Nürnberg



- Erhöhte Sicherheit
- Reduzierte Kosten
- Verbesserte Produktivität
- Gesteigerte Zufriedenheit

Rechnerpool Admin. Systeme Recherche Bibliothek Projekte



Szenario: Provisionierung eines neuen Mitarbeiters

1) Ein neuer Mitarbeiter wird in der Personalabteilung angelegt

Personal-
verwaltung



Sachbe-
arbeiter

Hans Muster

Angeschlossene Systeme nur
zur beispielhaften Illustration

mi49hopa

NDS



Linux

mi49hopa



Bibliothek



00471108150

IDM
Engine

E-Mail-System

hans.muster@uni-erlangen.de



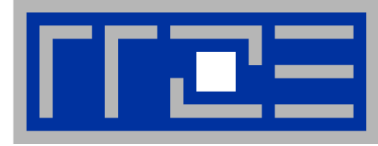
Telefon

09131-85-12345



2) IDM Engine erkennt die Neuanlage

3) IDM Engine erzeugt einen Zugang zu jedem an-
geschlossenen System und synchronisiert die erforder-
lichen Informationen gemäß vorab definierter Regeln

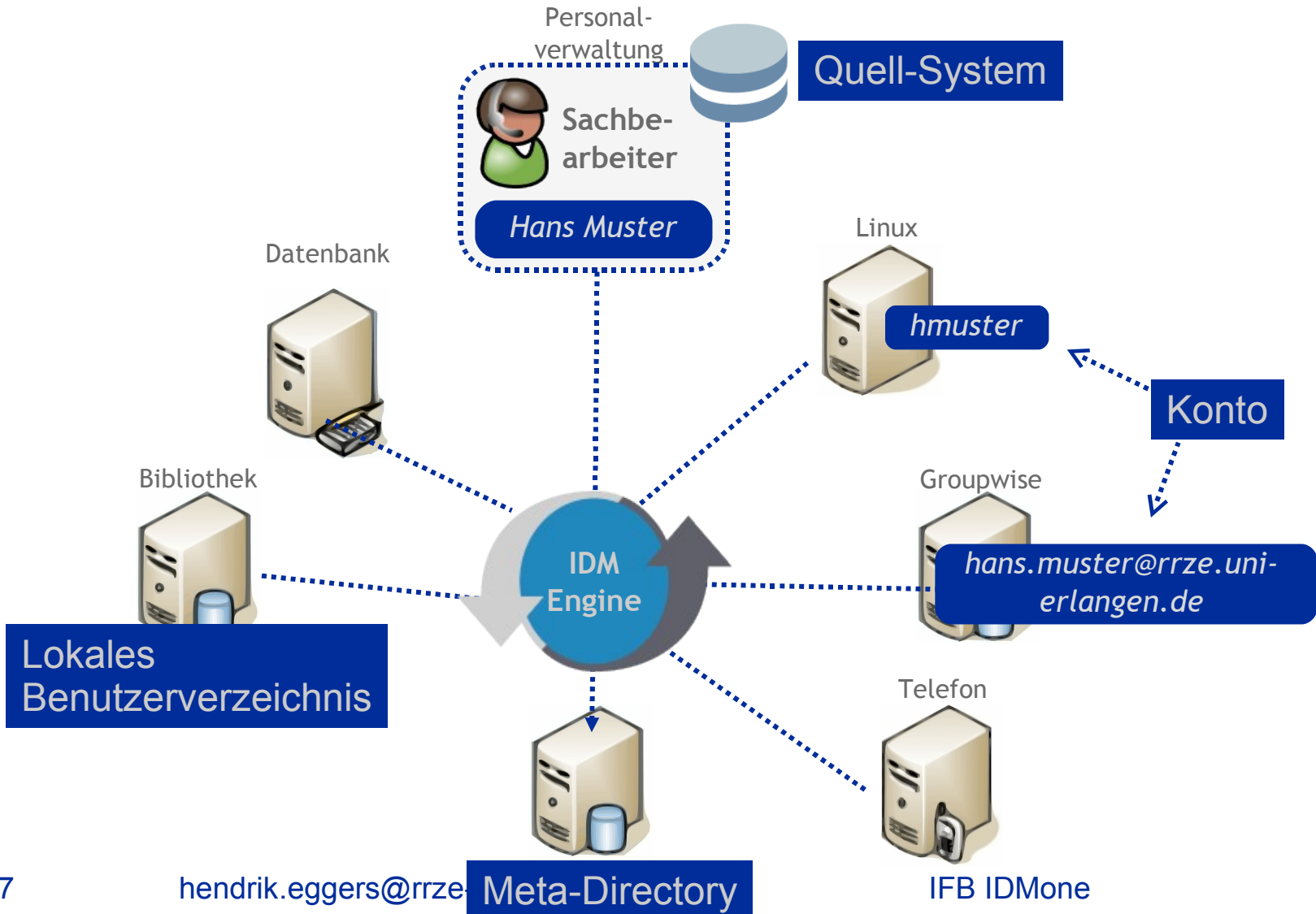


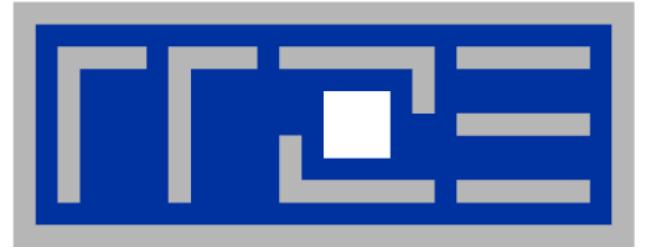
Exemplarische Funktionen

- **Starke, systemweite Password-Policies**
 - Beispiele: Min./max. Anzahl von Zeichen, minimale Anzahl von Großbuchstaben, Ziffern und Sonderzeichen, Passwort-Historie, Negativ-Listen

- **Password Self-Service**
 - Web-basierter Self-Service ermöglicht Benutzern das Zurücksetzen von Passwörtern (z.B. durch Hilfsfragen)
 - Passwort-Management direkt auf den nativen Plattformen (z.B. MS Windows) kann ermöglicht werden (noch zu entscheiden).

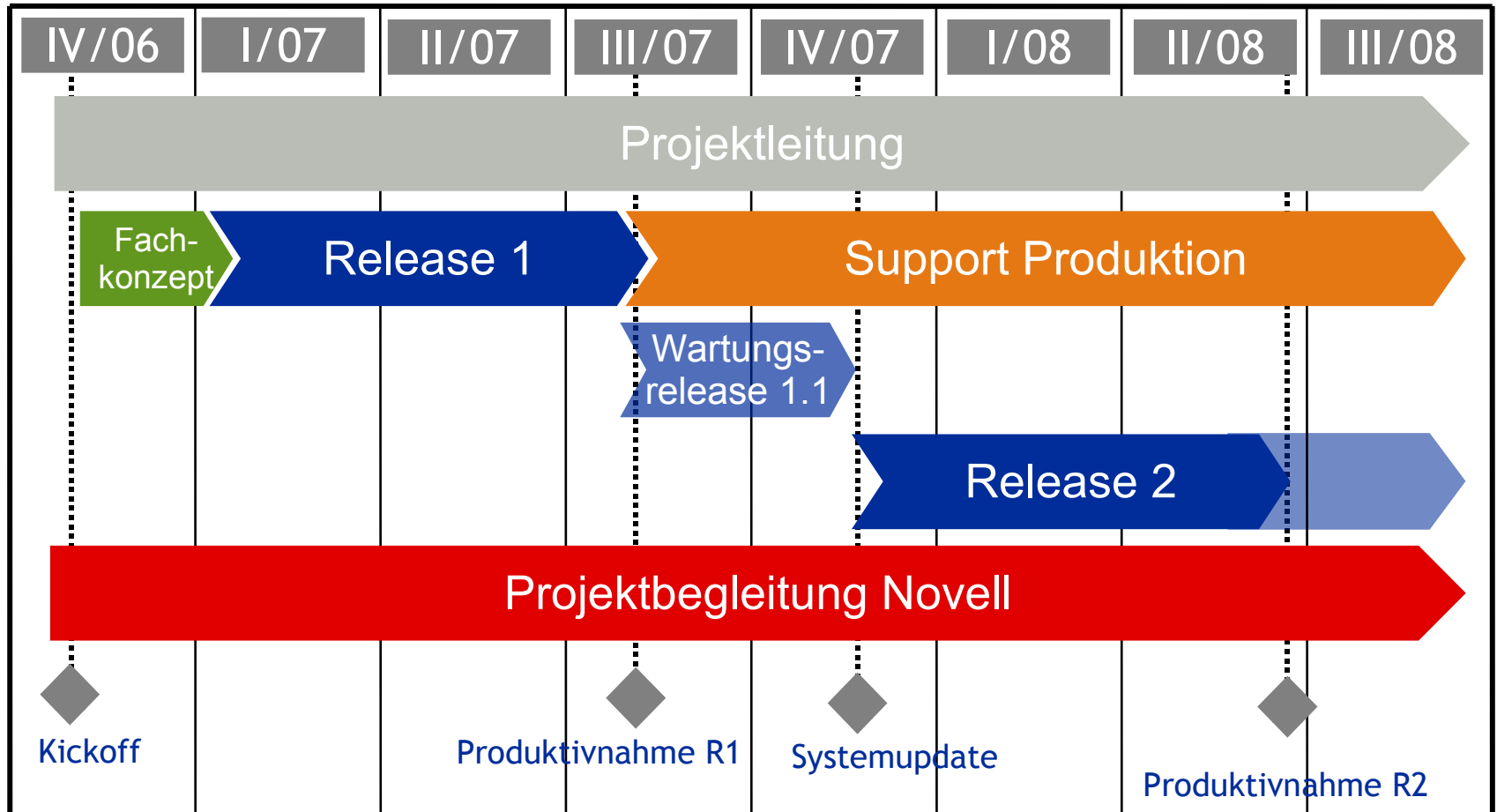
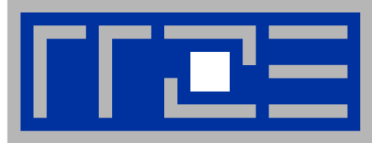
- **Bidirektionale Passwort-Synchronisation**
 - Falls gewünscht kann ein Passwort zwischen verschiedenen Systemen synchronisiert werden

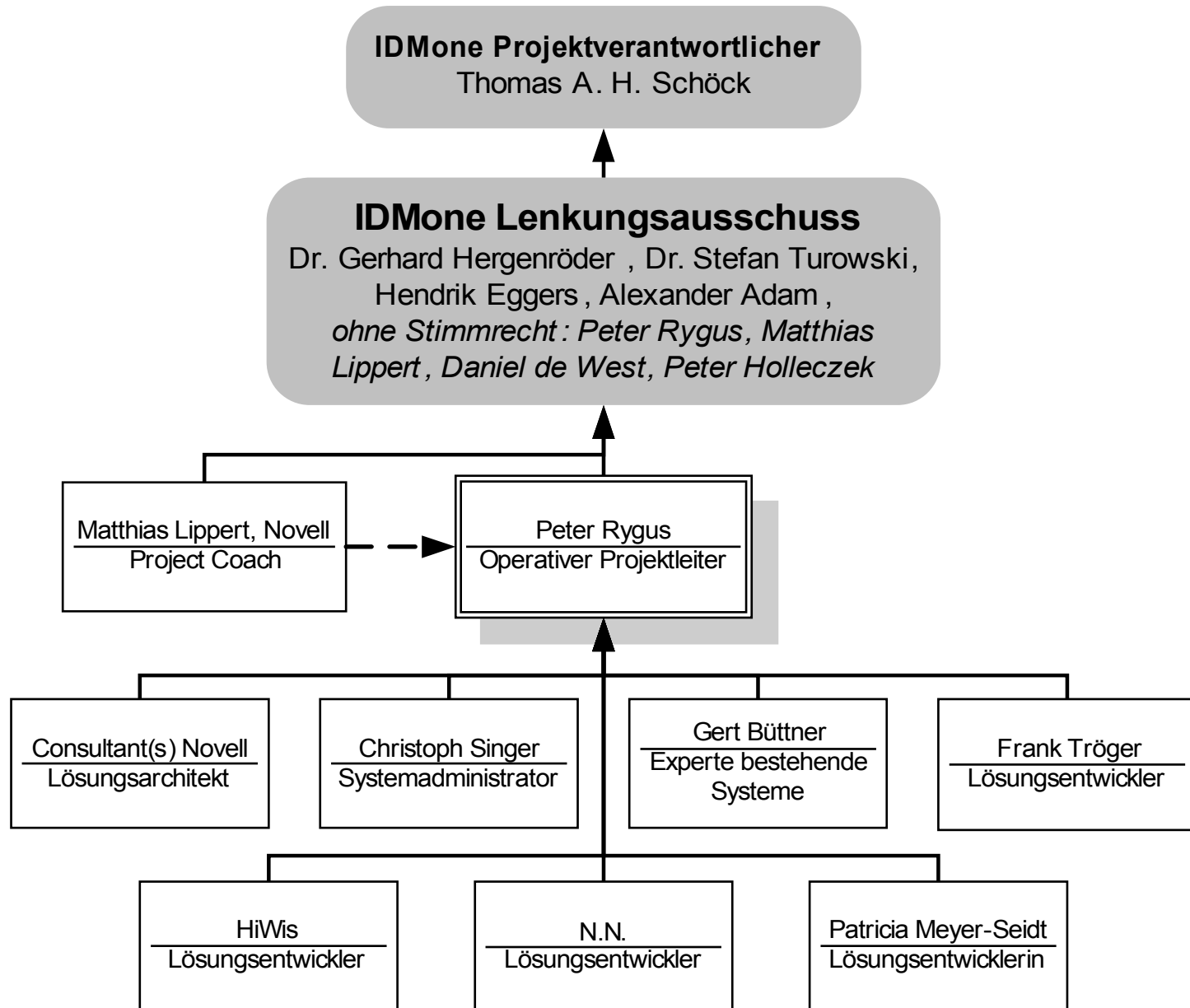
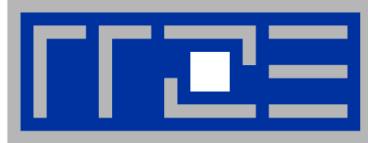


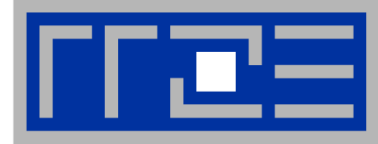


IDMone im Detail

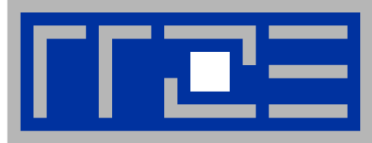
Initialer Zeitplan





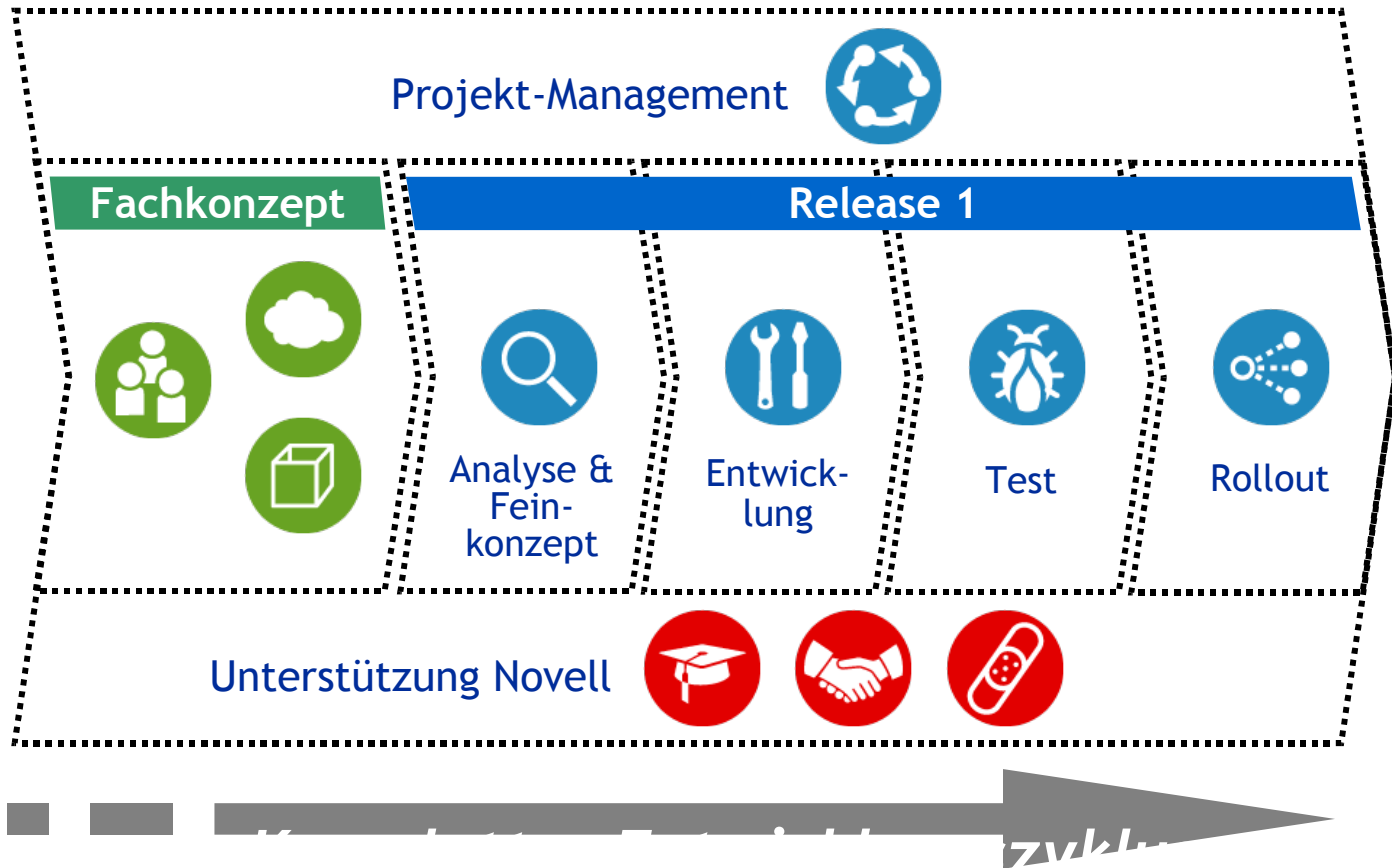


- **Bereitschaft aller Beteiligten, notwendige Veränderungen an Arbeitsabläufen mit zu tragen**
- **Technologie ist kein Allheilmittel => Abläufe müssen sauber definiert und implementiert sein**
- **Release 1 muss bereits spürbaren Nutzen für Endkunden und Administratoren zeigen**



Risiken

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



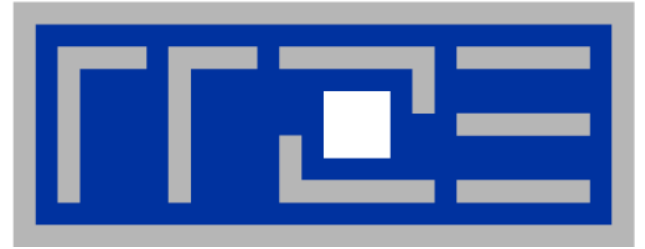
Priorisierung des Projektumfangs



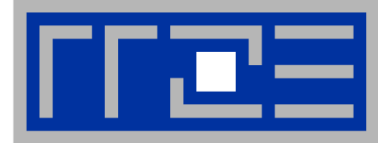
	Zielsystem							
Quellsystem	HIS SOS	UnivIS	SIPORT	SISIS	NDS	CIP	E-Mail	Self Service
A HIS SOS	Manuelle Neuanlage Manuelle Löschung	Neu anlegen Stammdaten ändern Löschen	Neu anlegen Stammdaten ändern Löschen	Neu anlegen Stammdaten ändern Löschen	Neu anlegen Stammdaten ändern Löschen	Neu anlegen Stammdaten ändern Löschen		
	HM/1	HL/1	H/H/1	MM/2	HL/3	ML/2		
B Self Service		Passwort synchronisieren	Passwort synchronisieren		Passwort synchronisieren	Passwort synchronisieren		Initiales Passwort vergeben Passwort manuell rücks.
	HL/1	HM/1	HL/1		ML/2	MH/2		HL/1
C E-Mail	E-Mail-Adresse übernehmen	E-Mail-Adresse übernehmen					E-Mail-Account anlegen, ändern, löschen	E-Mail-Adresse übernehmen
	LM/1	MM/1						



- **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, ...)**

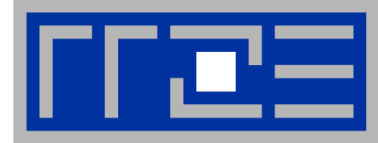


Das IDMone Fachkonzept im Überblick



Benutzergruppen

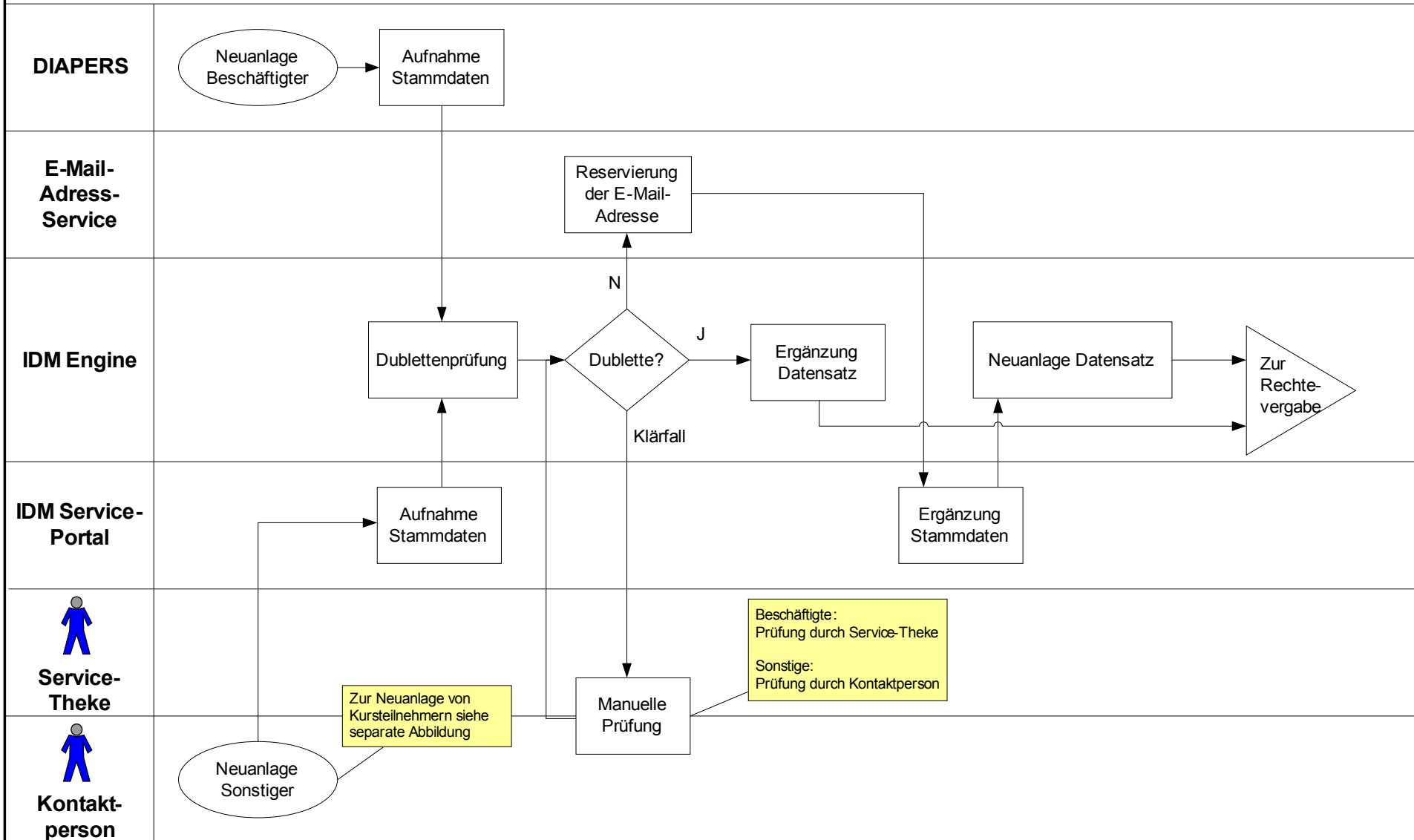
- **Studierende**
- **Beschäftigte**
- **Sonstige**
 - **Gäste aller Art**
 - **Externe**
 - ...
- **Organisationen und Organisationseinheiten**



Prozesse

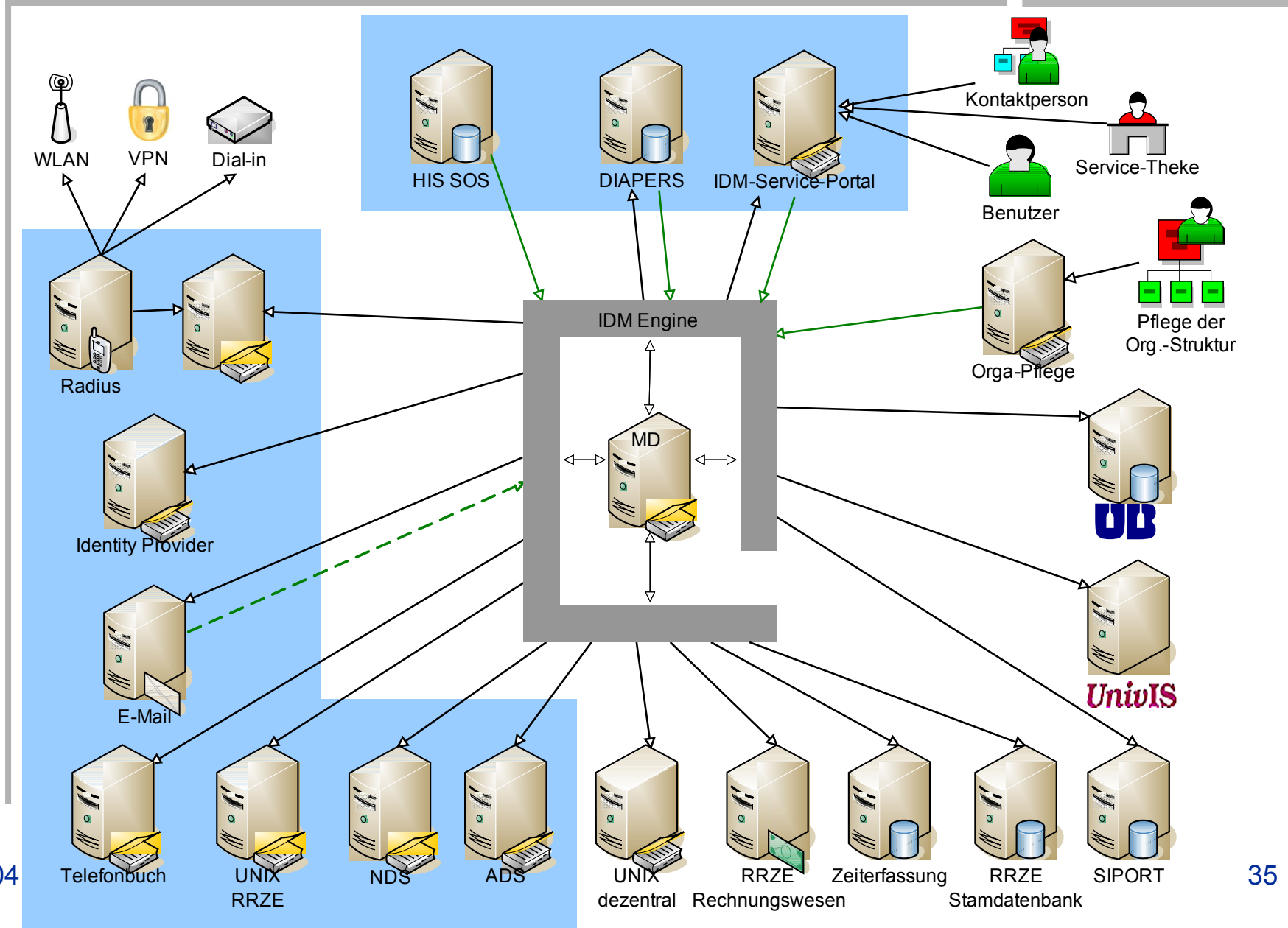
- **Übersicht über die wesentlichen Prozesse der Benutzerverwaltung nach Benutzergruppen dargestellt**
 - **Neuanlage**
 - **Archivieren (kein Löschen im IDM nur ggf. in den Zielsystemen)**
 - **Ermöglichen der Rückkehr an die Universität**
 - **Vermeidung von Kollisionen z.B. bei E-Mail-Adressen**
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

Neuanlage eines Personeneintrages für Beschäftigte und Sonstige

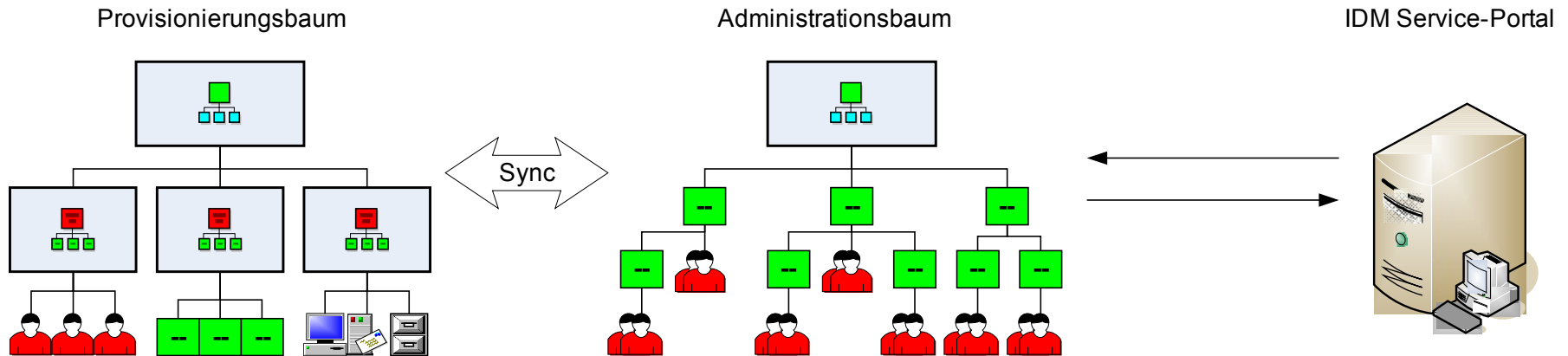




Zielarchitektur

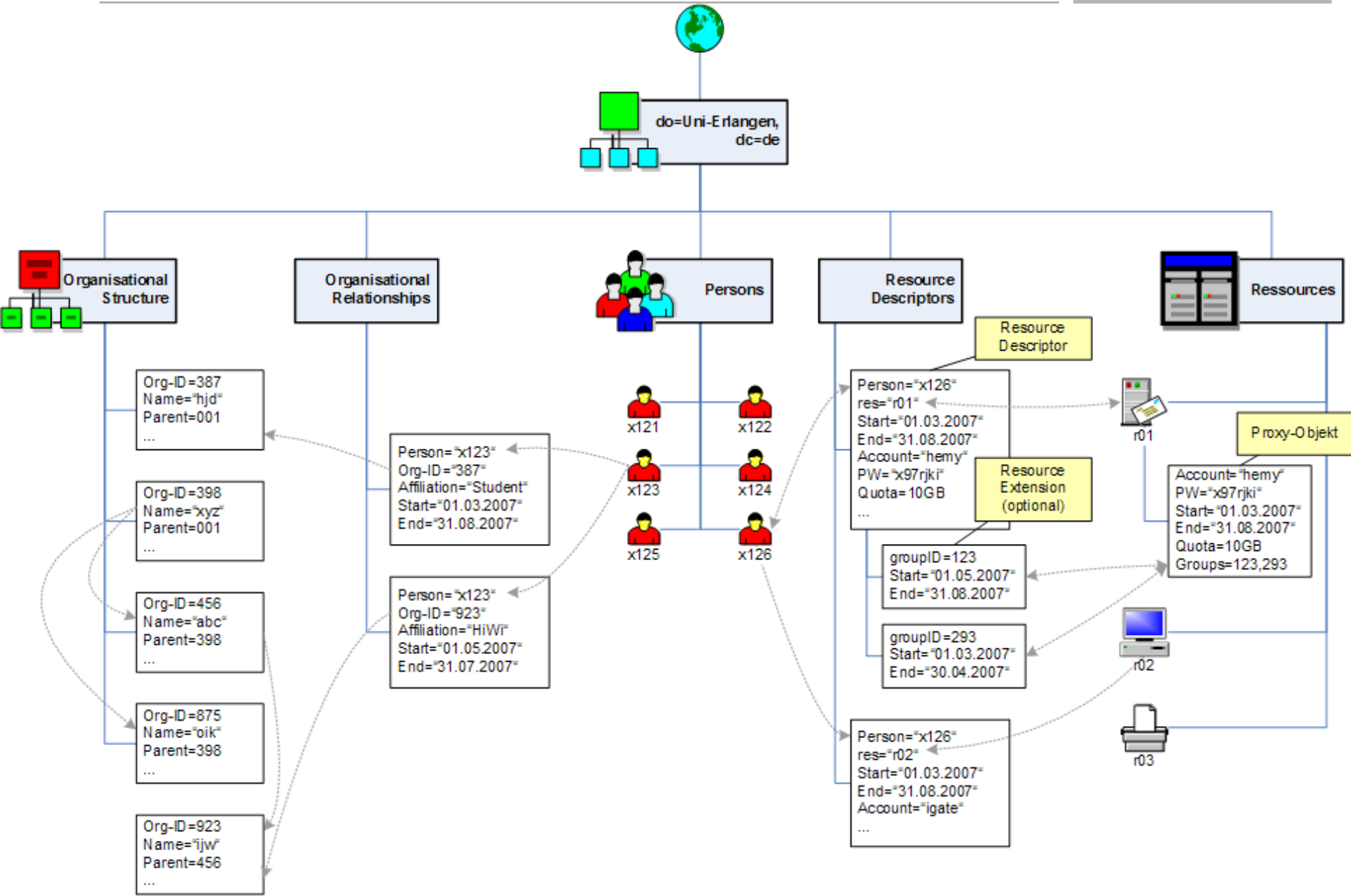


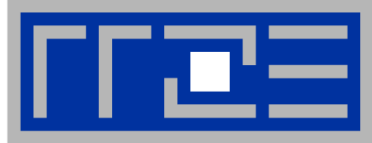
Das hybride Modell



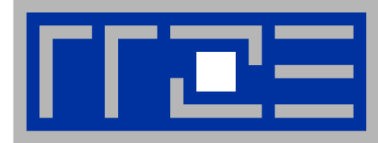


Der Provisionierungsbaum



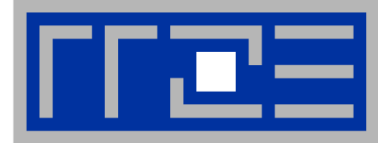


- **Zugehörigkeit einer Person zu einer Organisationseinheit ist wesentliche Basis für die Berechtigungsvergabe**
- **unterschiedliche Nutzer benötigen jeweils unterschiedliche Sichten auf die Organisation**
- **Ausgangsbasis: Gliederungsbescheid**
 - **Nicht ausreichend, da wesentliche Informationen 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

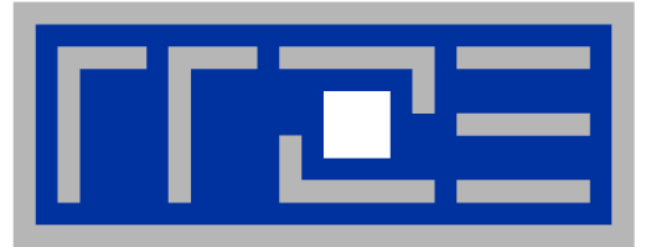


Die neuen Benutzerkennungen

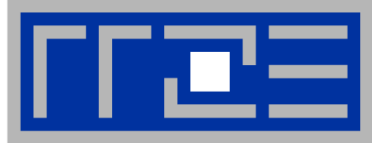
- **semantikkfrei**
- **aussprechbar**
- **8 stellig**

- **Muster {kv|vk}zz{kvkv|vkvk}**
 - **k = Konsonant**
 - **v = Vokal**
 - **zz = Ziffer+andere Ziffer**

- **Beispiele:**
ba23cedi, mi49hopa, hu63pola, no35daxe, ik87napu, um95kite

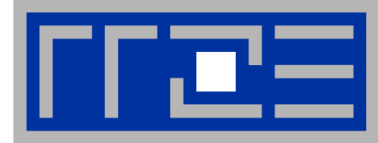


Was kommt im Feinkonzept?



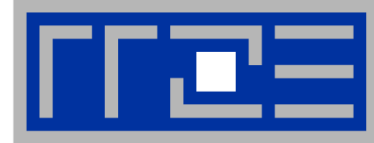
Grundlagen

- **Dienstleistungsportfolio** **15.03.07** **Hendrik Eggers**
- **Zielarchitektur** **15.06.07** **Hendrik Eggers**
- **Geschäftsprozesse** **13.04.07** **Hendrik Eggers**
- **Uses Cases** **26.03.07** **Frank Tröger**
- **Datenautoritäten und Datenflüsse** **15.06.07** **Peter Rygus**
- **Meta-Directory** **02.04.07** **Peter Rygus**
- **E-Mail-Reservierungsservice** **26.03.07** **Frank Tröger**
- **Testkonzept** **19.03.07** **Frank Tröger**
- **Migrationskonzept** **21.05.07** **Gert Büttner**
- **Konsensverfahren Datenschutz** **13.07.07** **Hendrik Eggers**



Zielsysteme

▪ E-Mail-System	26.03.07	Frank Tröger
▪ Administrationsbaum	26.04.07	Peter Rygus
▪ Linux	02.04.07	Frank Tröger
▪ HPC	02.04.07	Frank Tröger
▪ Solaris	02.04.07	Frank Tröger
▪ RADIUS	02.04.07	Frank Tröger
▪ Identity Provider	09.04.07	Florian Hänel
▪ ADS	23.04.07	Frank Tröger
▪ NDS	23.04.07	Novell
▪ RRZE Rechnungswesen	23.04.07	Peter Rygus
▪ Stammdatenbank	30.04.07	Frank Tröger
▪ UnivIS	23.04.07	Peter Rygus
▪ Altsystem	23.05.07	Gert Büttner
▪ Sitebar	07.05.07	Christoph Singer
▪ IDM-Service-Portal	15.03.07	Novell

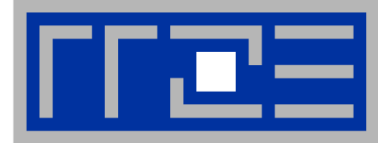


- **01.08.2007** **Roll-Out erster Systeme**
- **30.09.2007** **Zwischenbericht an Staatsministerium**
- **08/2007 – 02/2008** **Phase II**
- **03/2008 – 09/2008** **Phase III**
- **30.09.2008** **Projektabschlußbericht**



Woraus besteht ein Arbeitspaket?

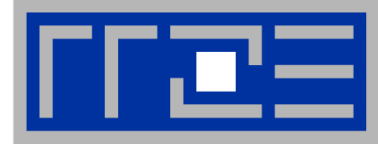
- **Kundengespräch + Gesprächsprotokoll**
- **Umfangsdefinition - Was soll laufen?**
 - Was wurde diskutiert?
 - Zu welchen Ergebnissen ist man gekommen und warum?
- **Konzept gemäß Novell-Vorlage im Wiki**
- **Treiber-Konfiguration**
 - Pilotierung
 - Umsetzung im Entwicklungssystem
- **Beispiel System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



- **Ende des „Brütens“**
- **Beteiligung der maßgeblichen Akteure / Fachanwendungsbetreuer**
- **Berichte über den aktuellen Stand**
- **Anregungen für die laufende und zukünftige Arbeit**

- **Monatlich immer Dienstags sofort nach der DB**

- **Erstmals am 08.05.2007**



WebSSO

- **Technische Vorarbeiten werden durch Florian Hänel (HiWi) unter der Anleitung von Peter Rygus geleistet**
- **Vorbereitende Maßnahmen für Produktivbetrieb durch Webmaster notwendig und ausstehend**
- **Beginn Anfang Mai**
- **erste Dienste sollen Ende Mai zur Verfügung stehen**

- **Praxisbeispiel WebSSO**

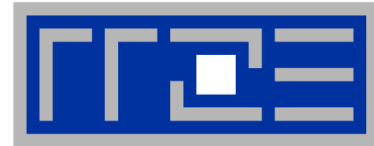


Links

- **öffentliche Webseite von IDMone**
- **Fachkonzept**
- **Novell Identity Manager**



**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



**Regionales
RechenZentrum
Erlangen**

Der IT-Dienstleister der FAU

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

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)