

Status IDMone

11.10.2007

**Sitzung ZKI Arbeitskreis Verzeichnisdienste,
Universität Hamburg**

Hendrik Eggers



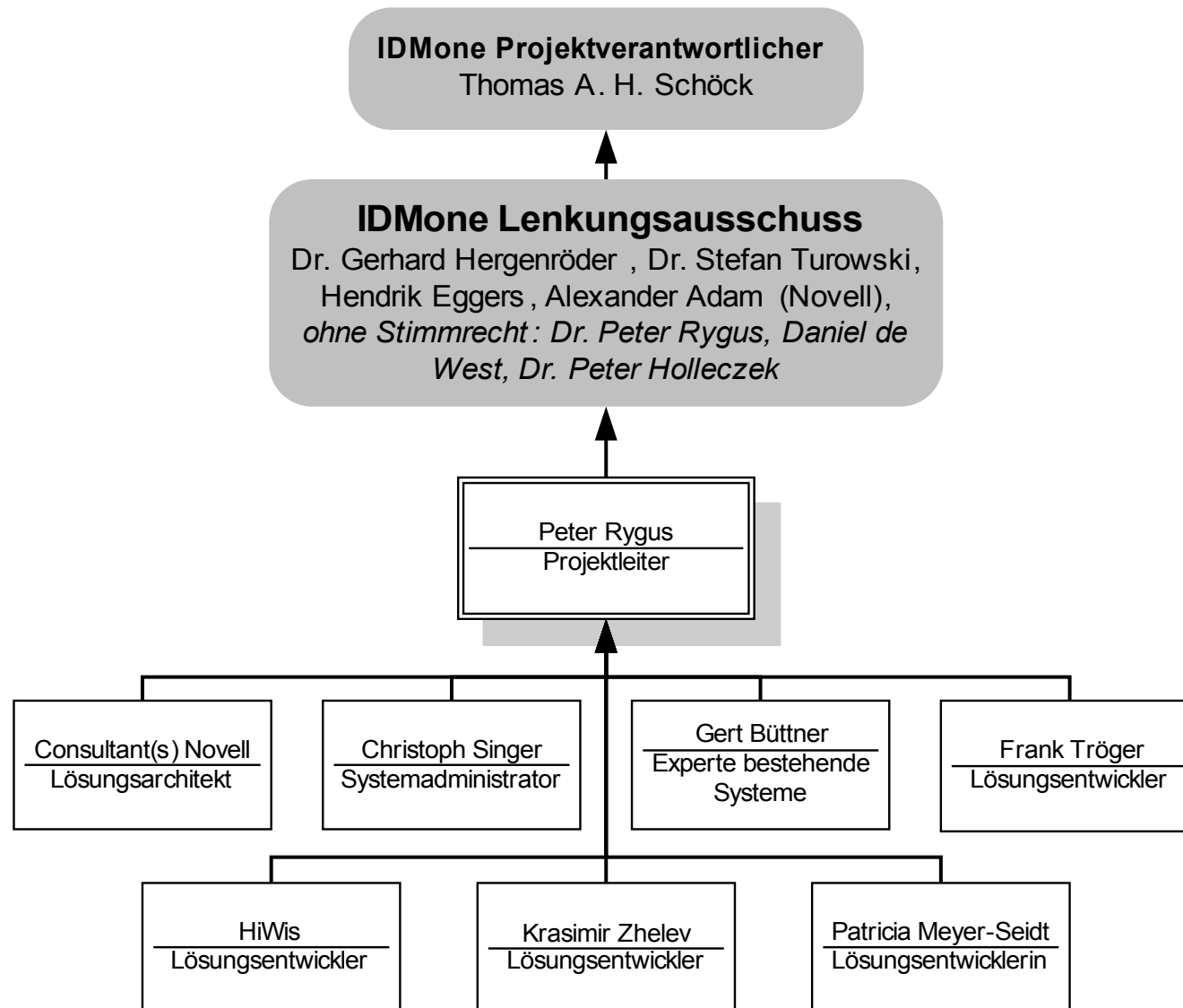
- **26.000 Studierende, 6.000 Beschäftigte, 10.000 Gäste pro Jahr**
- **Seit 1991 selbst entwickelte, gewachsene Benutzerverwaltung am RRZE**
- **Ca. 15 zentrale und x dezentrale Systeme, die mit Stammdaten arbeiten**
- **Keine globale Sicht auf Identitäten**
- **Manuelle Erfassung inhaltsgleicher Daten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

Anforderungen an IDMone

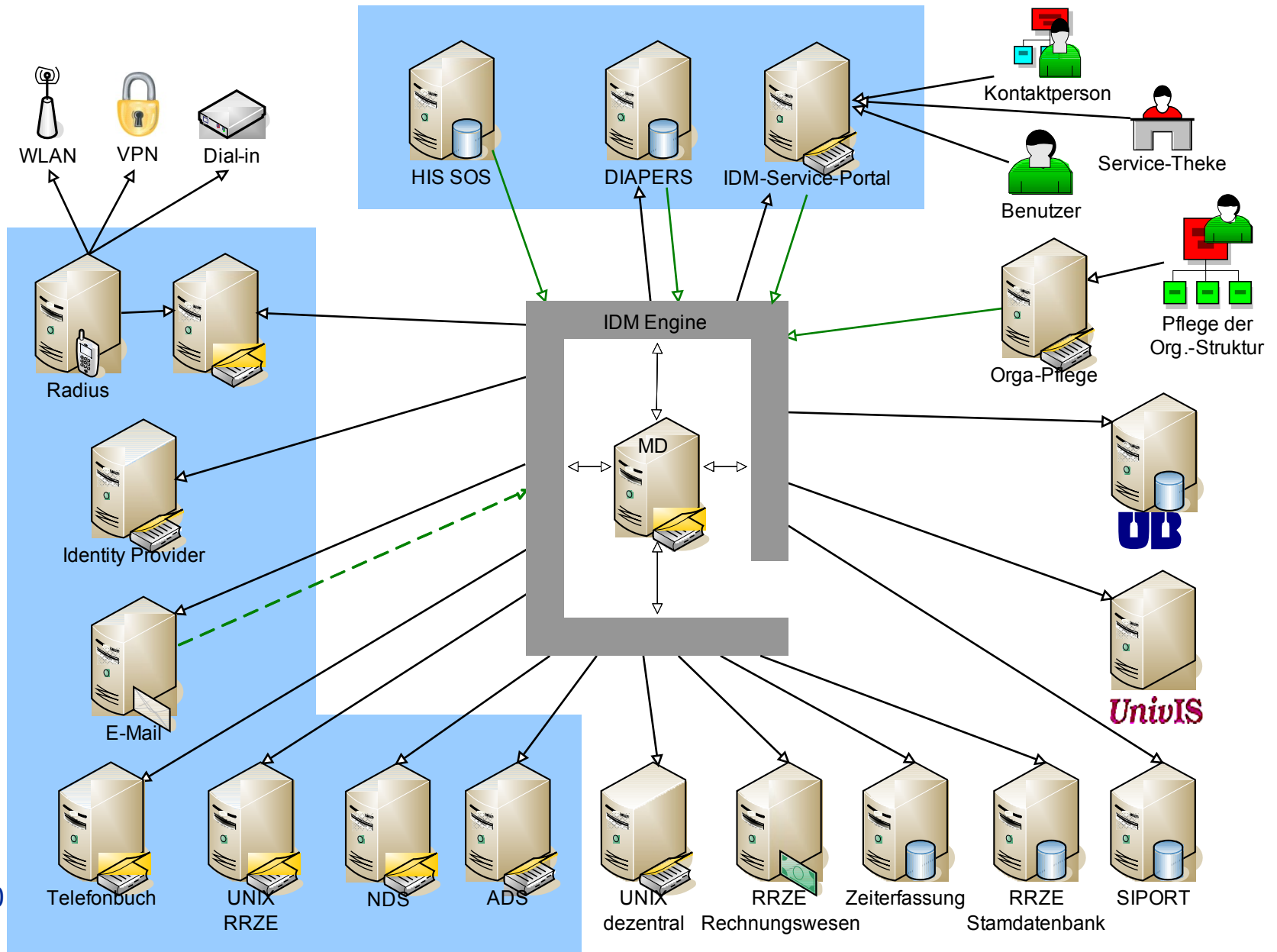
- **Personenorientiert**
- **Mehrere Beschäftigungsverhältnisse pro Person**
- **Mehrere Accounts pro Person, Beschäftigungsverhältnis und Zielsystem sind möglich**
- **Eine Person ändert häufig sein Beschäftigungsverhältnis**
- **Es gibt eine hohe Fluktuation in der Organisationsstruktur**
- **Das RRZE rechnet seine Dienstleistungen ab**
 - **mehrere 'Geldgeber' pro Ressource müssen möglich sein.**
- **Es muss möglich sein, Ressourcen hinzuzufügen und wegzunehmen**

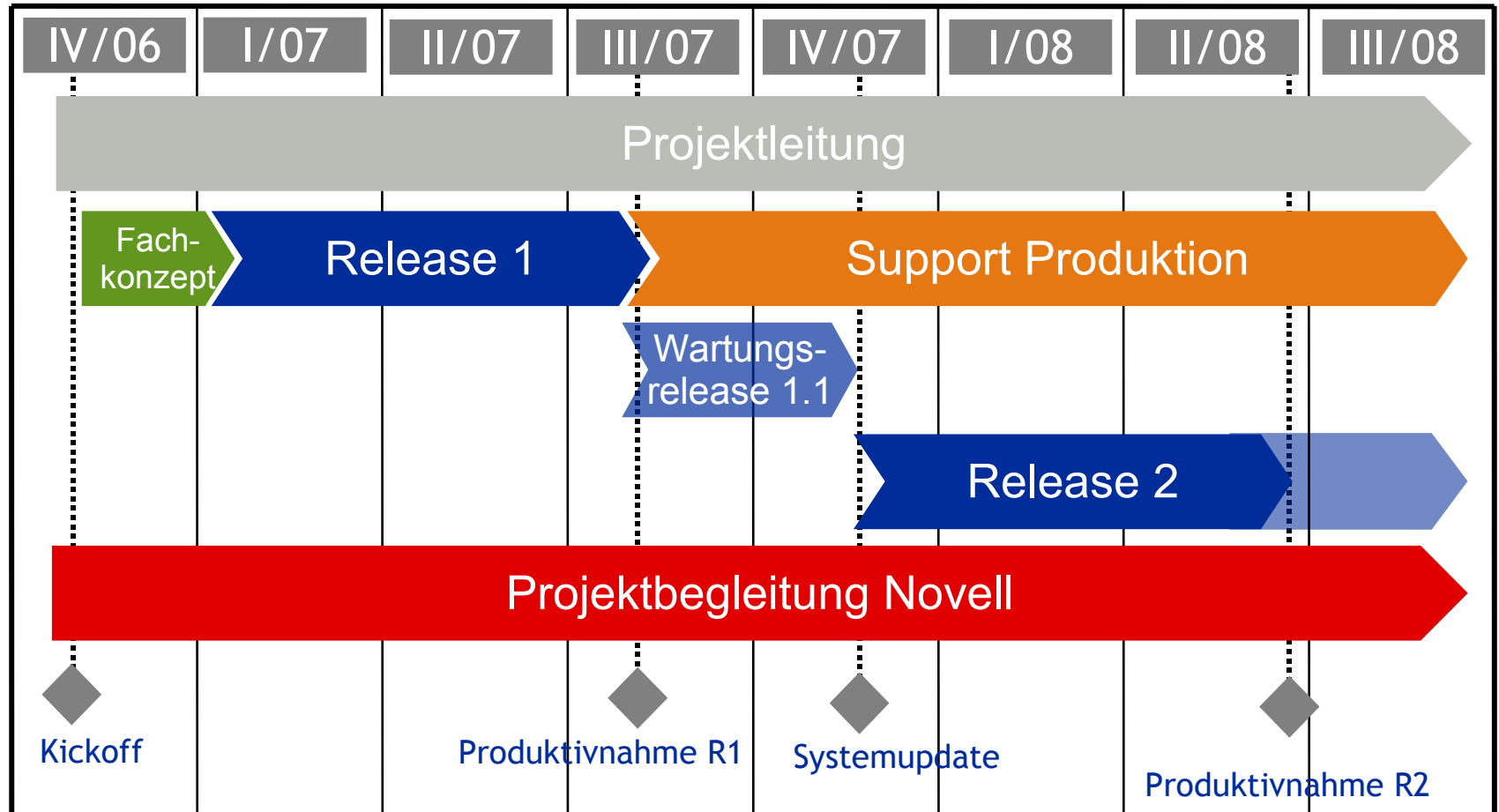
Anforderungen an IDMone II

- **Der Aufbau des Meta-Directory sollte möglichst nah am gewählten Produkt orientiert sein, um es optimal auszunutzen**
- **Durch geeignete Doku soll Transparenz geschaffen werden**
- **Der Aufbau des Meta-Directory darf die Flexibilität nicht einschränken**
- **Das System sollte modular aufgebaut sein um Updates ohne Einwirkung auf andere Dienste zu ermöglichen**
- **Das System sollte die Administration unterstützen, d.h. es sollte ein 'selbstheilendes' System sein, das Fehler reparieren kann und Karteileichen verhindert.**

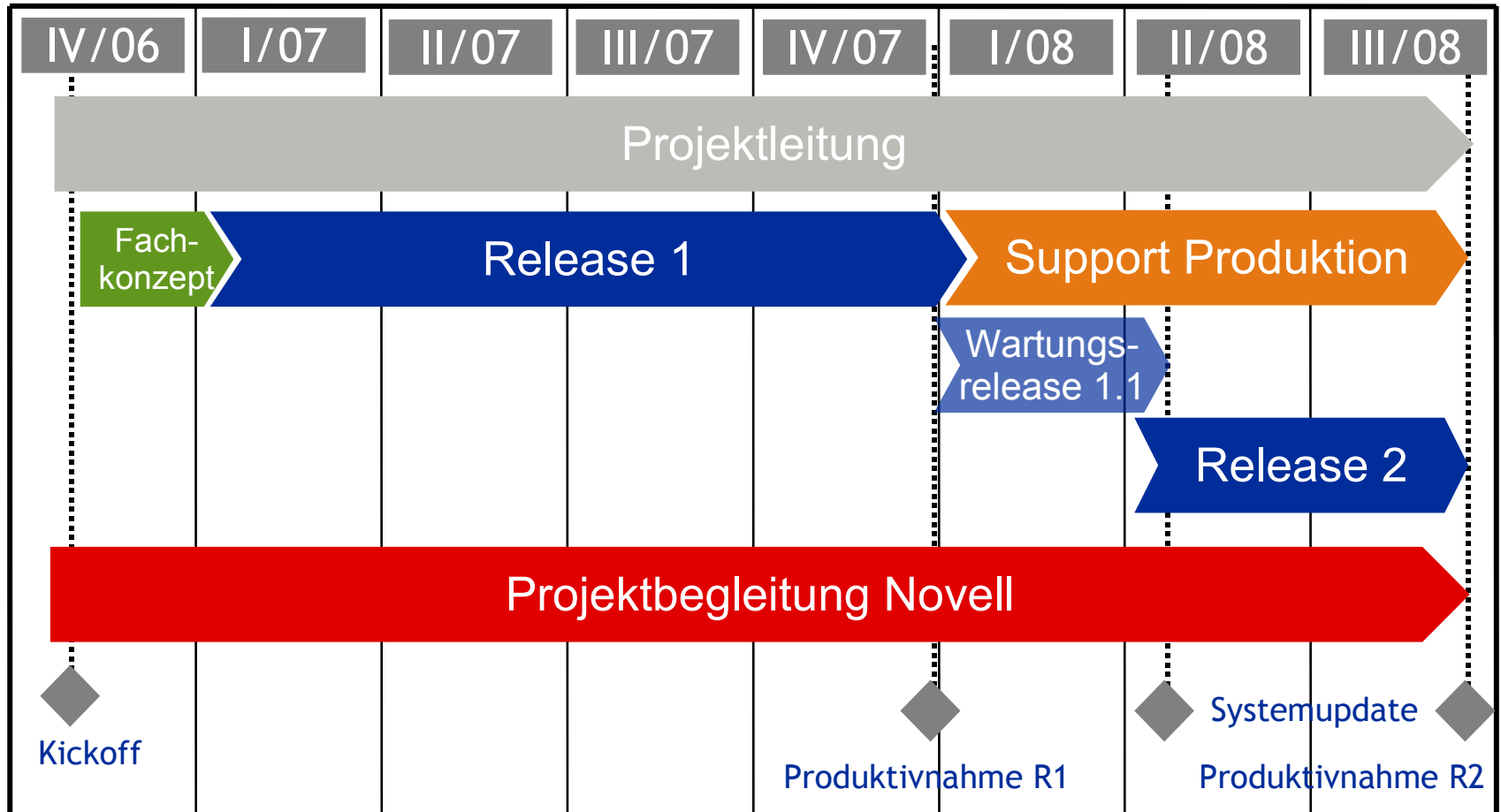


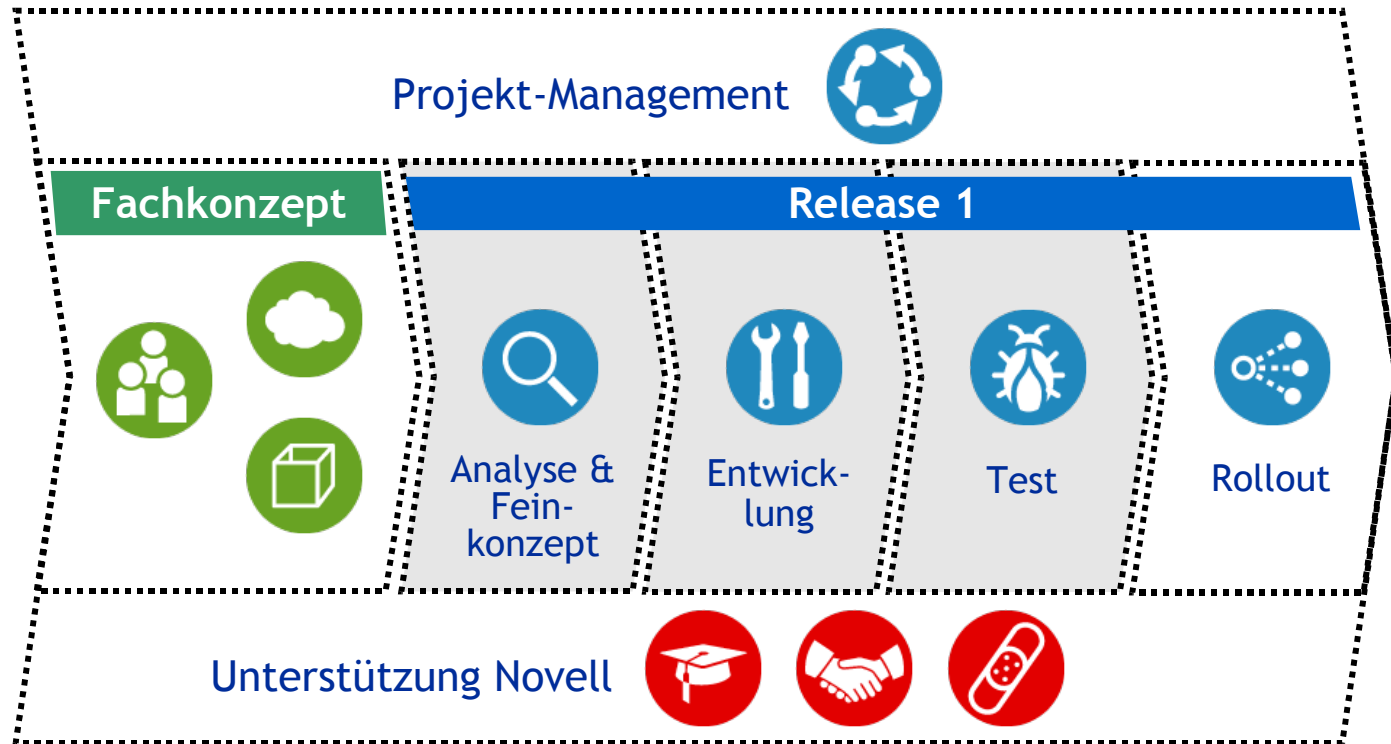
Zielarchitektur





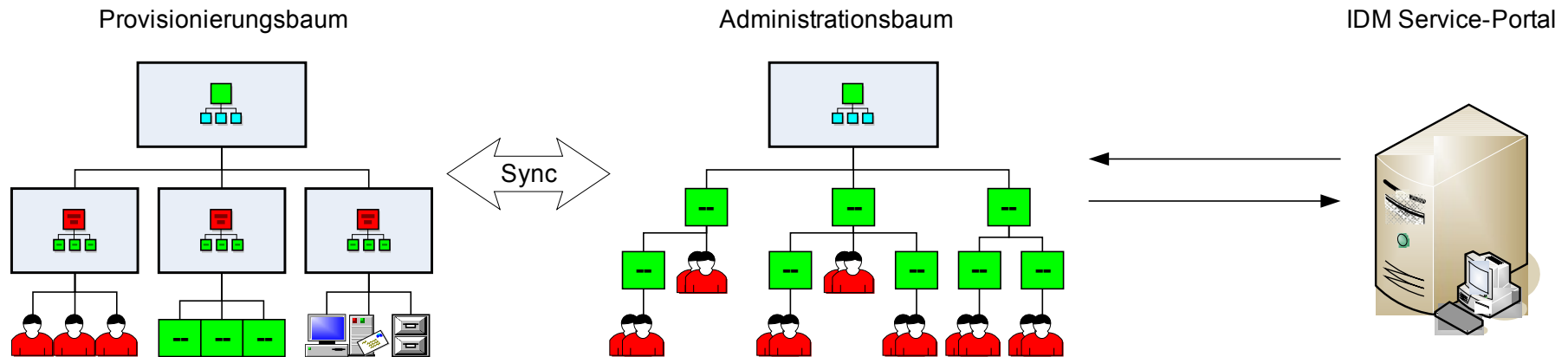
Korrigierter Zeitplan



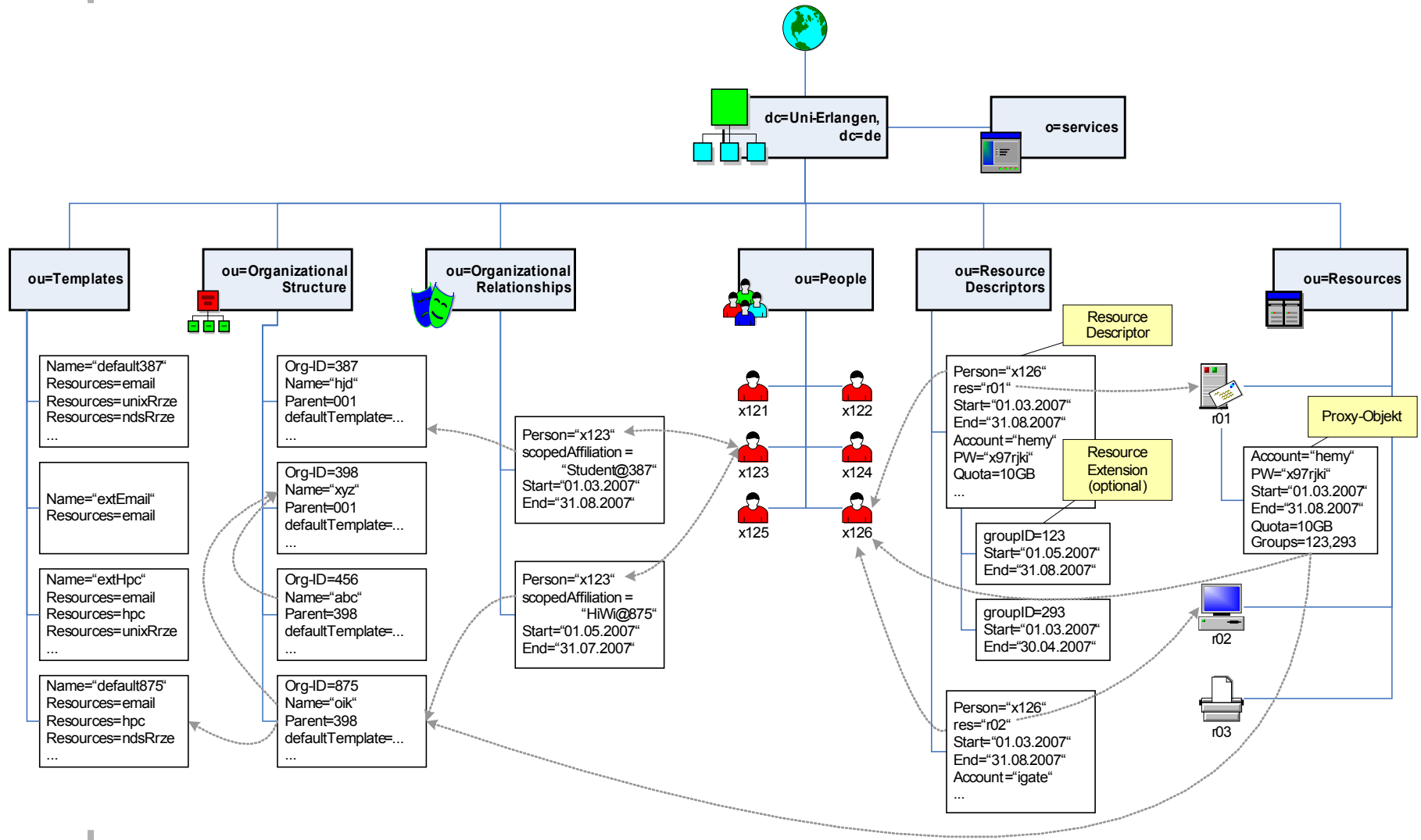


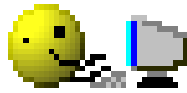
Kompletter Entwicklungszyklus

Das hybride Modell



Der Provisionierungsbaum

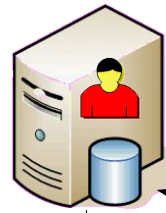




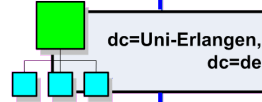
Admin

1

13



2



7

12

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"

x121

x122

x125

x126

newbie

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



UserApp

Proxy-Objekt



res=hpc

1

13

2

7

12

3

4

5

6

8

11

9

10

Aktuelle Showstopper

- **Fehlende zentrale Pflege der Organisationsstruktur**
- **Dienstleistungskatalog erst im Aufbau begriffen**
- **Spät gewonnene Erkenntnis, wie die Software intern funktioniert**
- **Hohe Ansprüche im Bezug auf das Zusammenspiel der Treiber und Objekte im Meta-Directory**



- **31.10.2007** **Fertigstellung des ersten Testsystems mit einem Quell- und zwei Zielsystemen**
- **01.12.2007** **Zwischenbericht an Staatsministerium**
- **09/2007 – 02/2008** **Anbindung und Test aller im Release 1 enthaltenen Systeme**
- **02/2008** **Roll-Out von Release 1**
- **02/2008 – 09/2008** **Release 2**
- **30.09.2008** **Projektabschlußbericht**

Kooperationsangebot

- **Partner für Open Source Referenz Implementierung**
 - **Verwendung von Open Source Komponenten, z.B.**
 - **Apache DS – <http://directory.apache.org/>**
 - **OpenLDAP**
 - **JBoss Portal – <http://www.jboss.org/products/jbossportal>**
 - **Wissensaustausch**
 - **Wiki-Zugriff**
 - **Schulung neuer MA**
 - **Regelmäßiger Austausch per VC**

Links

- **IDMone Webseite**
<http://www.rrze.uni-erlangen.de/forschung/laufende-projekte/idm.shtml>
- **IDMone Blog**
<http://www.blogs.uni-erlangen.de/IDM/>
- **IDMone im P&P Wiki**
https://www.pp.wiki.uni-erlangen.de/index.php/Grundlagen_IDMone
https://www.pp.wiki.uni-erlangen.de/index.php/Grundlagen_IDM_Service_Portal
https://www.pp.wiki.uni-erlangen.de/index.php/Use_Cases

**Vielen Dank für Ihre
Aufmerksamkeit!**



Dr. Peter Rygus

Projektleiter Identity Management

RRZE Martensstrasse 1

D-91058 Erlangen

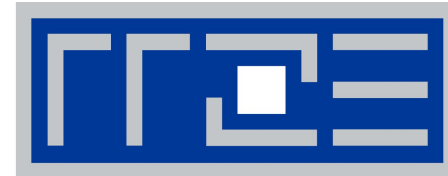
Tel.: +49 9131 85-28899

Fax: +49 9131 302941

peter.rygus@rrze.uni-erlangen.de

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

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)



Regionales
RechenZentrum
Erlangen

Der IT-Dienstleister der FAU

Dipl.-Kfm.

Hendrik Eggers

Leiter Stabstelle Projekte & Prozesse

RRZE ■ Martensstraße 1

91058 Erlangen

Tel.: +49 9131 85-27819

Mobil: +49-170-6219877

Fax: +49 9131 302941

hendrik.eggars@rrze.uni-erlangen.de



**Regionales
RechenZentrum
Erlangen**

Der IT-Dienstleister der FAU

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

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)