IdM an der Uni Erlangen: IDMone

ZKI AK Verzeichnisdienste, Aachen
Dr. Peter Rygus
26.02.2009

Friedrich-Alexander-Universität
Erlangen-Nürnberg

Die Universität Erlangen-Nürnberg

Kennzahlen

Zweitgrößte Universität in Bayern

25.855 Studenten
> 12.000 Mitarbeiter
5 Fakultäten
22 Departments / Fachbereiche
24 Kliniken
265 Lehrstühle (C4 / W3)
132 Studienfächer

250 Gebäude in 140 Gebäudegruppen in 4 Städten und das Wassersportzentrum bei Pleinfeld

Die „multilokalste“ Universität Deutschlands

Stand: WS 07/08

Die Universität Erlangen-Nürnberg

Ausrichtung

- breitestes Fächerangebot Deutschlands durch Bologna
- Konzept der „multilokalen vernetzten Breite“
- Einsatz moderner Medien
- Verteilte Vorlesungen, Übertragungen Hörsaal, Uni-TV, ...

Ausgangsituation IDMone

- 26.000 Studierende, 6.000 Beschäftigte, 10.000 Gäste pro Jahr
- Seit 1991 selbst entwickelte, gewachsene Benutzerverwaltung am RRZE (ca. 260 Scripte …)
- 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
- Prozessorientiert

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 System sein, das Fehler reparieren kann und Karteileichen verhindert.

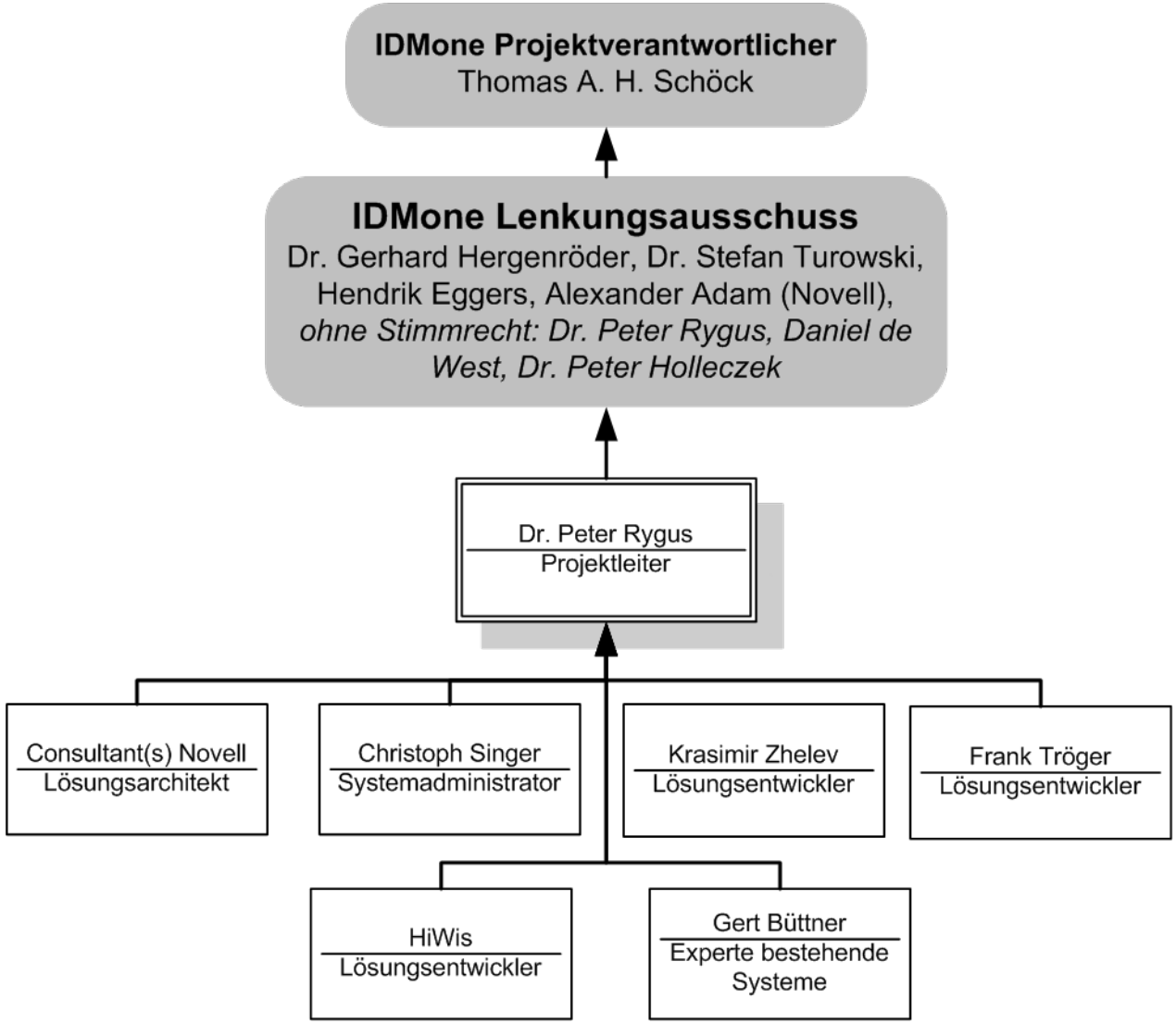
Ziele

- **Inbetriebnahme einer zentralen Identitätsverwaltung**
- **Automatisierte Bereitstellung von Basis-Dienstleistungen für alle Mitglieder der Universität**
- **Web-basierende Self-Service- und Administrationsoberfläche**
- **Bereitstellung von Schnittstellen für dezentrale Systeme (Authentifizierung (SSO) / Datenaustausch)**
- **Schaffung eines generischen IDM-Konzepts für das RRZE und andere Hochschulen**

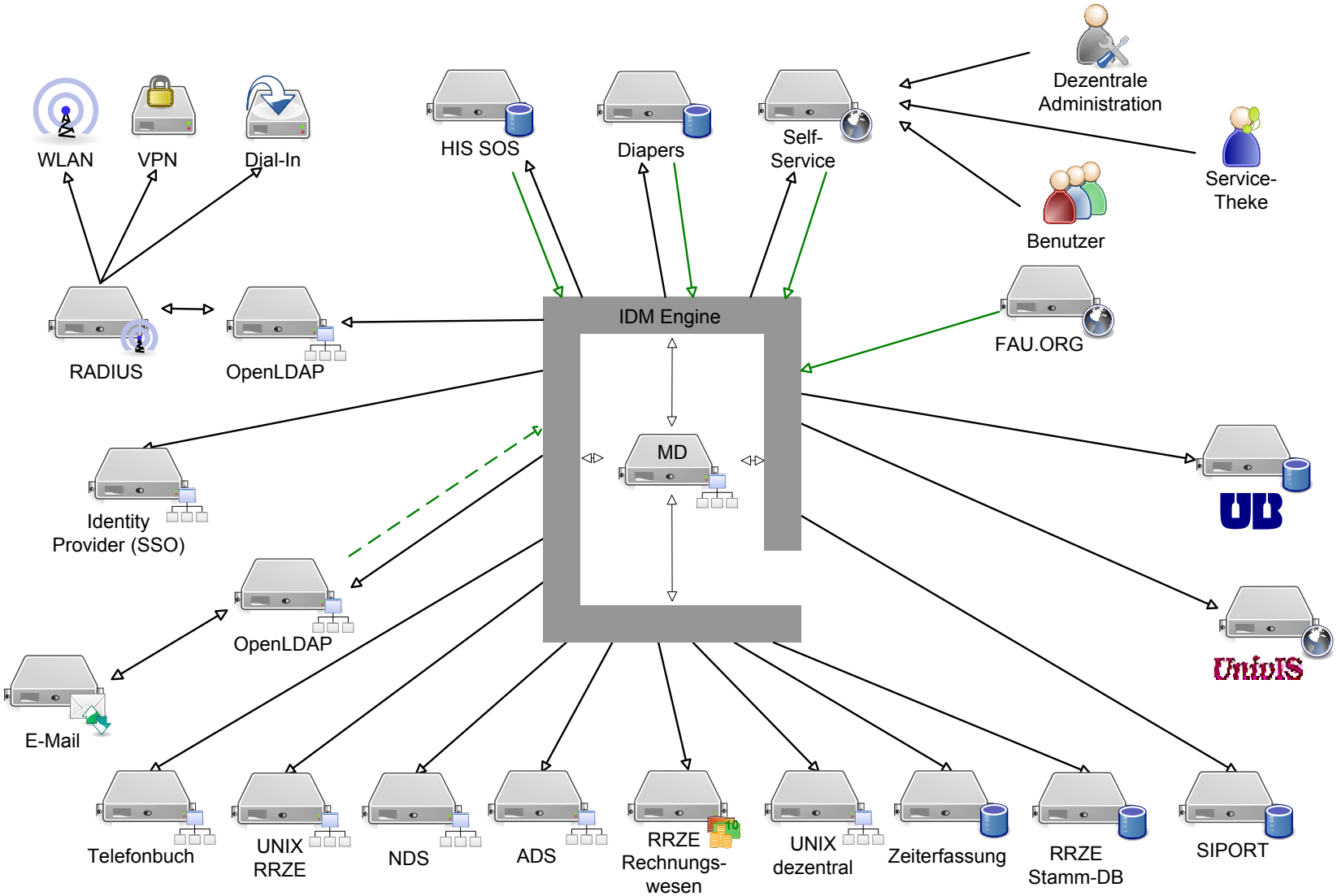
Projekt IDMone

- Zielvereinbarung der Universität Erlangen-Nürnberg mit dem StMWFK ermöglicht das Projekt IDMone
- Projektstart: 01.11.2006
- Projektlaufzeit: 2 Jahre
- Probleme:
  - Personelle Ausstattung
  - Späte Vervollständigung des Teams

Organigramm IDMone



Zielarchitektur



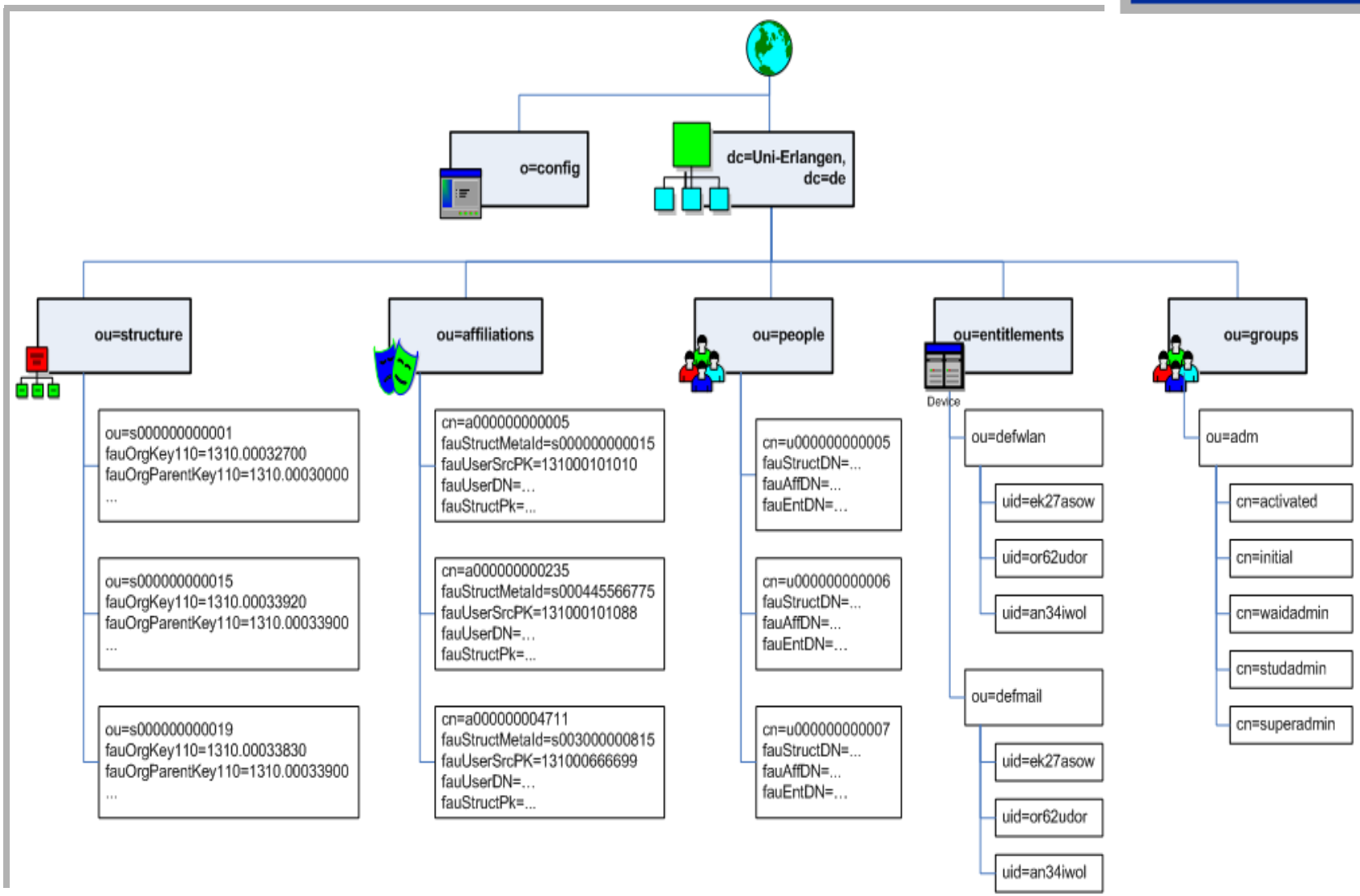
Aufbau des Meta-Directory

- Es existieren subtrees für die Organisationsstruktur (ou=structure), Personen (ou=people), Beschäftigungsverhältnisse (ou=affiliations), Rechte (ou=entitlements) und Gruppen (ou=groups)
- Die Objekte darunter werden flach abgelegt
- Ausnahme: Rechte werden nach Zielsystemen gruppiert
- Für jede Person existiert ein Eintrag im subtree ou=people
- Jede Person hat beliebig viele Beschäftigungsverhältnise
- Einträge unter ou=people und ou=affiliations sind dopelt verlinkt
- Jedes Beschäftigungsverhältnis hat einen Zeiger auf eine Organisationseinheit
- Für jede Organisationseinheit existiert ein Eintrag im subtree ou=structure

Aufbau des Meta-Directory (2)

- Jede Person hat beliebig viele Rechte (accounts, quota, …)
- Rechte werden im subtree ou=entitlements abgelegt
- Einträge für Personen und Rechte sind dopelt verlinkt
- Einträge für Rechte haben einen Zeiger auf ein Beschäftigungsverhältnis (Ausnahmen: direkte Rechte der Person)
- Es gibt eine logische Hierarchie in den Rechten
  - Realisiert durch Objektklassen und Attribute (Zeiger)
- Gruppen dienen zur Vergabe von Zugriffsrechten im Web-Frontend (WAID)
- Vorbereitung auf die Verwendung von ‚nested groups‘

Aufbau des Meta-Directory (3)



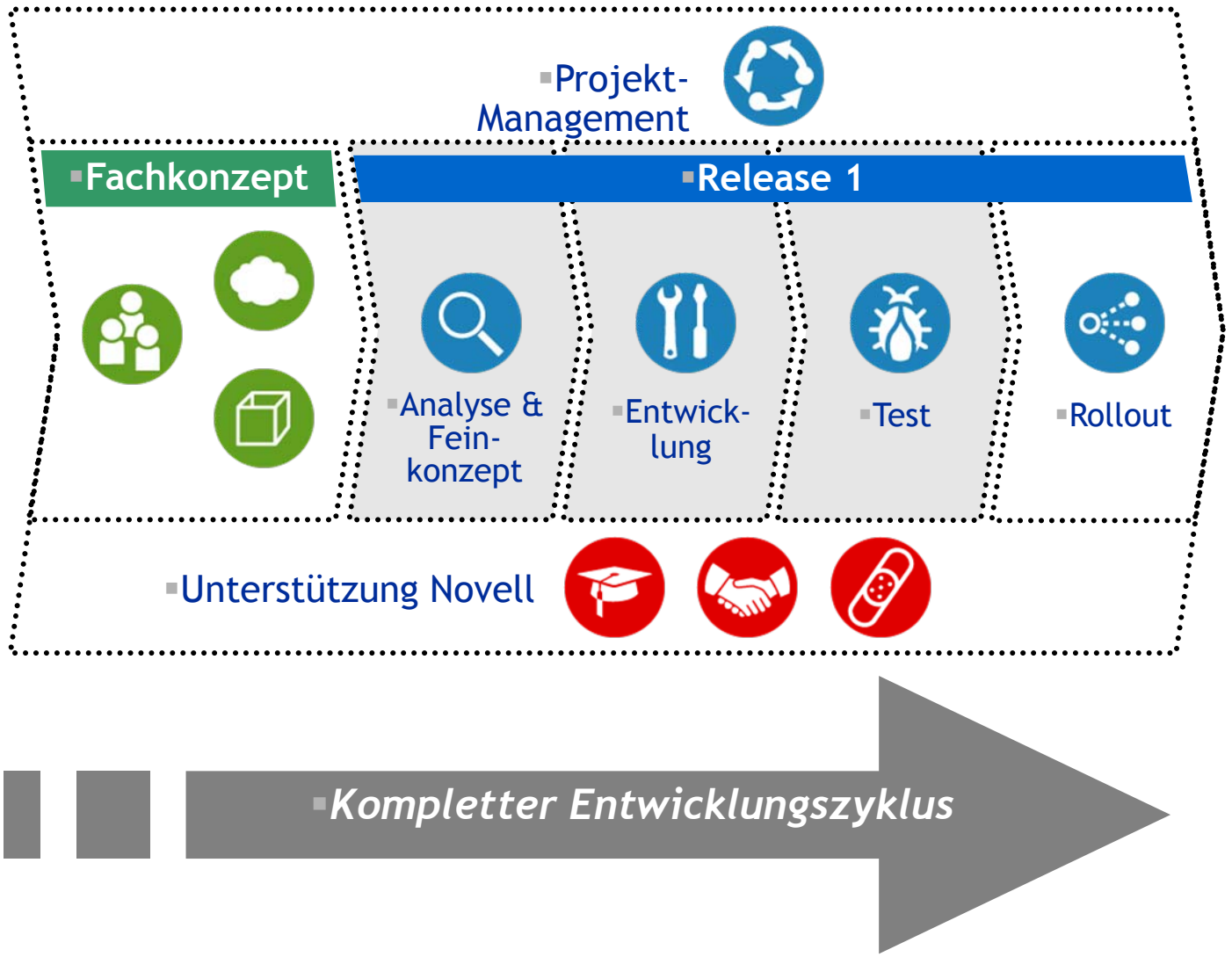
Konzept

- Jede Person erhält eine semantikfreie Benutzerkennung
- Bestandskennungen werden übernommen
- Benutzerkennungen werden unbefristet vergeben und nie wiederverwendet
- Diese Kennung soll für möglichst viele Dienste genutzt werden
- Das Passwort für die mit dieser Kennung provisionierten Dienste (Zielsysteme) wird synchronisiert
- Jede Person kann beliebig viele unabhängige Kennungen haben
- Die Passwörter dieser Kennungen werden getrennt verwaltet
- Mit jeder dieser Kennungen können beliebig viele Dienste provisioniert werden

Konzept (2)

- Rechte können additiv (z.B. quota) oder exklusiv vergeben werden (z.B. default WLAN)
- Dezentrale Administration wird über Gruppen ermöglicht
- (Noch) keine Rollen
- Objekte für die Organisationsstruktur, Beschäftigungsverhältnisse und Personen erhalten eindeutige, unbefristet vergebene Ids
- Diese Objekte werden nie gelöscht, sondern nur Datenreduziert und verschoben

Vorgehensweise



Bausteine

- Verwendung von PRINCE2
- Regeln
  - Team-
  - Dateiablage
  - Konventionen für Dateinamen
- Berichtswesen mittels Blog
  - Wochen-
  - Arbeits-
  - Reise-
  - Risikomanagement mittels bugzilla
- Tools
- Weiche Faktoren
  - Team-Normung
  - Kick-Off-Meeting
  - Eskalationsaussprachen
  - Schnittstellen- / Stakeholder-Analyse
- Evolutionäre Entwicklung

Stärken & Schwächen von PRINCE2

- kann falsch angewendet werden
- Gefahr des Selbstzwecks
- Stark dokumenten-orientiert
  RE muss selbst gestaltet werden
- anpassbar
- „Management by Exception“ bietet Freiheit für Projektleiter
- Öffentlich verfügbar
- Strukturen und Vorlagen

Tools im Details

- Ideensammlung mittels Mind Map in freemind
- Projektplanung mittels GanttProject
- Entwicklungsumgebung Eclipse
- OpenOffice.org
- Microsoft Visio (wo es sich nicht vermeiden lässt)
  - eigenes Icon-Set
- Prozessmodellierung mittels BPMN (Agilian + Eclipse)
- Media Wiki als zentrale Informationssammlung
- Datenablage mittels Versionsverwaltung subversion
- Zentrales Help Desk System OTRS für Außenkommunikation

Status

- IDMone wurde als Projekt beendet
  - Übergang in den Regelbetrieb
  - Trennung von Kapazitäten für Entwicklung und Betrieb
- Funktionsumfang noch gering
  - Provisionierung der studentischen Prüfungsverwaltung („Mein Campus“)
  - Provisionierung der bestehenden RRZE Benutzerverwaltung
    - Ablösung der Importe aus HIS SOS
    - Lieferung der Mitarbeiterdaten aus DIAPERS
    - Übergabe der Daten aus WAID
  - User Self Service via WAID
  - Admin Service via WAID
- Noch kein vollständiger Datenbestand
- Handarbeit zur Zuordnung („Branding“) nötig
  - Soll durch WAID unterstützt werden

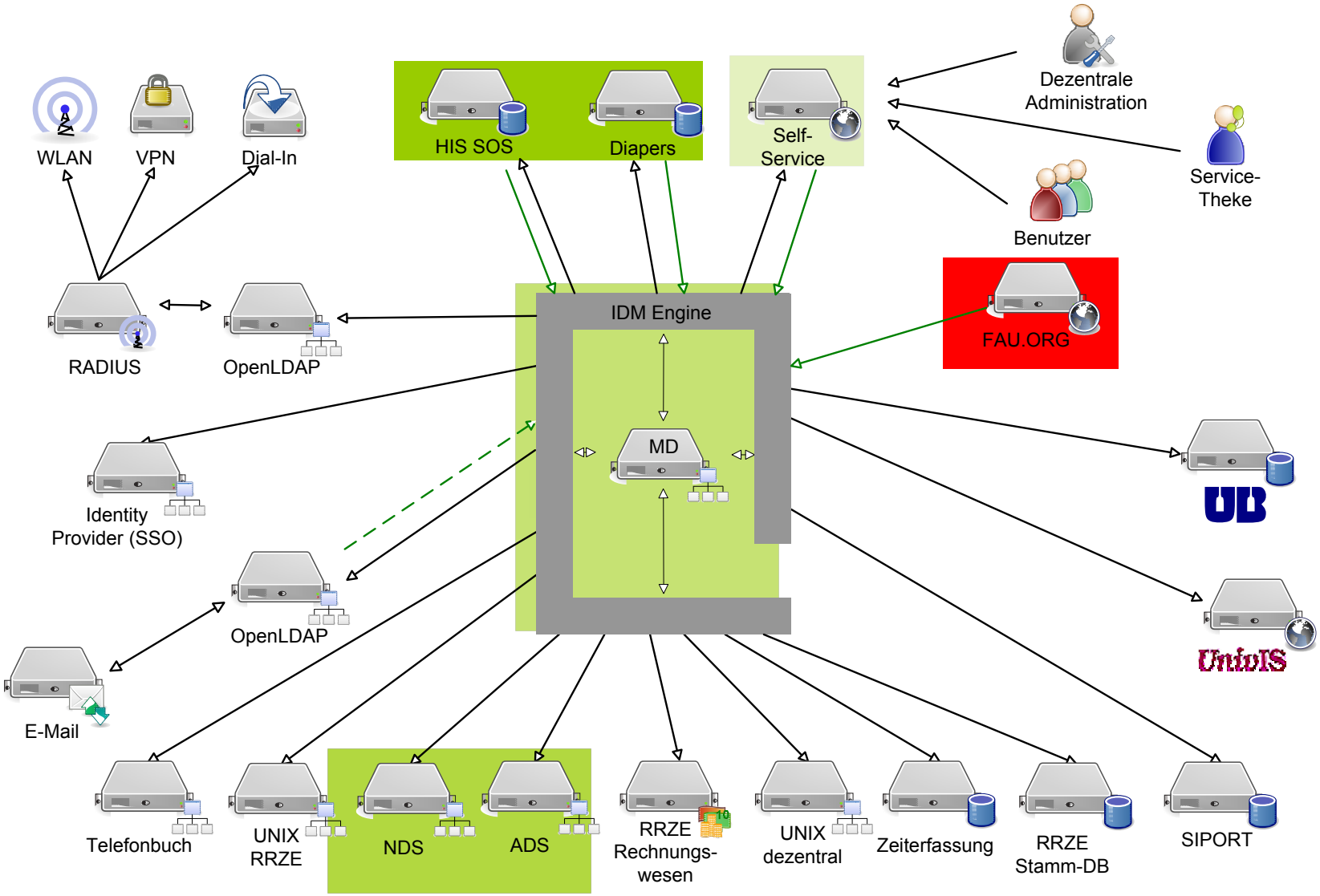
Status (2)

- **Neuentwicklung des Web-Frontends (WAID) für den Self-Service**
  - Online (näheres dazu im zweiten Teil)
- **Audit lauscht mit**
  - **Auswertung etwas mühsam**
  - **Ungeahnte Datenflut**
  - **Noch Arbeit nötig**
  - **Umstellung auf Novell Identity Audit geplant**
- **Aufbau des Meta-Directory hat sich bewährt**
  - **Flexibel genug für neue Anforderungen**
- **Anbindung von Diapers derzeit ohne Trigger**
- **Lesende Anbindung von HIS SOS derzeit ohne Trigger**
- **Lesende Anbindung des Altsystems**
  - **Nur markierte Einträge werden berücksichtigt**

Status (3)

- Zusammenführung verschiedener Einträge einer Person (Matching)
  - Erste Erfahrungen führen zur Anpassung der Parameter
- Zielsystemtreiber in Arbeit
  - Anbindung ADS exemplarisch fertig
  - Anbindung NDS exemplarisch fertig

Status aktuell



Showstopper

- Fehlende Organisationsstruktur
- Fehlender Dienstleistungskatalog
- Spät gewonnene Erkenntnis, wie die Software intern funktioniert
- Hohe Ansprüche im Bezug auf das Zusammenspiel der Treiber und Objekte im Meta-Directory
- Zu hohe Erwartungen an Hilfe durch externes Consulting

FAU.ORG

- Technische Implementation eines Systems zur Verwaltung der offiziellen und inoffiziellen Organisationsstruktur der Universität
  - Bereitstellung eines vollumfänglich spezifizierten Systems
  - Bereitstellung einer Weboberfläche
  - Datenlieferung an alle Systeme, die Kostenstellen oder Organisationsstrukturinformationen verwenden
- Zentrale Vergabe von uniweit einheitlichen Kostenstellen

Dienstleistungsportfolio

- Gestaltung eines Dienstleistungsporfolios für das RRZE
  - Erhebung der bisher angebotenen Dienstleistungen
  - Ausdünnen der bisher angebotenen Dienstleistungen
  - Angebot von nachfrageorientierten Dienstleistungspaketen
  - Erstellung eines transparenten Preisverzeichnisses
  - Veröffentlichung in verschiedenen Medien (Print, Web, …)

Ausblick

- ‚Phase der Konsolidierung' bis Ende Februar
  - Systempflege etc.
- ‚Branding' via WAID
- Aufbau der Gäste/Sonstigenverwaltung
- Anbindung von UnivIS
- Provisionierung von WLAN, VPN, SSO, …

Nachhaltige Nachnutzung

- 06/2008 – jpwgen
- 07/2008 – Tango Icons
  Ergänzungen zum offiziellen Icon Set des Tango Desktop Project von Beate Kaspar
- 09/2008 – jidgen

- … more to come

Vielen Dank!

peter.rygus@rrze.uni-erlangen.de