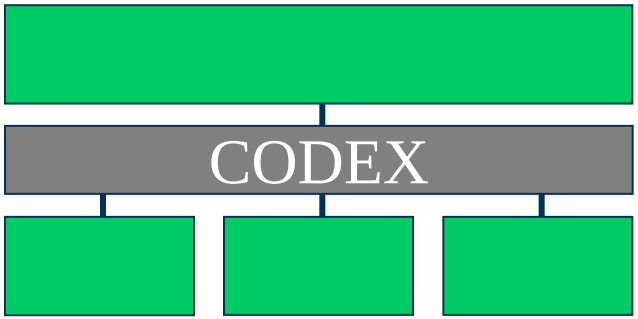
Prozessorientierung/ Prozessmanagement & Identity Management

Jena

Schmalkalden

Weimar



Erfurt

Nordhausen

Ilmenau

11. März 2011

Dr. Alejandra Lopez – TU-Ilmenau

Matthias Kühm – Uni Erfurt

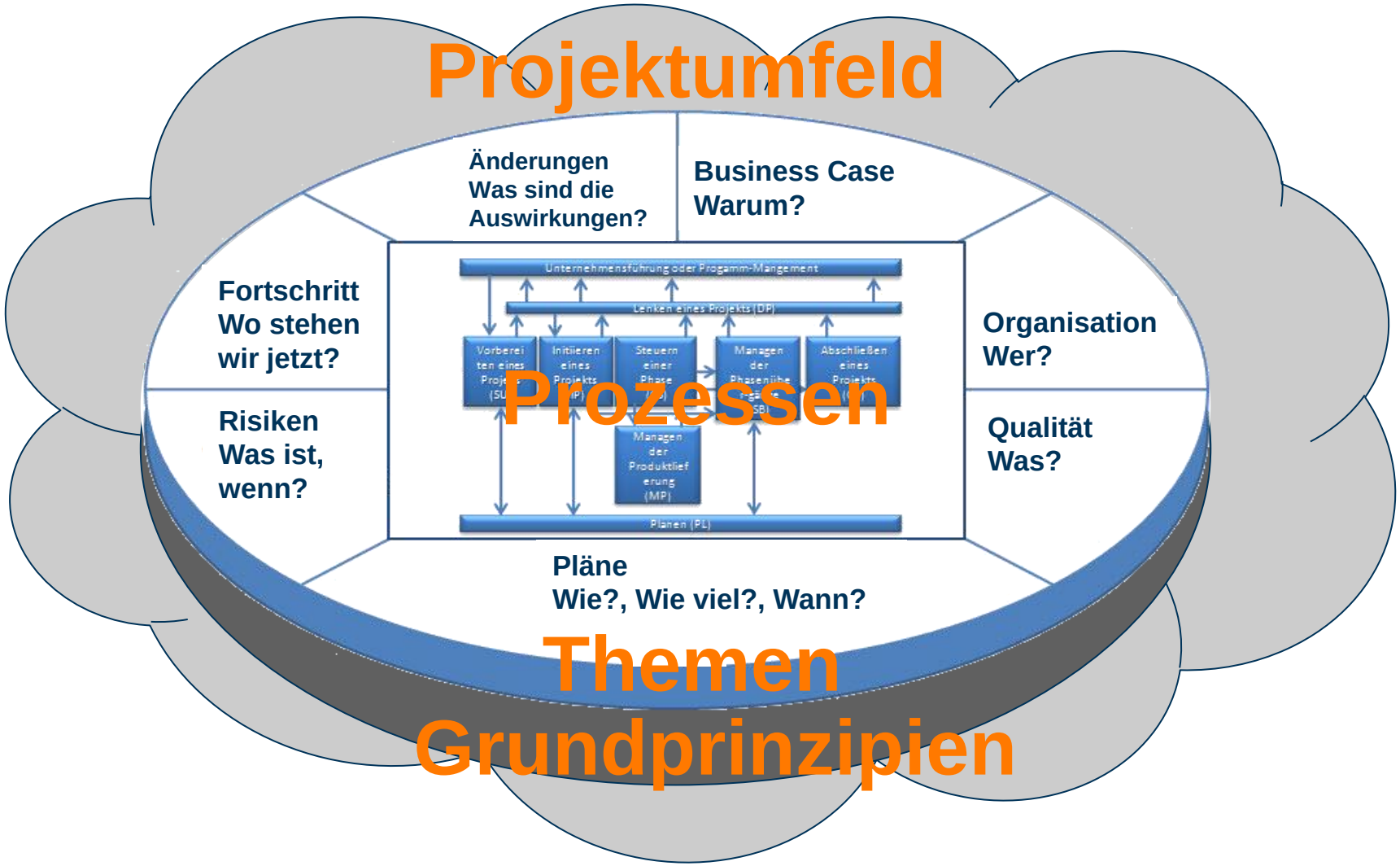
Projekt „Identity Management - Universität Erfurt“ (IdM-UniErfurt)

- Innerhalb des Kooperationsprojekts zwischen den Thüringer Hochschulen „Kooperative Reorganisation der IT-Dienste der Thüringer Hochschulrechenzentren (Codex – MetaDirectory)“ wurde in Erfurt ein Vorprojekt zur Einführung eines Identitätsmanagements gestartet:
  - Offizieller Start des Vorprojekts am 01.06.2010.
  - Am 10.09.2010 wurde das Hauptprojekt IdM-UniErfurt gestartet.
  - am 30.06.2011 wird das IdM-UniErfurt in seiner ersten Form in Produktion genommen werden.
- Wir haben versucht ein PRINCE2-konformes Projekt zu führen.

Was ist PRINCE2?

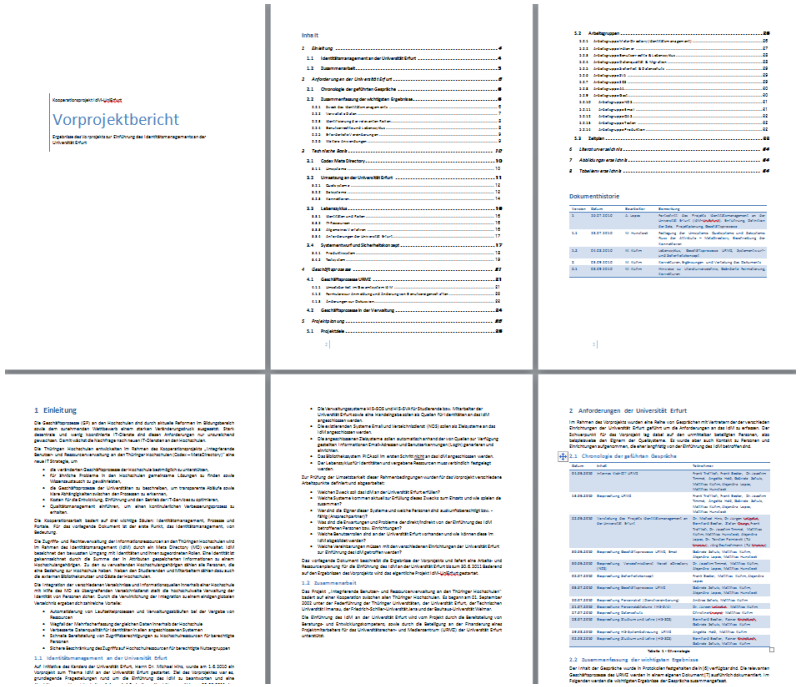
- PRINCE2 ist eine Projektmanagementmethode
- „Projects In Controlled Environments“
- PRINCE2 setzt Leitlinien für die Planung, Delegierung, Organisation und Steuerung aller Aspekte eines Projekts.
- Vorteile:
  - Prince2 beinhaltet etablierte Best Practices.
  - Begriffe stehen vor dem Start eines Projekts fest.
  - Festgelegte Strukturen für die Organisation, Delegation und Kommunikation.
  - Management „by Exception“.
  - Prince2 gliedert Planung, Überwachung und Steuerung nach Phasen
  - Definiert für jedes Projektziel bestimmte Toleranzen, die den Handlungsrahmen für delegierte Befugnisse festlegen.

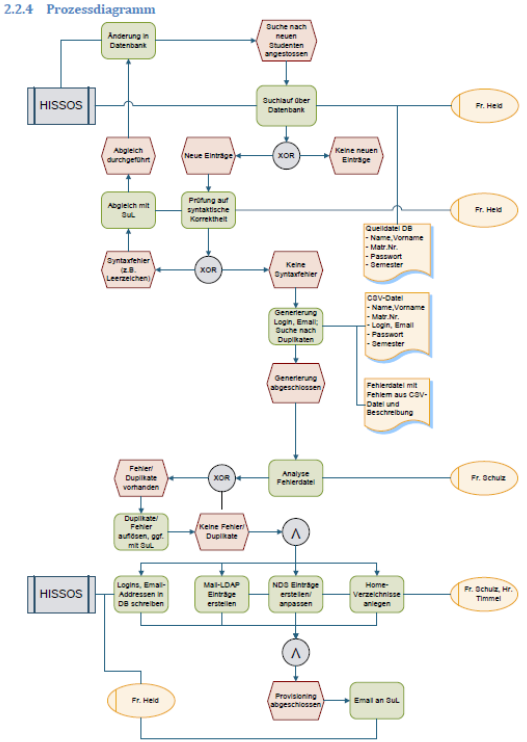
Die Struktur von PRINCE2



Business Case

- Zweck des Themas „Business Case“ ist die Einrichtung geeigneter Mechanismen für die Beurteilung, ob ein Projekt wünschenswert, lohnend und realisierbar ist (und bleibt), um auf dieser Grundlage über die (weitere) Investitionen entscheiden zu können.





Vorprojekt IdM-UniErfurt

- Offizieller Start des Vorprojekts am 01.06.2010.
- Zielsetzung:
  - Anforderungen der Universität Erfurt erheben
  - Ziele für das Projekt bis 30.06.2011 definieren
  - Kontaktaufnahme zur beteiligten Einrichtungen, Ansprechpartner festlegen, Prioritäten bestimmen
  - Systementwurf (Umsysteme, Test- und Produktionssystem, Einbettung in IT-Landschaft)
  - Schulung für neue Mitarbeiter durchführen.
  - Managementprodukte: Business Case, Arbeitspakete, Zeit- und Ressourcenplan für Projektlaufzeit, Umfang und Abhängigkeiten, Auslastung der Mitarbeiter, Kosten, Qualität, Nutzen und Risiken definieren.
- Team: Alejandra Lopez (UniRZ Ilmenau, Leiter), Matthias Hunstock (UniRZ Ilmenau), Matthias Kühm (URMZ Erfurt)

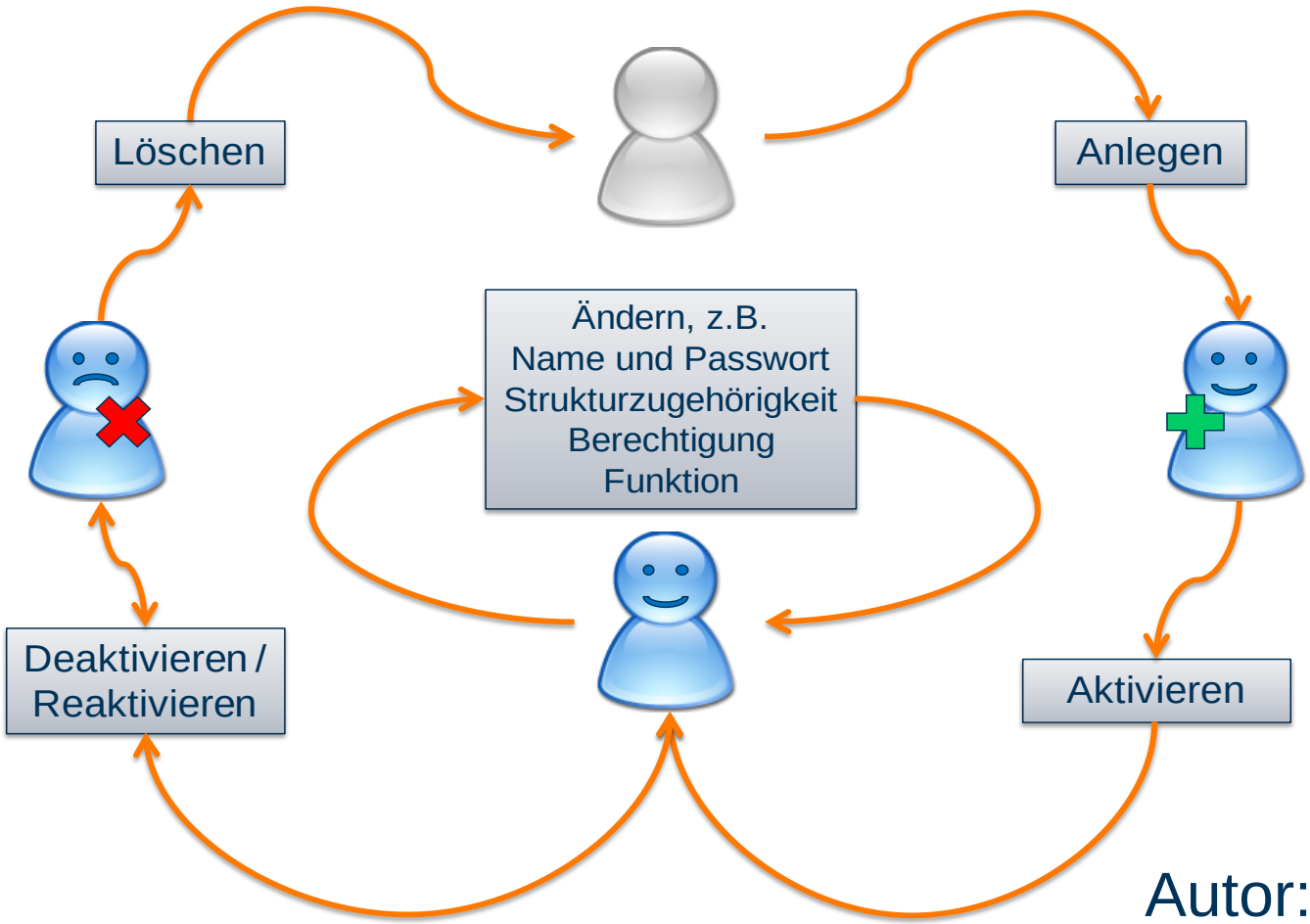
Rahmenbedingungen IdM-UniErfurt

- Verwaltungssysteme HIS-SOS und HIS-SVA sowie eine Handeingabe sollen als Quellen für Identitäten an das IdM angeschlossen werden
- Die existierenden Systeme Email und Verzeichnisdienst (NDS) sollen als Zielsysteme an das IdM angeschlossen werden
- Die angeschlossenen Zielsysteme sollen automatisch anhand der von Quellen zur Verfügung gestellten Informationen Email-Adressen und Benutzerkennungen (Login) generieren und einrichten
- Die Festlegung von Benutzerrechten und Lebenszyklen für Identitäten und Ressourcen erlangen eine hohe Priorität

Benutzerrechte/Lebenszyklus

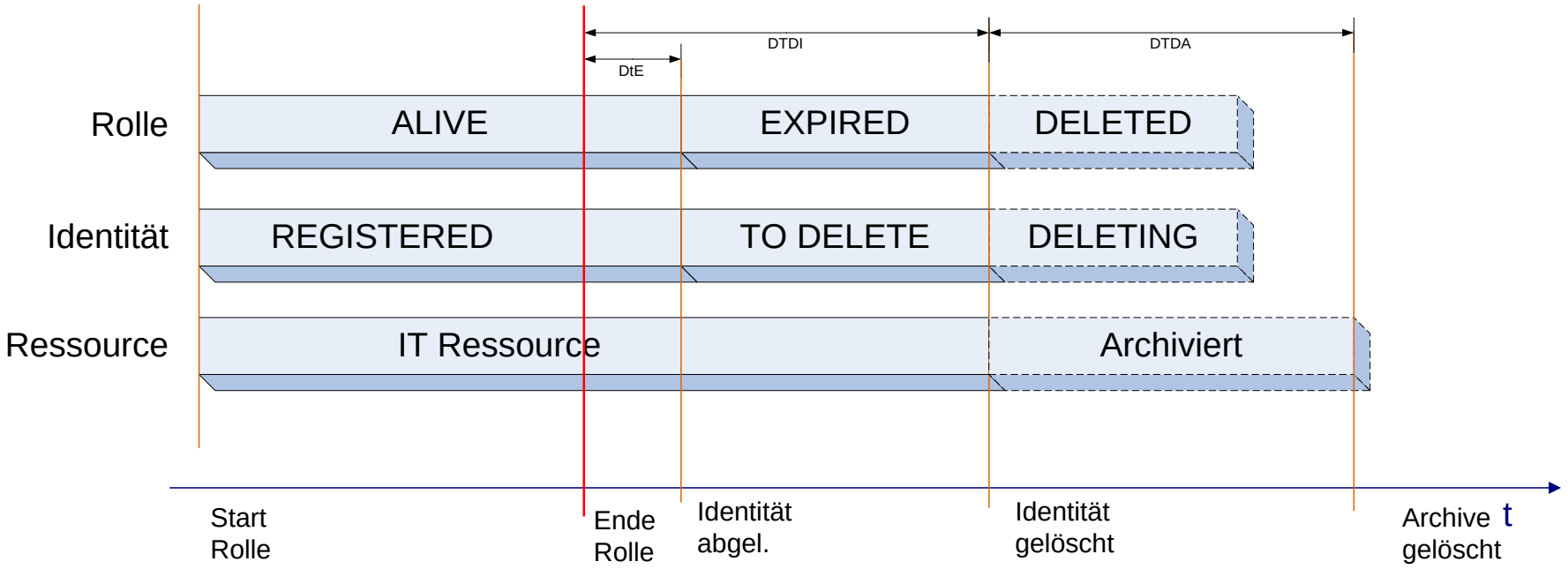
- Grundvoraussetzung für Einführung des IdM ist Festlegung von Benutzerrechten & Lebenszyklen
  - Welche Ressourcen werden Identitäten bezüglich der identifizierten Rollen zur Verfügung gestellt?
  - Wie lange nach Ausscheiden (z.B. Exmatrikulation) werden Daten durch das IdM verwaltet?
  - Wie lange nach Ausscheiden sind Ressourcen weiter nutzbar? Wann werden Benutzerkonten gelöscht?
  - Wie wird mit Daten in persönlichen Verzeichnissen verfahren (Email-Korrespondenz, Dokumente)?

Identitätslebenszyklus



Autor: J.D.

Lebenszyklus



Herausforderungen

- Vielzahl von Email-Domains wirklich notwendig?
  - Vorschlag: Reduzierung auf *uni-erfurt.de*
- Großer Aufwand bei Änderung von Benutzernamen infolge von Namensänderungen
  - Vorschlag: unveränderlicher Benutzername (neues Schema?)
- Doppelte Provisionierung z.B. für Doktoranden aktuell möglich!
  - Zukünftig ein Email-Konto + ein Login pro Identität
- GroupWise-Nutzung für Mitarbeiter uneinheitlich geregelt
  - Vorschlag: als Standard festlegen
- Synchronisation der Laufzettel-/Anmeldeprozesse
  - Benutzer müssen vor Zugriff auf Ressourcen Benutzerordnung des URMZ akzeptieren!

Zielsetzung für das Hauptprojekt

(1) Einführung eines produktiven Systems zum IdM an der Universität Erfurt auf Basis des Codex Meta Directory bis 30.06.2011

(2) Anbindung der Verwaltungssysteme HIS-SVA und HIS-SOS sowie der Handeingabe THUAPOS-light an das IdM und Übernahme von Identitäten in das MD zum Zweck der Provisionierung

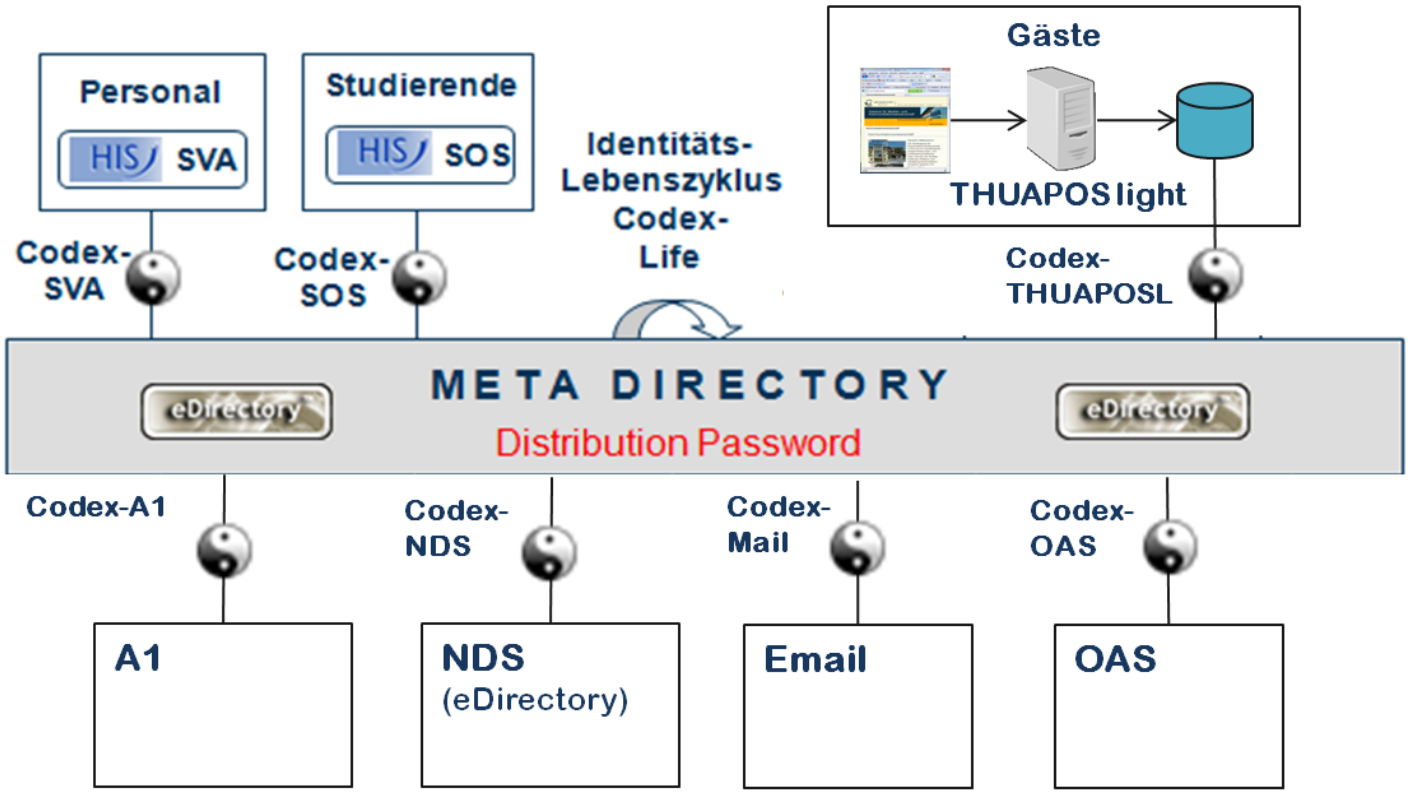
(3) Anbindung der existierenden Zielsysteme Email und NDS sowie des Authentifizierungssystems A1 an das IdM und Automatisierung von grundlegenden Aufgaben im Zusammenhang mit dem Provisioning von verwalteten Identitäten

(4) Einführung eines operativen Auskunftssystems zur informationellen Selbstbestimmung, Unterstützung des Servicebüros URMZ und Passwortverwaltung

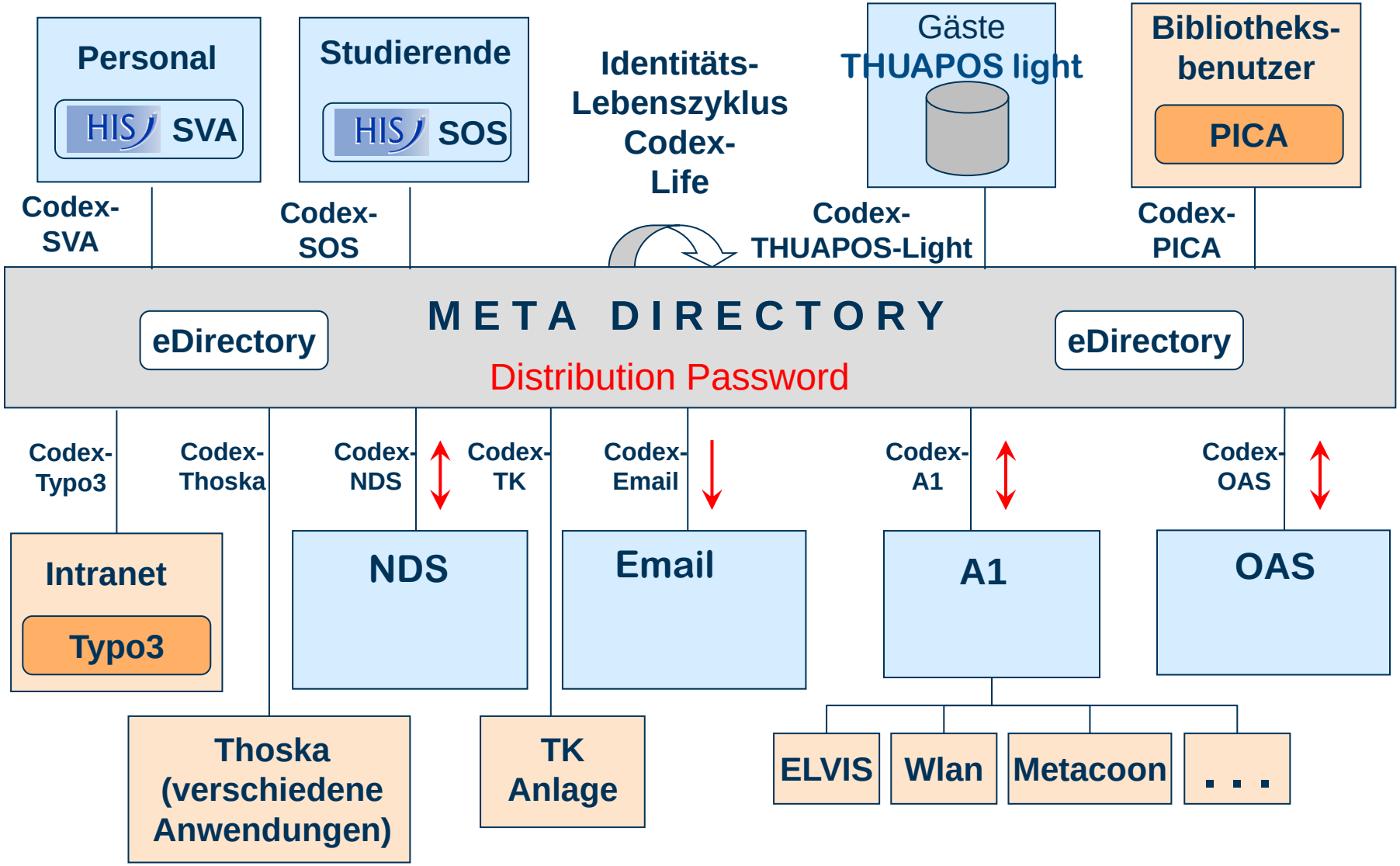
(5) Festlegung von Benutzerrechten und Lebenszyklen für Identitäten und Ressourcen, Umsetzung in Gesamtsystem IdM

(6) Optimierung der Geschäftsprozesse im Zusammenhang mit dem Provisioning von Angehörigen und Mitgliedern der Universität Erfurt

Entwurf Umsysteme



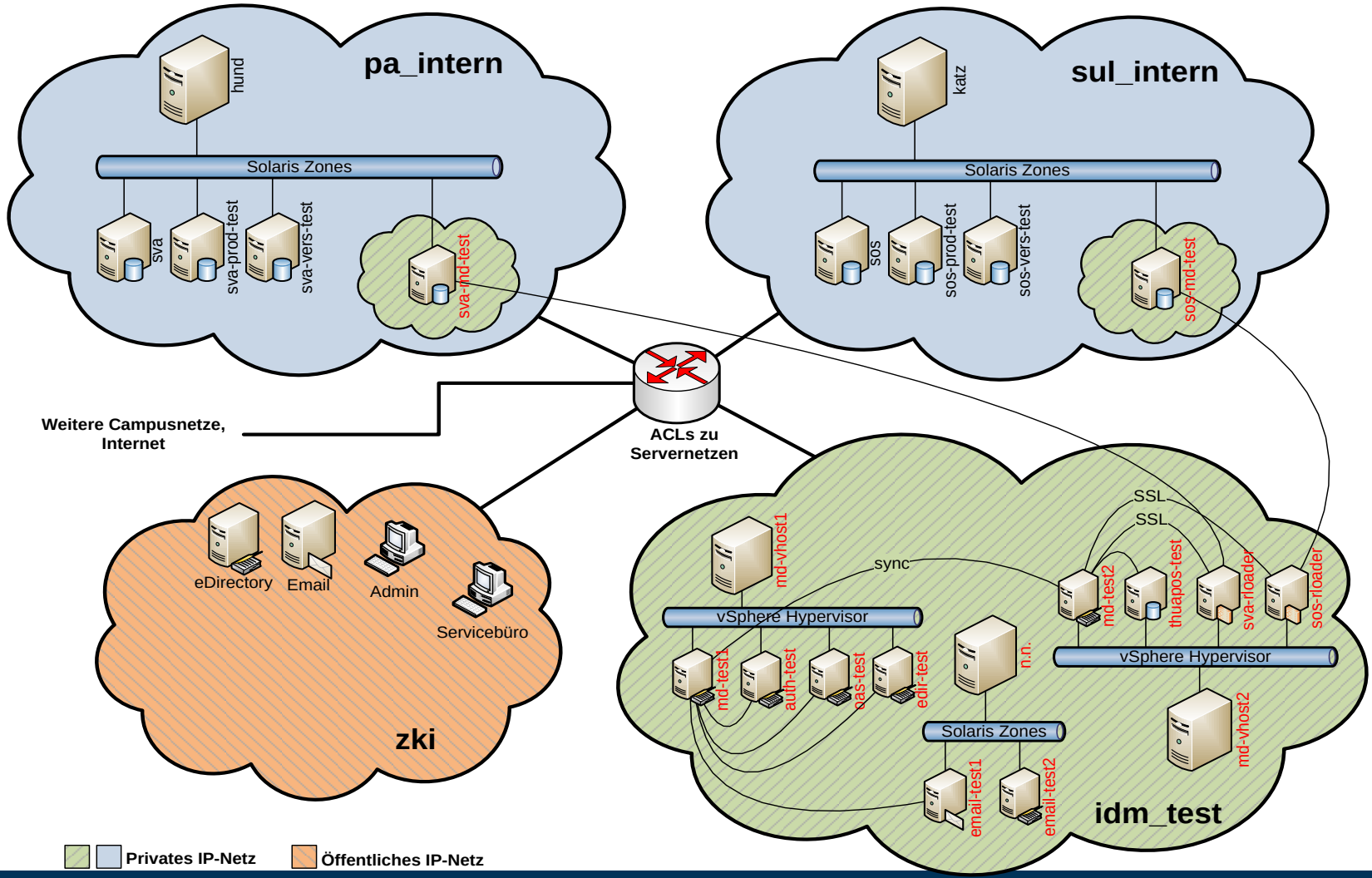
Entwurf Umsysteme



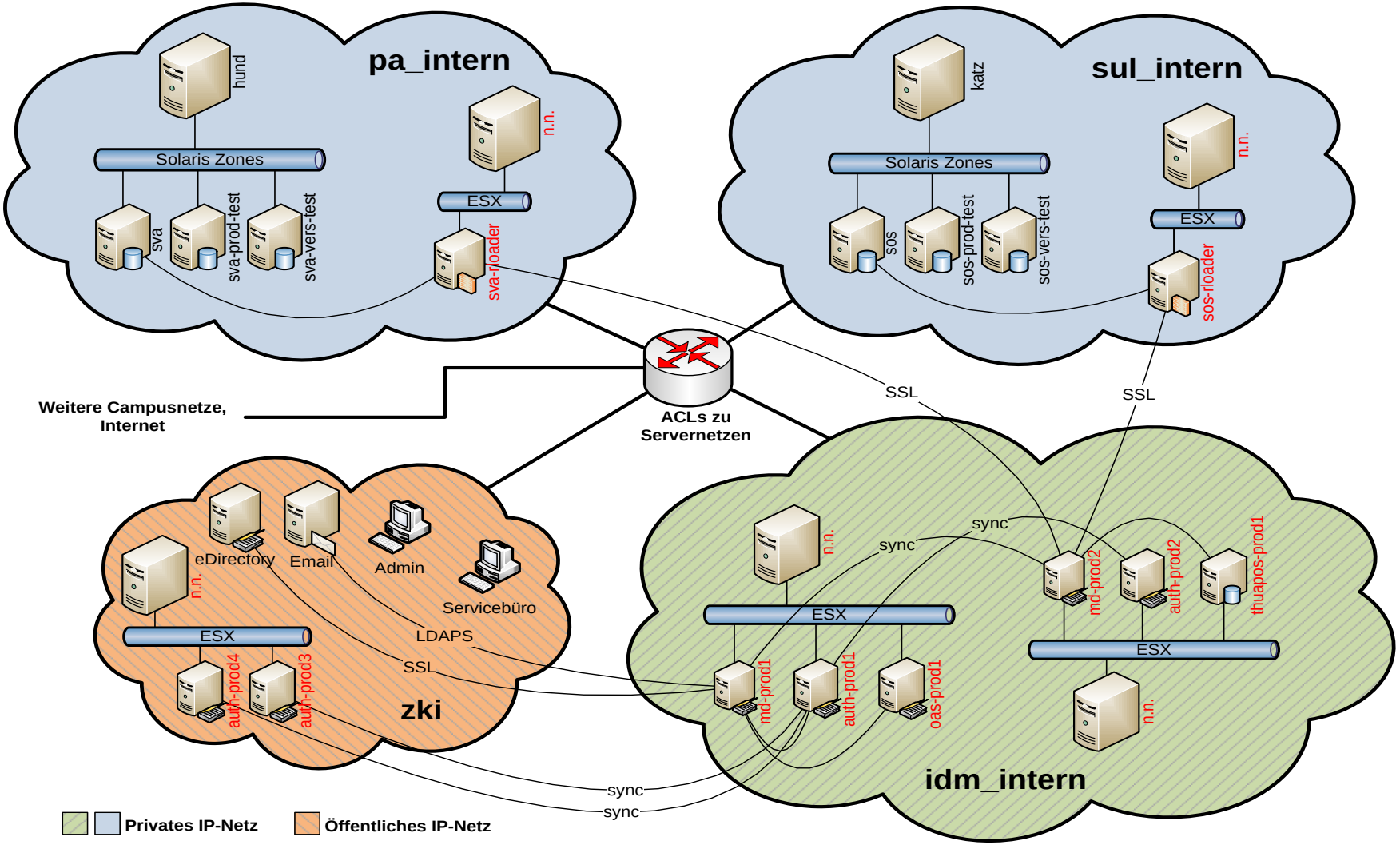
IdM-UniErfurt V1 (2010-2011)

IdM-UniErfurt V2 oder weitere

Entwurf des Testsystems:



Entwurf des Produktionssystems:



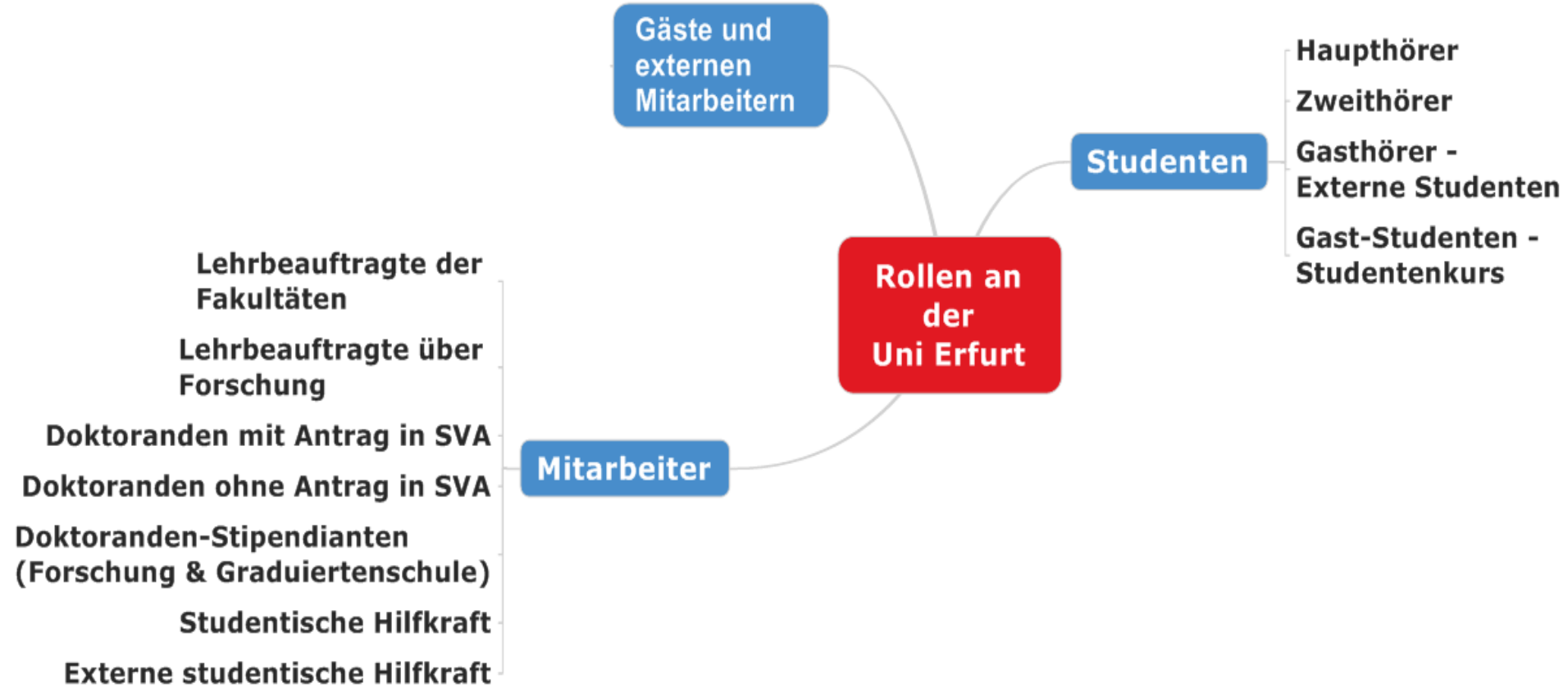
Verwaltete Daten

- Codex-Schema sehr umfangreich → Anforderungen aller beteiligten Hochschulen erfasst
  - Für den Betrieb des IdM ist nur eine Teilmenge wirklich notwendig!
  - Nicht benötigte Attribute bleiben unbelegt
- Vorschlag zur Selbstverpflichtung für das IdM an der Uni Erfurt: Nur Daten verwalten,
  (1) die für die Provisionierung in den Zielsystemen notwendig sind,
  (2) die für die eindeutige Identifizierung von Personen im MD verwendet werden,
  (3) die eine eindeutige Assoziation mit Personen bzw. Rollen in den Quellsystemen ermöglichen.

Verwaltete Daten - Überblick

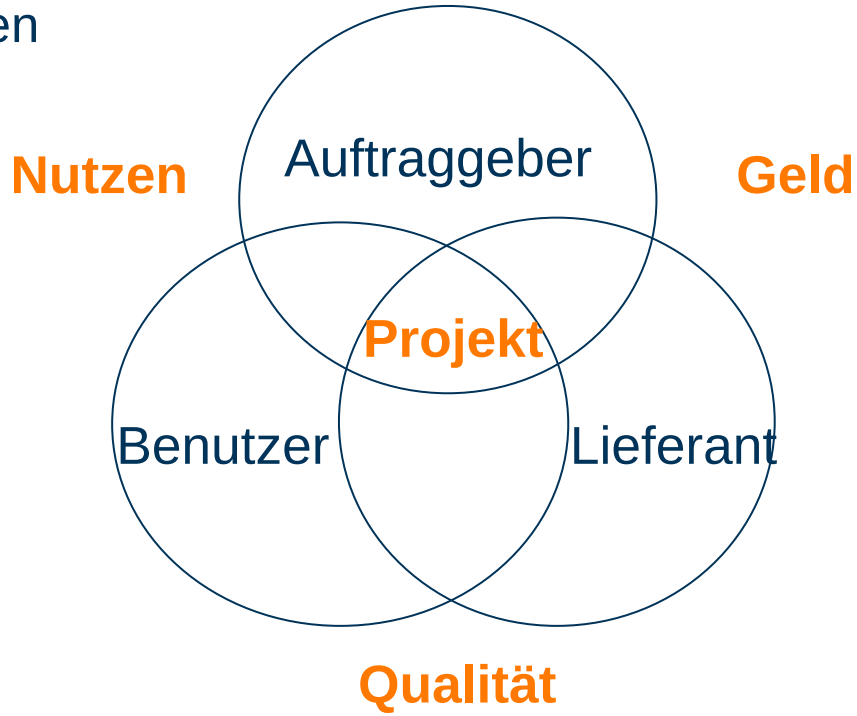
Attribut	Kurzbeschreibung / Verwendung	Quellsystem(e)
Familienname	Identifizierung von Personen, Generierung von Basisdaten, z.B. Login oder Mailadresse	SOS, SVA, Handeingabe
Vornamen	siehe Familienname	SOS, SVA, Handeingabe
Namenszusätze	siehe Familienname	SOS, SVA
Geburtsdatum	eindeutige Identifizierung von Personen bei Namensgleichheit	SOS, SVA, Handeingabe
SVA-interne Personalnummer	dauerhaft eindeutige Zuordnung der Einträge in Quellsystem und MetaDirectory	SVA
Matrikelnummer	dauerhaft eindeutige Zuordnung der Einträge in Quellsystem und MetaDirectory	SOS
Geschlecht / Anrede	Erstellung von Schreiben mit korrekter Anrede	SOS, SVA, Handeingabe
akademischer Grad	Erstellung von Anzeigenamen	SVA, Handeingabe
Titel	Erstellung von Anzeigenamen	SVA, Handeingabe
Immatrikulationsdatum	Einordnung von Studierenden	SOS
Name der Organisation	organisatorische Zugehörigkeit der Person	SVA, Handeingabe
Personalkategorie	Charakter der Beschäftigung, z.B. zur Erkennung studentischer Hilfskräfte	SVA, Handeingabe
Strukturzugehörigkeit	Ableitung von Berechtigungen	SVA, Handeingabe
Kostenstelle bzw. Kostenträger	Ableitung der Strukturzugehörigkeit	SVA
Gültigkeitsbeginn / Beginn	Realisierung des Lebenszyklus	SOS, SVA, Handeingabe
Gültigkeitsbeginn / Ende	Realisierung des Lebenszyklus	SOS, SVA, Handeingabe

Rollen an der Uni Erfurt (Ist)

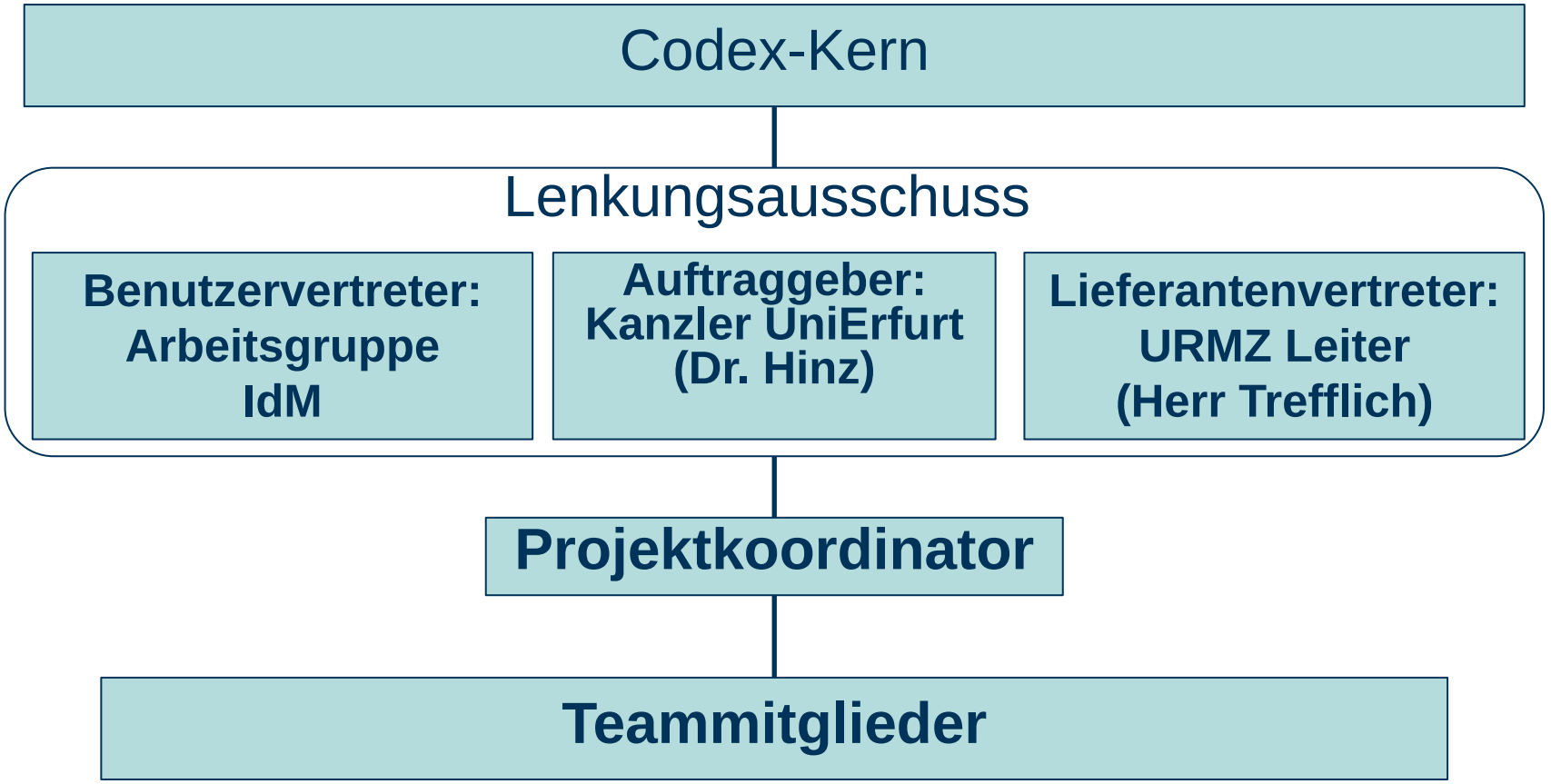


Organisation und Rollen im Projekt:

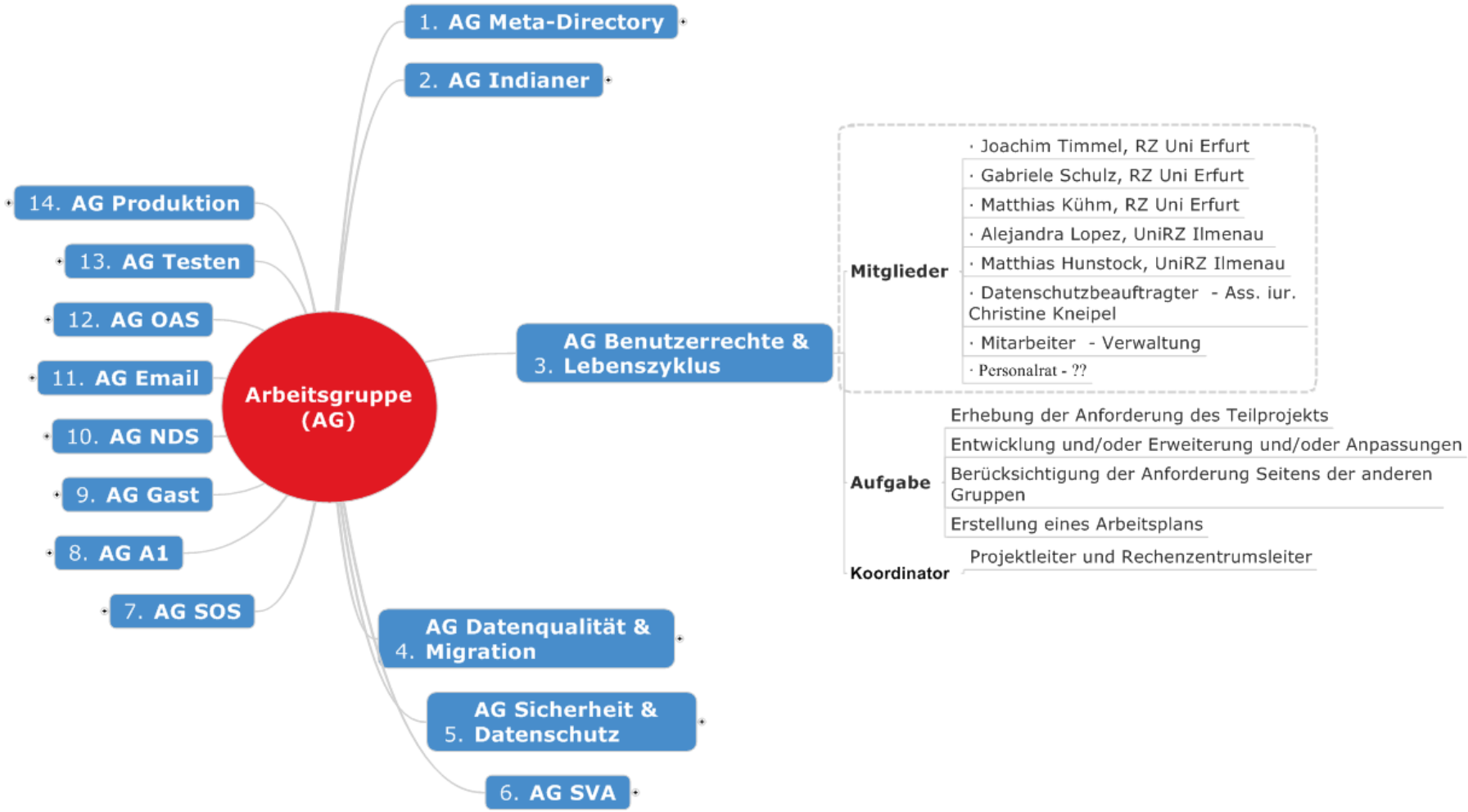
- Definition und Festlegung der Organisationstruktur des Projekts
- Zuordnung der Zuständigkeiten und Verantwortlichkeiten (das Wer?)
- Unterschiedliche Interesse an einem Projekt in der Projektorganisation abbilden
- Rollen definieren



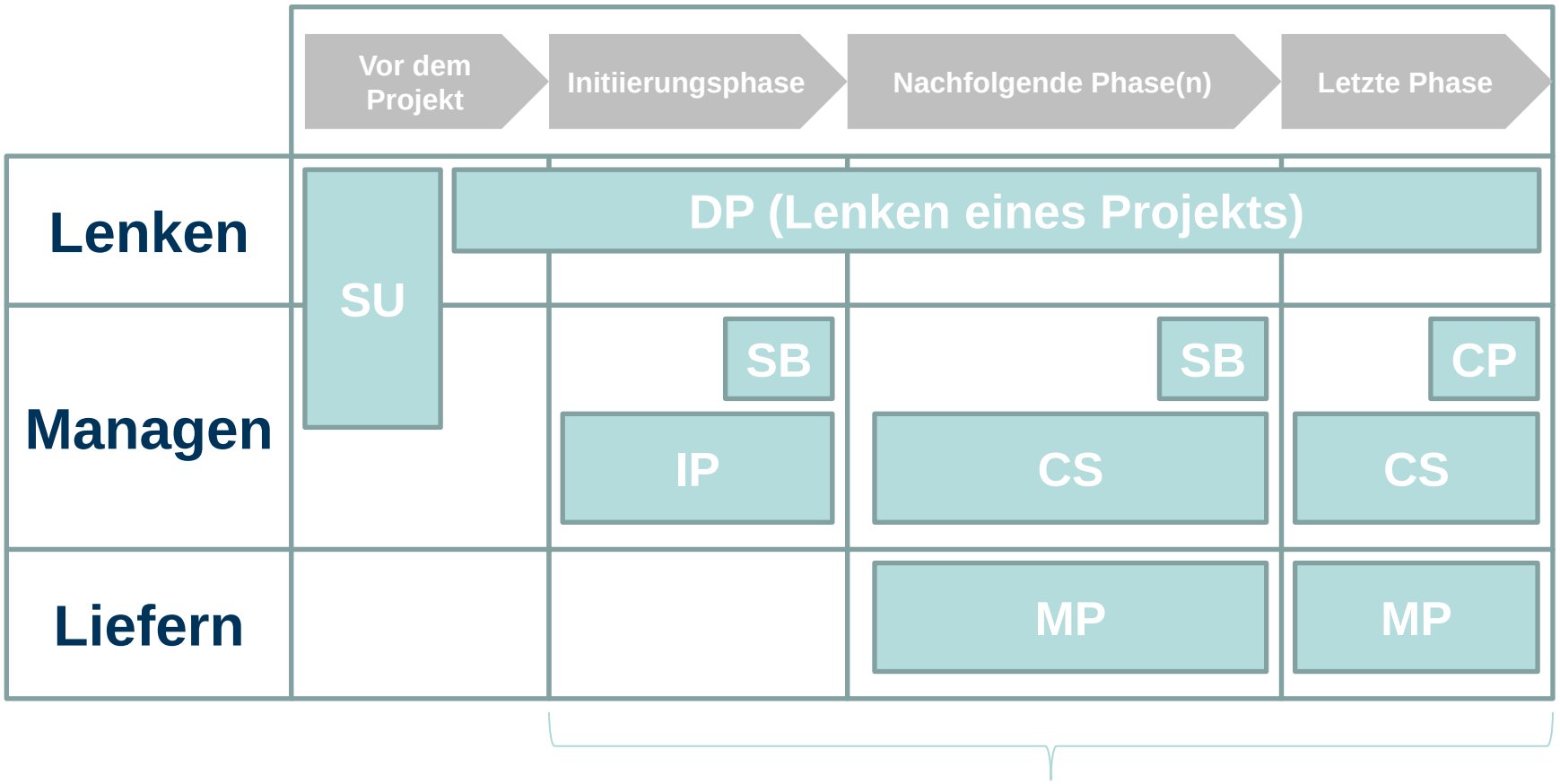
Organisationstruktur des IdM-UniErfurt:



Arbeitsgruppen und Arbeitspakete:



PRINCE2 Prozesse

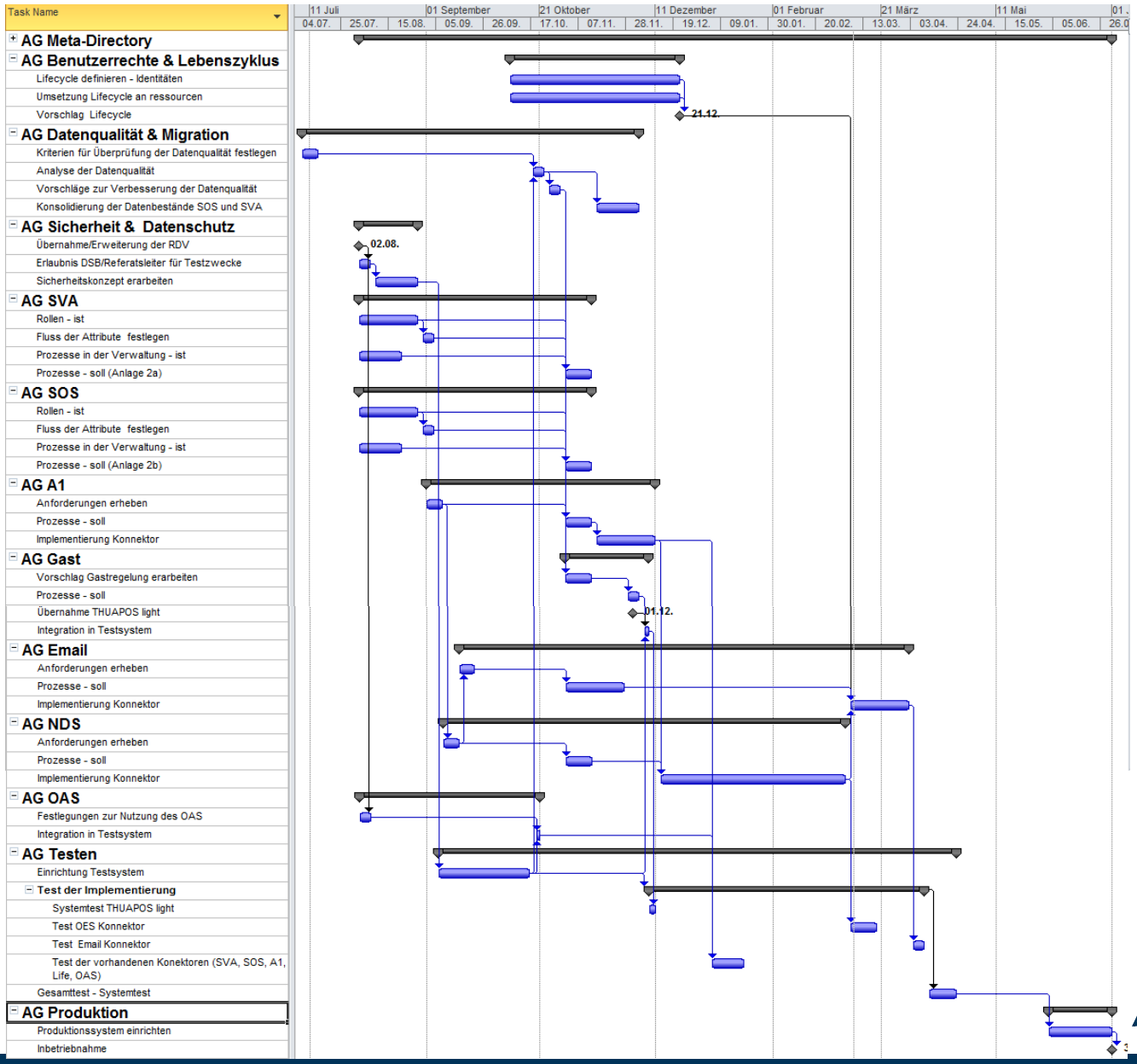


Mindestens 1 Phase je Projekt

Zeitplan


Vorprojekt
Sep. 2010
Dez. 2010
Initiierung des Projektes
IdM-UniErfurt,
Abschluss der Anforderungsaufnahme
Implementierung und
Integration aller Komponenten in Testsystem
April 2011
Juni 2011
Abschluss des Projekts,
Übergang in Produktivbetrieb

Zeitplan



30.06.2011

Resümee

- Ziele und Plan definieren
- Zuordnung der Zuständigkeiten und Abhängigkeiten
- Projektverlauf kontrollierbar
- Kosten vorausschauen
- Prozesse definieren und optimieren
- Erfahrungen von Projekt zu Projekt übertragen
- Gemeinsam wiederverwendbare Komponente entwickeln

Danke schön für Ihre Aufmerksamkeit

UNIVERSITÄT ERFURT

Identitätsmanagement an der Universität Erfurt

ZKI Arbeitskreis Verzeichnisdienste

FH Frankfurt am Main, 11. März 2011

UNIVERSITÄT ERFURT

Herausforderungen

Entwicklungen seit dem Vorprojekt

UNIVERSITÄT ERFURT

Mail-System

- Vielzahl von Mail-Domains
  - Festlegung auf einheitliche Mail-Domain *uni-erfurt.de*
    - Automatische Einrichtung mit Einführung des IdM
  - Nicht mehr verwendete Email-Domains laufen aus
    - Adressen in Domains für Externe werden ab sofort nicht mehr vergeben, Bestandskonten umgestellt (bis Juli 2011)
    - Bestandskonten von Studierenden werden nach Bereinigung im April 2011 auf neue Domain umgestellt (bis Juli 2011)
    - Adressen in Domain für Studierende werden bis Ende 2012 als Aliase beibehalten
  - Aber: Struktur im Mail-LDAP bleibt vorerst erhalten (Mail-Verteiler)
- Uneinheitliche Regelung der Nutzung von Groupwise für Mitarbeiter
  - Nutzung von Groupwise für alle Mitarbeiter wird angestrebt, aber aufgrund von Personalmangel auf unbestimmt Zeit aufgeschoben
- Fazit: Kaum Reduzierung der Komplexität für Mail-Konnektor

UNIVERSITÄT ERFURT

Benutzerverwaltung

- Änderung der Benutzerkennung
  - Schema verwendet Name und Teile des Vornamens → Änderung der Benutzerkennung bei Namensänderung erforderlich
  - Änderung des Schemas konnte nicht durchgesetzt werden
  - IdM muss daher die Änderung der Benutzerkennung unterstützen
    - Anforderungen für Implementierung wurden formuliert
    - Prozess mit Einbindung der Benutzer wurde festgelegt
- Doppelte Provisionierung in Zielsystemen
  - Konsens in universitärer AG Identitätsmanagement, dass IdM pro Identität eine Benutzerkennung und eine Email-Adresse verwaltet
  - Aktueller Bestand in Zielsystemen erfordert Zusammenführung von Benutzerkonten, insbesondere mit verschiedenen Mailadressen, die einer Person zugeordnet werden können
    - Bereinigung im Zusammenhang mit Umstellung Mail-Domain
  - Sonderfall Zweiteintrag in NDS wird (eingeschränkt) weitergeführt, aber nicht durch IdM verwaltet

UNIVERSITÄT ERFURT

Synchronisierung der Laufzettel-/Anmeldeprozesse

- Etablierte Prozesse werden für Studierende weitergeführt und erweitert
  - Ausdehnung auf Gasthörer (bisher nicht erfasst)
  - Benutzerordnung des Rechenzentrums (URMZ) muss mit Immatrikulation/ Registrierung bei Abt. Studium & Lehre akzeptiert werden (bisher nur Zustimmung zur Einrichtung eines Email-Kontos)
  - Serienbriefe mit Benutzerkennung, Email-Adresse und Anfangspasswort werden aus HIS-SOS erstellt und mit Studienunterlagen versendet
    - Daten fließen über Konnektor nach HIS-SOS (bisher manuell)
- Prozess für Einrichtung von Mitarbeitern wird neu etabliert
  - Automatische Provisionierung mit Eintrag in HIS-SVA
    - Anmeldeformular durch den Bereich entfällt
  - Provisionierungsdaten werden durch Servicebüro URMZ ausgehändigt (im Rahmen des Laufzettelprozesses)
    - Benutzerordnung des URMZ muss mit Unterschrift akzeptiert werden
    - Dienstliche Kontaktinformationen werden erfasst
  - Email-Adresse wird mit Nutzung (=Änderung des Anfangspassworts) nach HIS-SVA übertragen

UNIVERSITÄT ERFURT

Synchronisierung der Laufzettel-/Anmeldeprozesse

- Prozesse für Einrichtung sonstiger Personen werden weitergeführt und erweitert
  - Anmeldeformular (mit dienstlichen Kontaktdaten) an Servicebüro URMZ
  - Einrichtung über Handeingabe (bisher manuell in den Zielsystemen)
  - Ausgabe der Provisionierungsdaten durch Servicebüro URMZ
    - Benutzerordnung des URMZ muss mit Unterschrift akzeptiert werden

- Prozesse für Deprovisionierung von Mitarbeitern und sonstigen Personen werden neu etabliert
  - Existierender Laufzettel für Abmeldung funktioniert praktisch nicht
  - Mit Endedatum aus IdM werden Benutzerkonten deaktiviert
    - Nachnutzung Email-Adresse für Mitarbeiter: 6 Monate
  - 12 Monate nach Deaktivierung werden Benutzerkonten in Zielsystemen zusammen mit den Personendaten im IdM gelöscht
  - Automatische Benachrichtigungen vor Deaktivierung

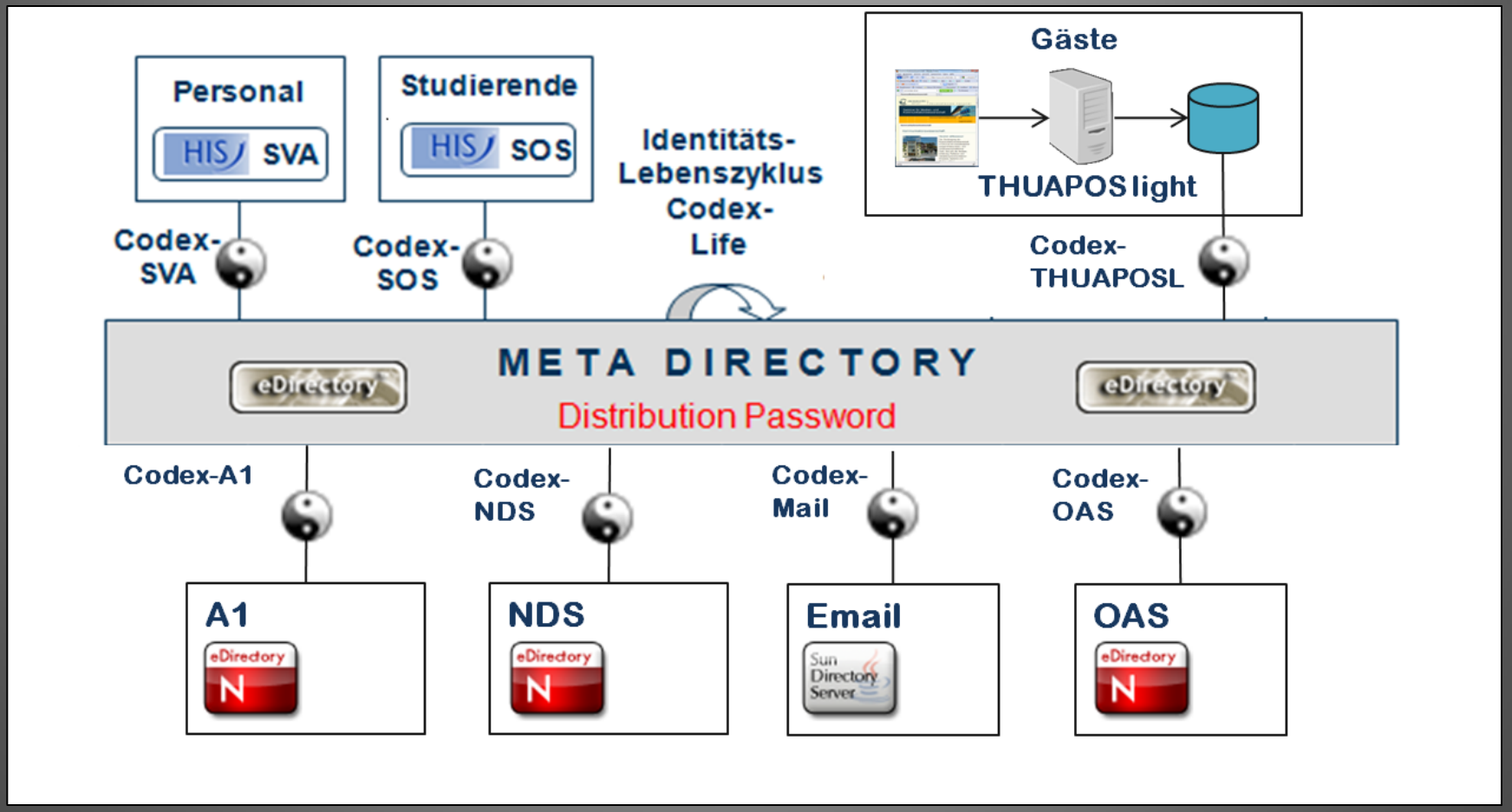
UNIVERSITÄT ERFURT

Anbindung der Umsysteme

Entwicklungsstand

UNIVERSITÄT ERFURT

Überblick Umsysteme



UNIVERSITÄT ERFURT

Quellsysteme

- HIS-SOS
  - Übernahme des Konnektors aus Codex-Projekt, Anpassung an Anforderungen abgeschlossen
  - Besonderheit: Informix-Datenbank
  - In Testsystem integriert, Anbindung an Testdatenbank mit GX-Zugriff
- HIS-SVA
  - Übernahme des Konnektors aus Codex-Projekt, Anpassung des Anforderungen weitestgehend abgeschlossen
  - Besonderheit: Informix-Datenbank, Integration mit COB und FSV
  - In Testsystem integriert, Anbindung an Testdatenbank mit GX-Zugriff
- Handeingabe THUAPOS-light
  - Anforderungen direkt in Entwicklung im Rahmen des Codex-Projekts eingeflossen, Version 1.0 bald erreicht
  - Aktuelle Version in Testsystem integriert

UNIVERSITÄT ERFURT

Zielsysteme

- Authentifizierungssystem (A1)
  - Übernahme des Konnektors/der Verzeichnisstruktur aus Codex-Projekt, einrichtungsspezifischen Anforderung für weitere Entwicklung erhoben (insbesondere ValueAdder)
  - In Testsystem integriert
- Operatives Auskunftssystem (OAS)
  - Übernahme des Konnektors/des Verzeichnisses aus Codex-Projekt, weiterführende Anforderungen (u.a. Passwortmanagement) erhoben
  - In Testsystem integriert
- Mail-System/NDS
  - Anforderungen erhoben, Spezifikation für Implementierung in Arbeit
  - Implementierung/Integration in Testsystem bis Ende April

UNIVERSITÄT ERFURT

Ausblick

Projektende 30.6.2011

UNIVERSITÄT ERFURT

Was ändert sich mit Einführung des IdM?

- Vereinfachung und Beschleunigung der Einrichtung von neuen Mitarbeitern im Universitäts-Netzwerk
  - Wegfall des Anmeldeformulars für Personen in HIS-SVA
  - Einrichtung erfolgt mit Übernahme der Daten zum Arbeitsverhältnis durch PA
- Automatische Einrichtung der Studierenden mit Immatrikulation durch Abt. Studium und Lehre
- Umgehende Einrichtung sonstiger Personen vor Ort im Servicebüro URMZ möglich
- Automatische Deprovisionierung von Benutzern anhand der vom IdM verwalteten Ablaufdaten
- Mehr Transparenz in der Benutzerverwaltung durch dokumentierte Schnittstellen und Prozesse, klare Regelungen zur Vergabe und Bereinigung von Benutzerkonten (Identitätslebenszyklus)

UNIVERSITÄT ERFURT

Ende