Fachhochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

Berlins größte und vielfältigste Fachhochschule

Projekt JUDIT - (J)User Directory Information Tree

Konzept und Umsetzung

Aufbau einer Identity-Management-Infrastruktur

Stefan Zech · 01.12.2008

fhtw

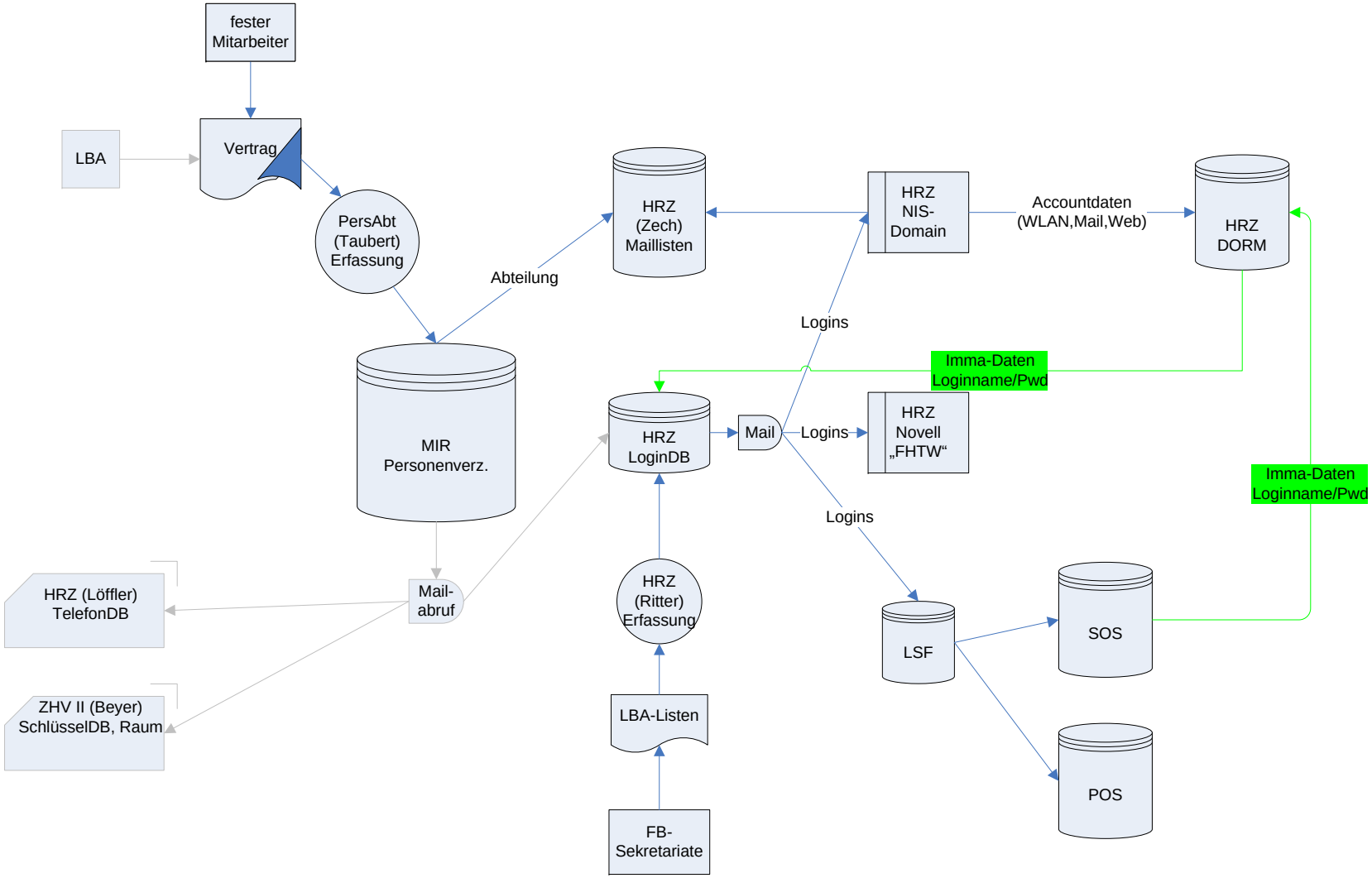
Agenda

- Historie – wie wir zu einem IDMS kamen
- Ausgangssituation
- Projektorganisation
- IDM-Design
- IDM-Einführung
- Ausblick

JUDIT – die Geburt (2007)

- Keimzelle: hochschulweites (Teil-)Projekt mit Neuaufbau einer zentralen Nutzerverwaltung
- nebulöse Vorstellung über Personalaufwand, Kosten und Umfang (Prozesse)
- mehrfache MA-Ausschreibungen ergebnislos
- HIS – Auftrag: Untersuchung IST-Situation
  - => warten auf HISinOne (Lösungskonzept unklar)
- HRZ-interner Neubeginn: Projekt JUDIT
    - Offline DB (Access) – nicht dezentralisierbare Nutzereinrichtung
    - Informationsverbreitung: eMail mit CSV-Daten
    - Speicherung von Klartextpassworten
    - mehrere Passwörter
    - Bearbeitungsdauer

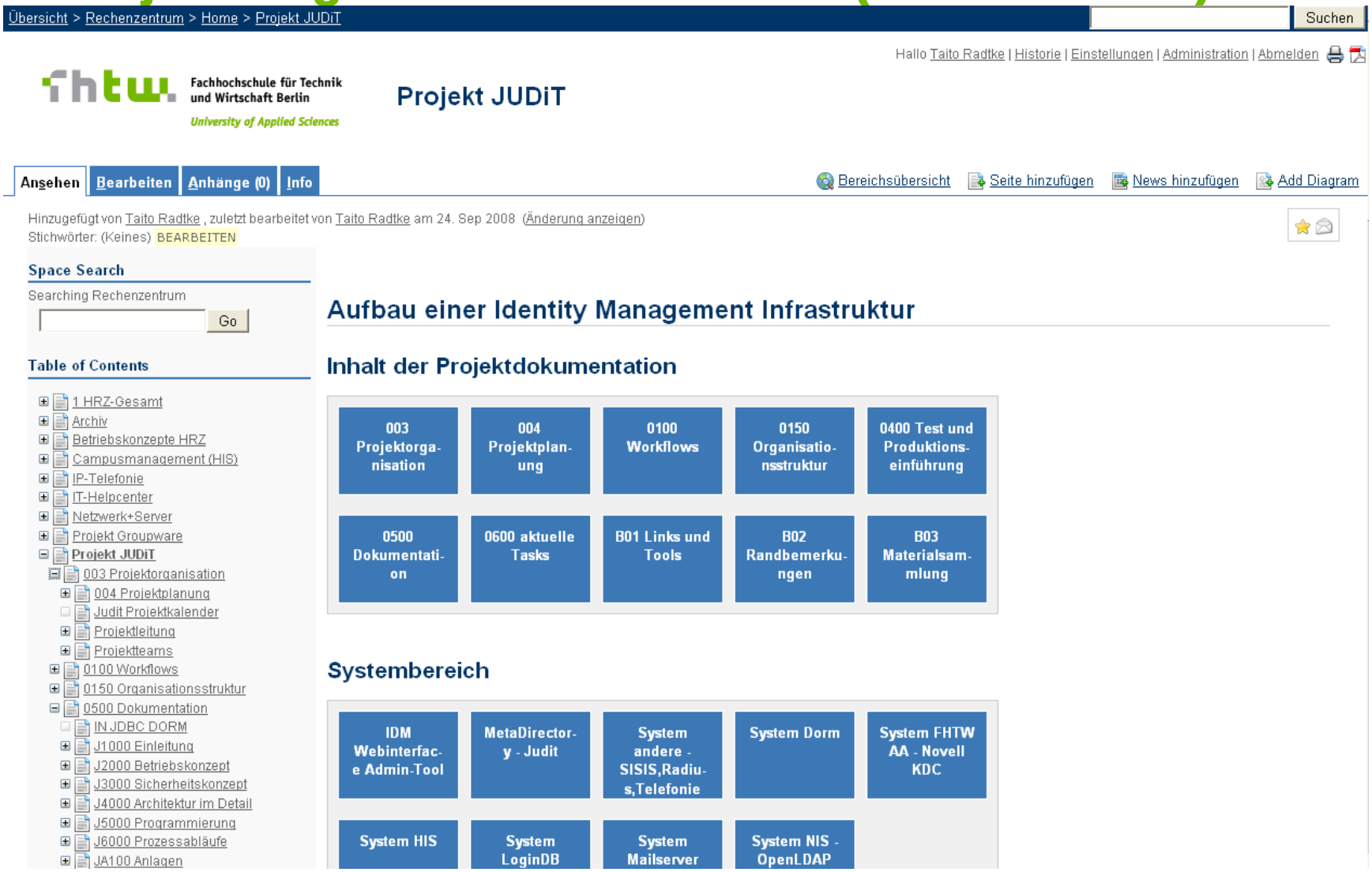
Ausgangssituation - Abläufe



JUDIT - Projektorganisation

- beteiligte Personen
  - involviert: ca. 10 Systembetreuer
  - IDM-Konzeption und -Umsetzung: 2-3 Personen
  - externe Unterstützung durch ständige Begleitung eines IDM-Spezialisten der Fa. KENOXA
- Etappe 1 (Mitte 07 – Mitte 08)
  - RZ-interne Entwicklung eines Basissystems unter Beschränkung auf eigene Prozesse und Systeme
    - openLDAP
    - NIS
    - 2x eDir (FHTW-weit und Verwaltungsbereich)
    - LSF (inkl. TAN-Erzeugung)
    - Groupware (openXchange)
  - aber(!) frühzeitige Zusammenarbeit mit Personalrat und Datenschutz-Beauftragten

Projektorganisation – Ewiki (Confluence)



JUDITs Vorbereitungen

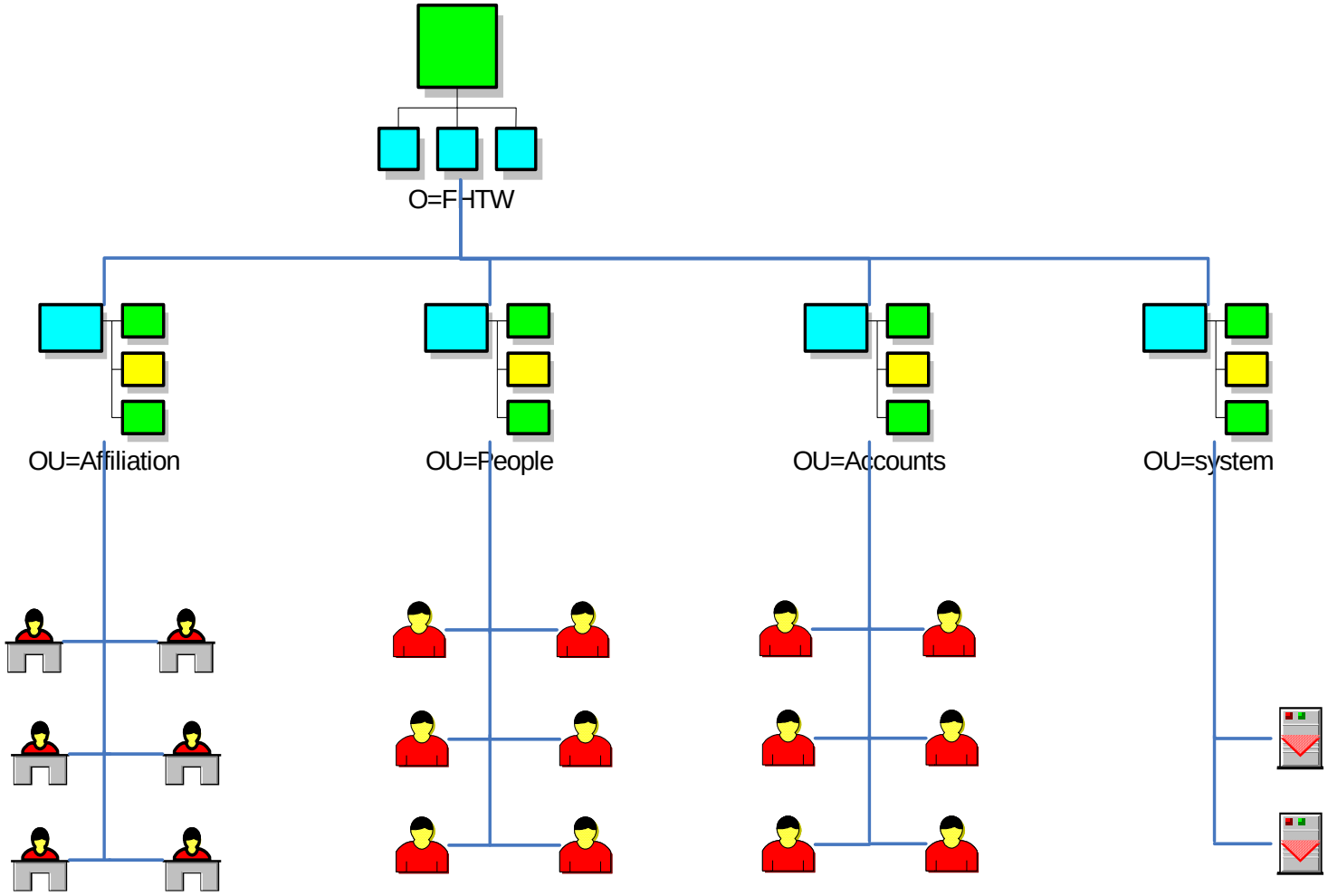
- Beobachtung größerer Universitätsprojekte (IDMOne, TUM, TUBIS...)
- Besuch CODEX-Projekt Weimar
- Entscheidung: Novell IDM (Verzeichnisbasierend)
- Schemaanlyse – wie üblich => eduPerson nicht aureichend, andere Schemaerweiterungen komplex und nicht übertragbar
- Ergebnis: wenige(!) Schemaerweiterungen
  - 5 ObjectClasses (juditEdu*)
    - eduPerson- und Organizational Role-Erweiterungen
  - 2 Auxilliary Classes (juditIDM*)
    - Steuerung des IDM und Provisionierung

JUDITs Anforderungen an ein MetaDirectory

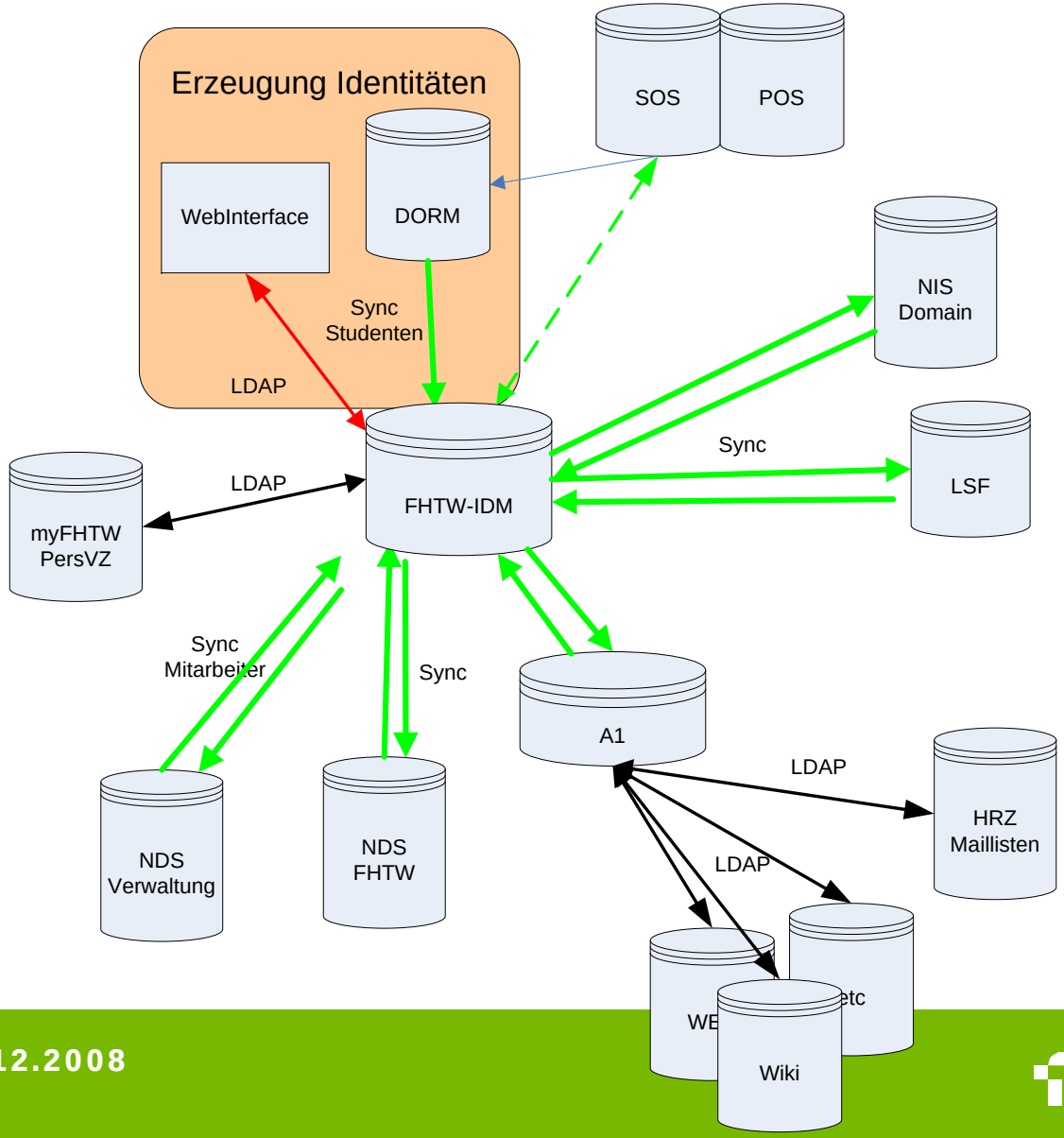
- Jede Person besitzt nur genau eine **Identität**.
- Eine Identität kann mehrere definierte **Affiliation**s (Beziehungen) zur FHTW besitzen:
  - Student, Faculty, Staff & Affiliate
- Für jede Beziehung existiert innerhalb der Organisationsstruktur mindestens eine **Rolle** (Funktion)
  - Beispiel: Dekan im FB5, Vorsitzender im ASTA
  - => Grundlage für automatische Provisionierung beliebiger Ressourcen

Abbildung = Identität + m(Affiliation + n Rollen)

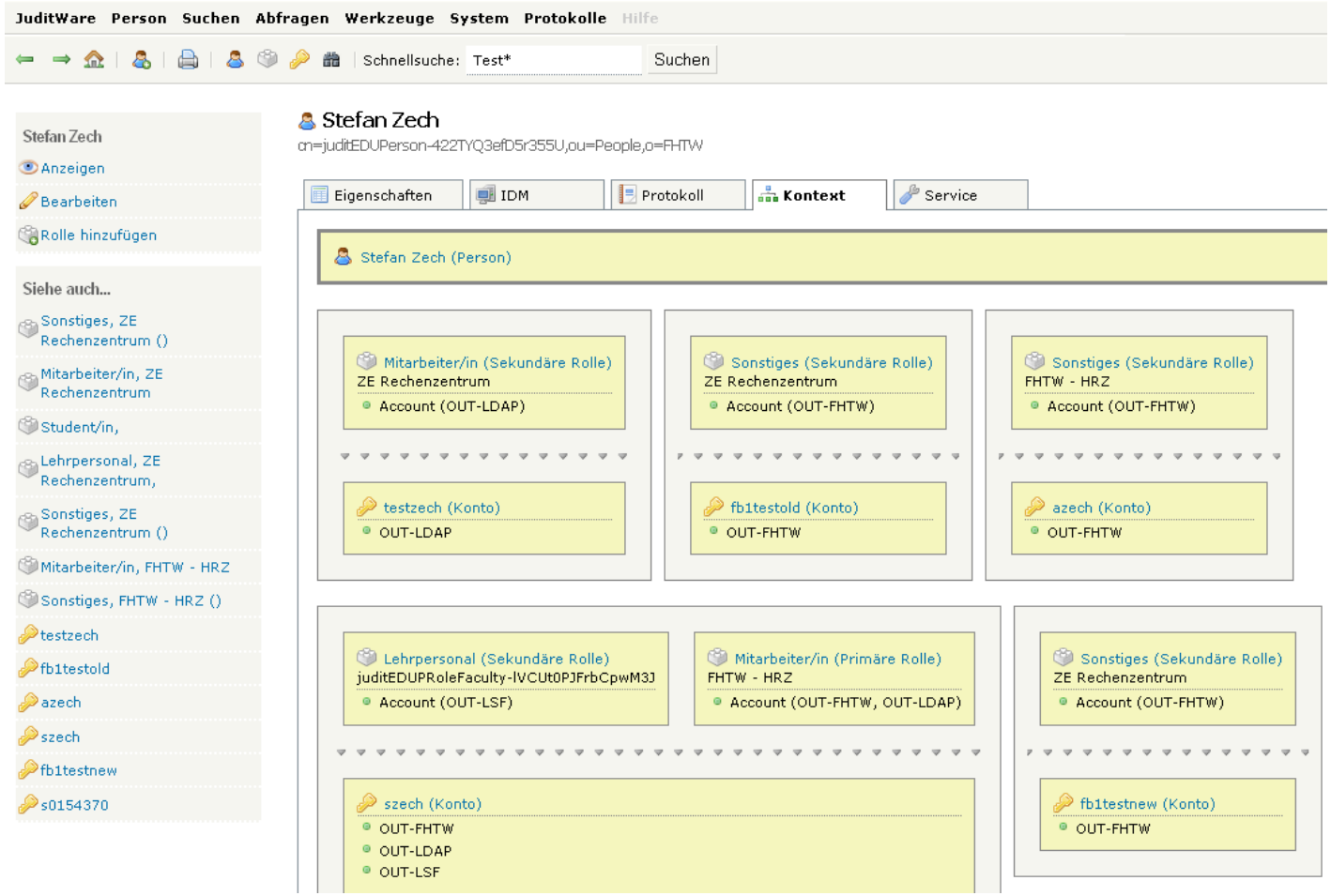
Struktur des MetaDirectory-Baums



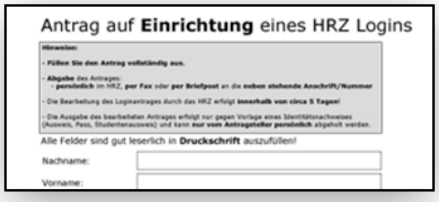
Gesamtziel - Architektur



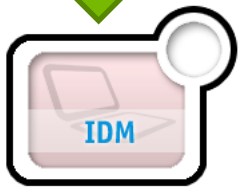
JUDITware – das Administrationsinterface



JUDIT – neuer Workflow für Accounts



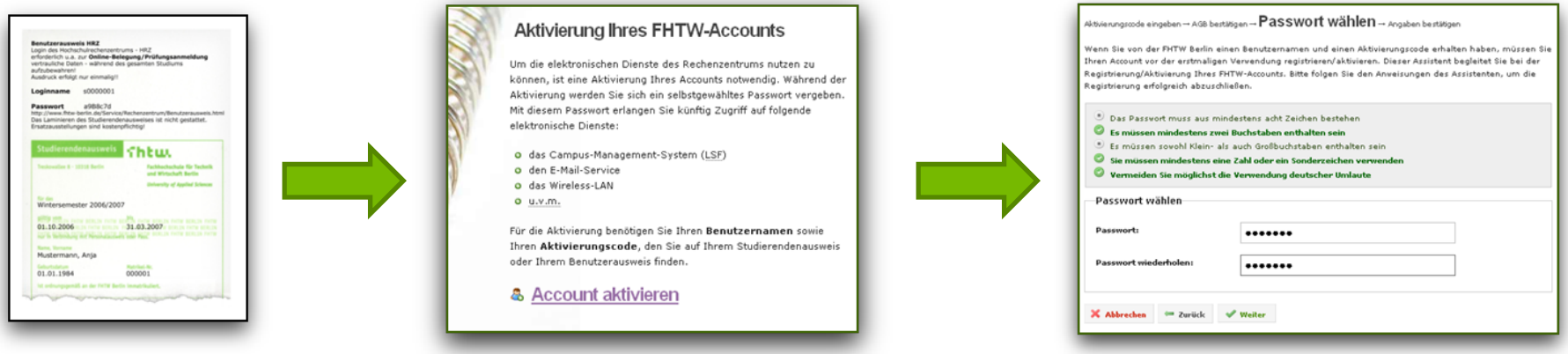
Registrierung



Benutzername & Aktivierungscode

JUDIT – Accountaktivierung

http://start.fhtw-berlin.de



JUDIT – Ausblick

- weitere Systeme anbinden
- öffentliches Registrierungsinterface – auch für nicht-Studenten inkl. Approval (Personalstelle, Bibliothek)
- Integration offizieller(!) Organisationsstruktur

Fachhochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

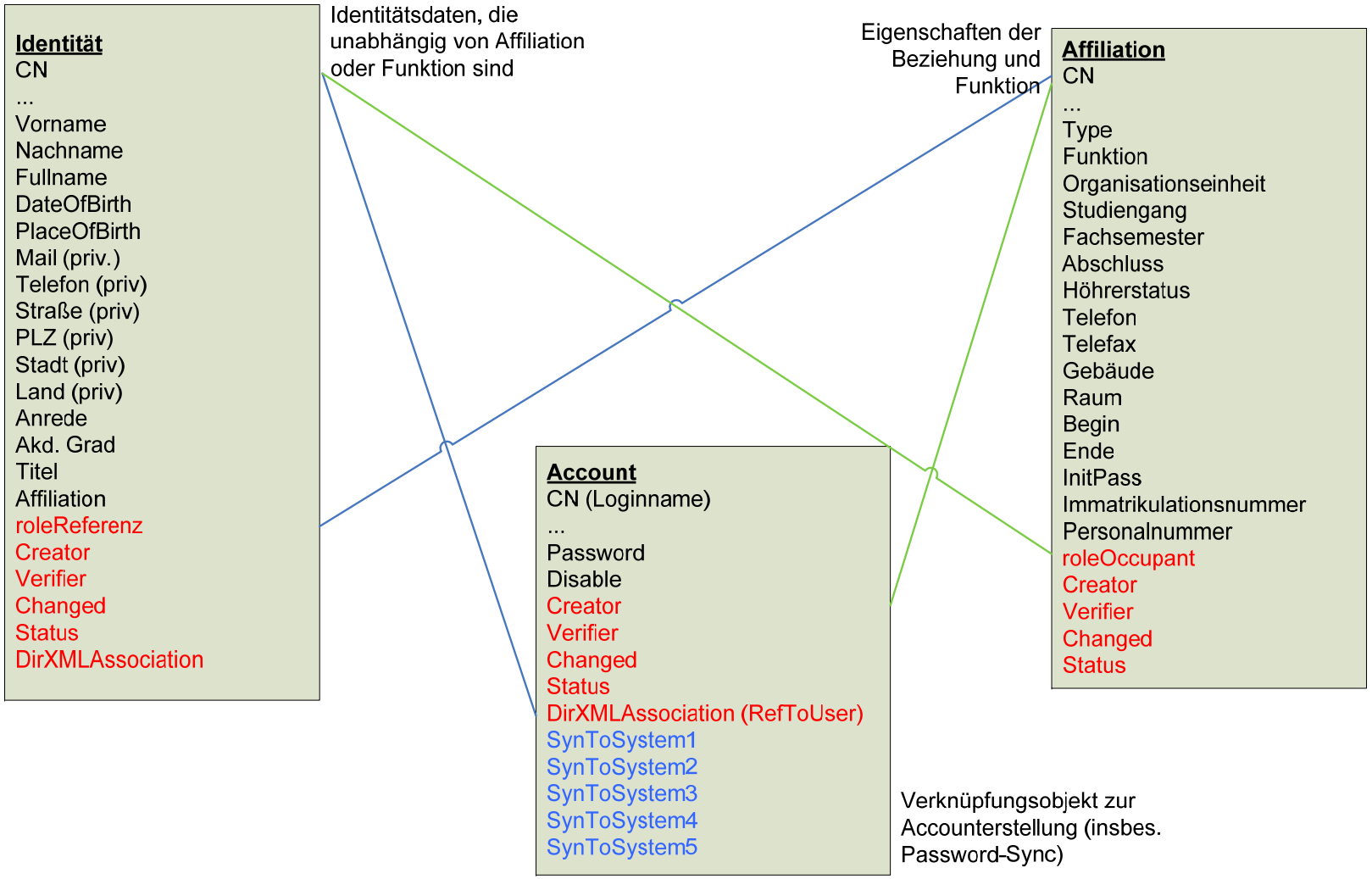
Fragen?

Fachhochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

Vielen Dank für Ihre Aufmerksamkeit!

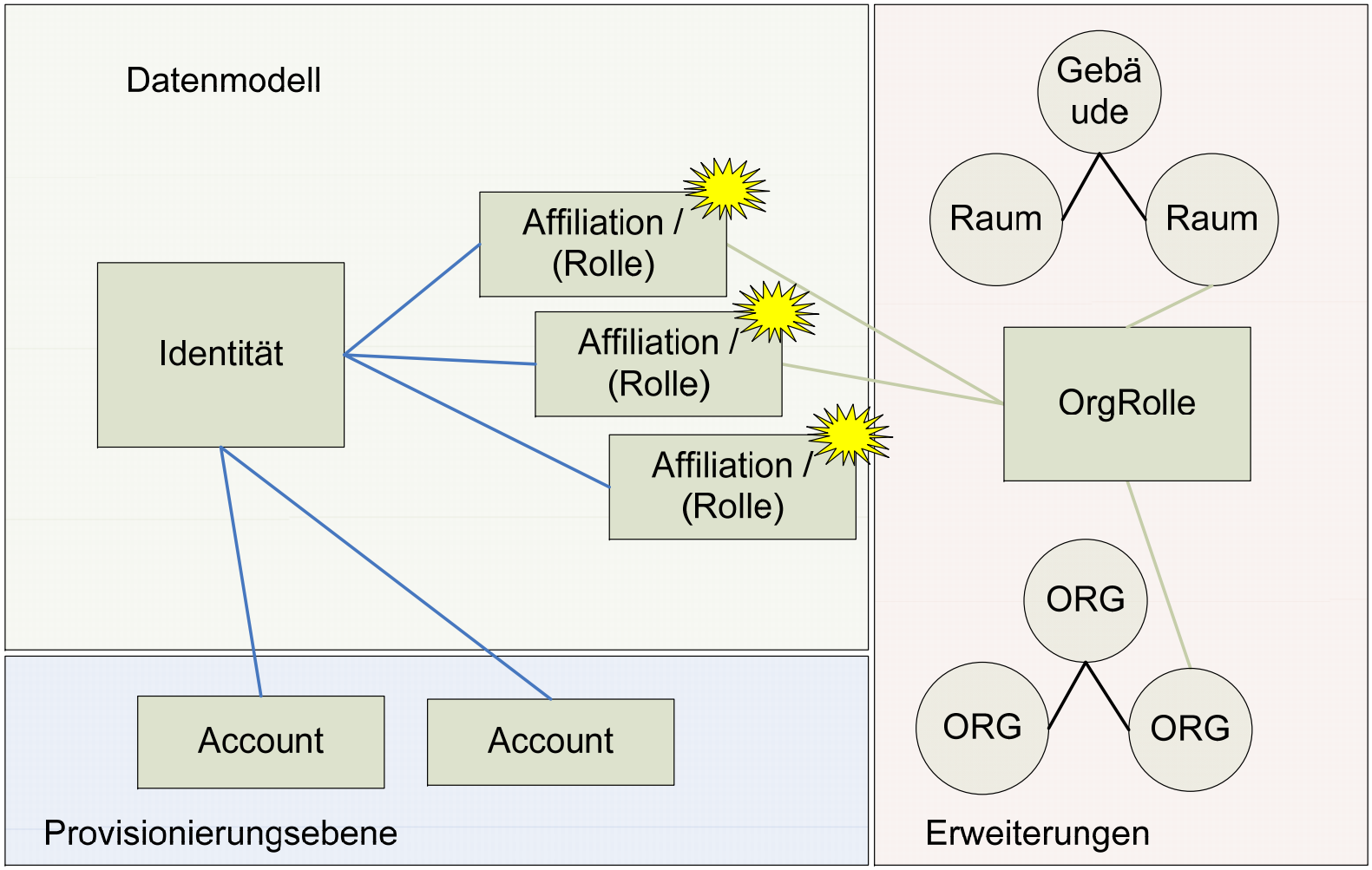
Umsetzung - Etappe 1



Verwaltung der Resource Account

- die MetaDirectory-Resource *Account* (Auszug):
  - _ein_ Loginname
  - _ein_ Passwort
  - n Zielsysteme
- Bedingungen
  - mehrere Accounts pro Identität möglich
  - automatische Provisionierung aufgrund der Rolle
- Lösung
  - Jede Identität kann mehrere Rollen besitzen
  - Jede Rolle kann zu eigenständigen Accounts führen
  - Läuft eine Rolle aus –> Deprovisionierung der betroffenen Accounts in einzelnen Systemen

Konzept – Aufbau MetaDirectory



Ausgangssituation

- ca. 9500 Studenten, ca. 800 Lehrkräfte, ca. 260 Verwaltungsangestellte
- Seit ca. 1994 Access-LoginDB im Einsatz zur Provisionierung der zentralen Systeme im HRZ
- SingleSignOn in Ansätzen
- Manuelle Erfassung gleicher Identitätsdaten in versch. Systemen (z. B. LSF, Mir, Pos) für Lehrkräfte
- Keinerlei automatischer Abgleich der Identitätsdaten nach Account-Einrichtung
- Eingeschränkte Anbindung der Fachbereiche

Gewünschte Ergebnisse

- Weniger Papierdokumente
- Weniger Anfragen an den Helpdesk
- Kostensenkungen
- Datenqualität
- Self-Service !!
- Benutzerfreundlich, problemarm
- Automatisierung u. Optimierung u.a. von: Accountantragsstellung, Datenerfassung, Passwortrücksetzung
- Produktivität für IT, Verwaltung und Fachbereiche erhöhen
- Arbeitsmotivation verbessern

Umsetzung

- Kleine Schritte („technische und psychologische Annäherung“)
- Aufbau einer gesunden Basis, danach beständiger Ausbau
- Erfahrungen anderer Hochschulen

- „Das MetaDirectory ist nicht dazu da, alle Probleme in Prozessen oder IT-Systemen zu lösen!“ (Codex Projektgruppe)

Das Projekt

- Organisation
- Hauptpunkte
- Projektetappenplan
- Projekt-Etappe 1
- Überblick Teilphasen Etappe 1
- Momentaner Projektstand
- Technologietag 2 – Arbeit in Gruppen

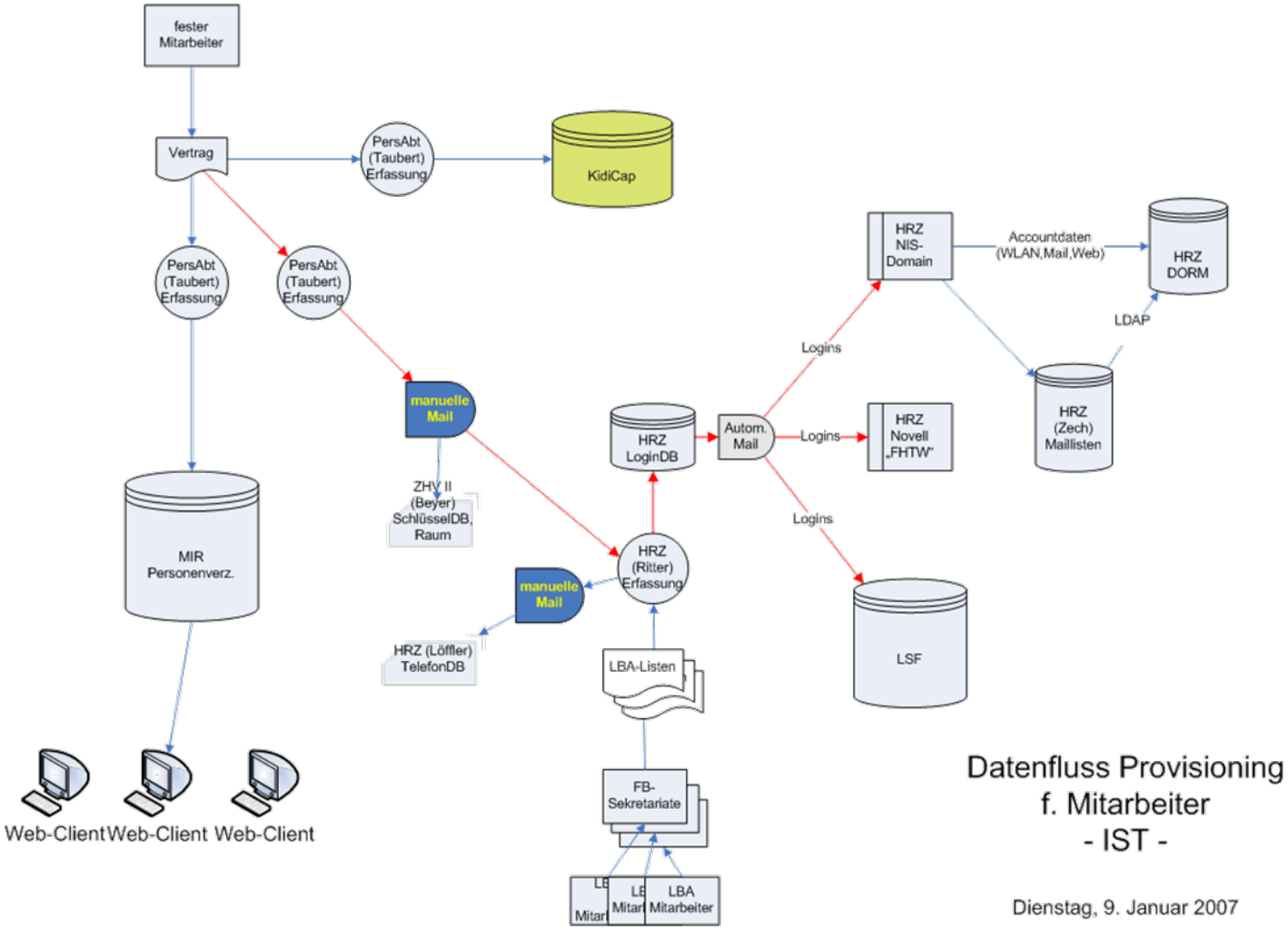
Projektorganisation

- 5 Teilgruppen
- Teilgruppe Basis, AA, HIS, SISIS, Workflow
- Absprachen Arbeitspakete mit Teilprojektleitern
- Teilprojektleiter organisieren Umsetzung AP in Gruppen
- Zeitliche Verbindlichkeit für Projekt-Etappen
- Konzeptionelle Arbeit in Gruppen ausbauen
- Projekt muss gelebt werden
- Fragen, Ideen, Verbesserungen jederzeit willkommen!

Projekthauptpunkte

- Analyse der Daten und Autorisierung
- Konzeptionelles Design einer zentralen Identitätsverwaltung
- Implementierung einer Prototypumgebung
- Weiterentwicklung zu einer Finalimplementierung
- Entwicklung eines Sicherheitskonzeptes und Weiterentwicklung der IDM-Lösung
- Integration weiterer Identitätenverzeichnisse
- Integration der IDM-Lösung in regionale/globale IDM-Strukturen (Shibboleth)

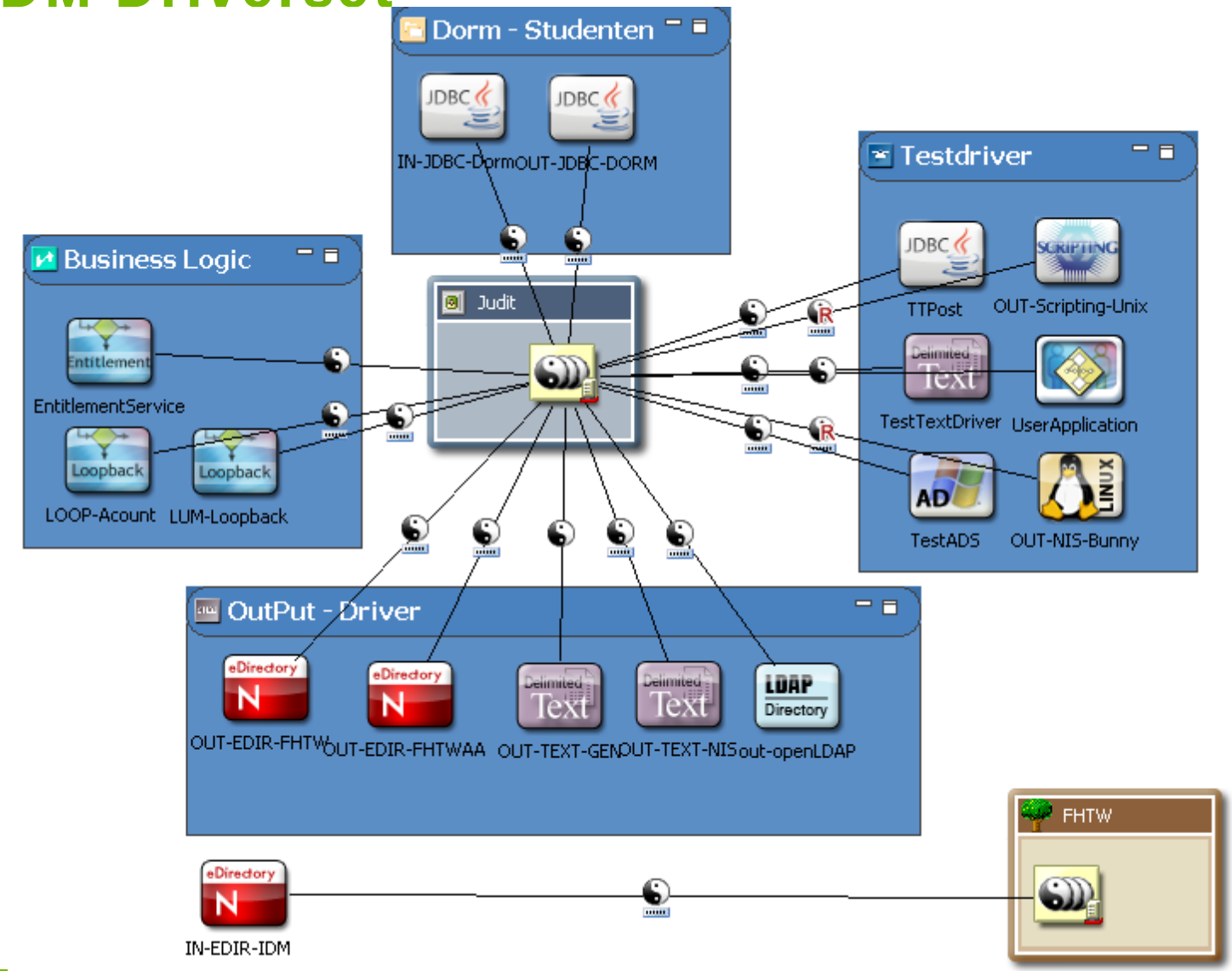
Ausgangssituation



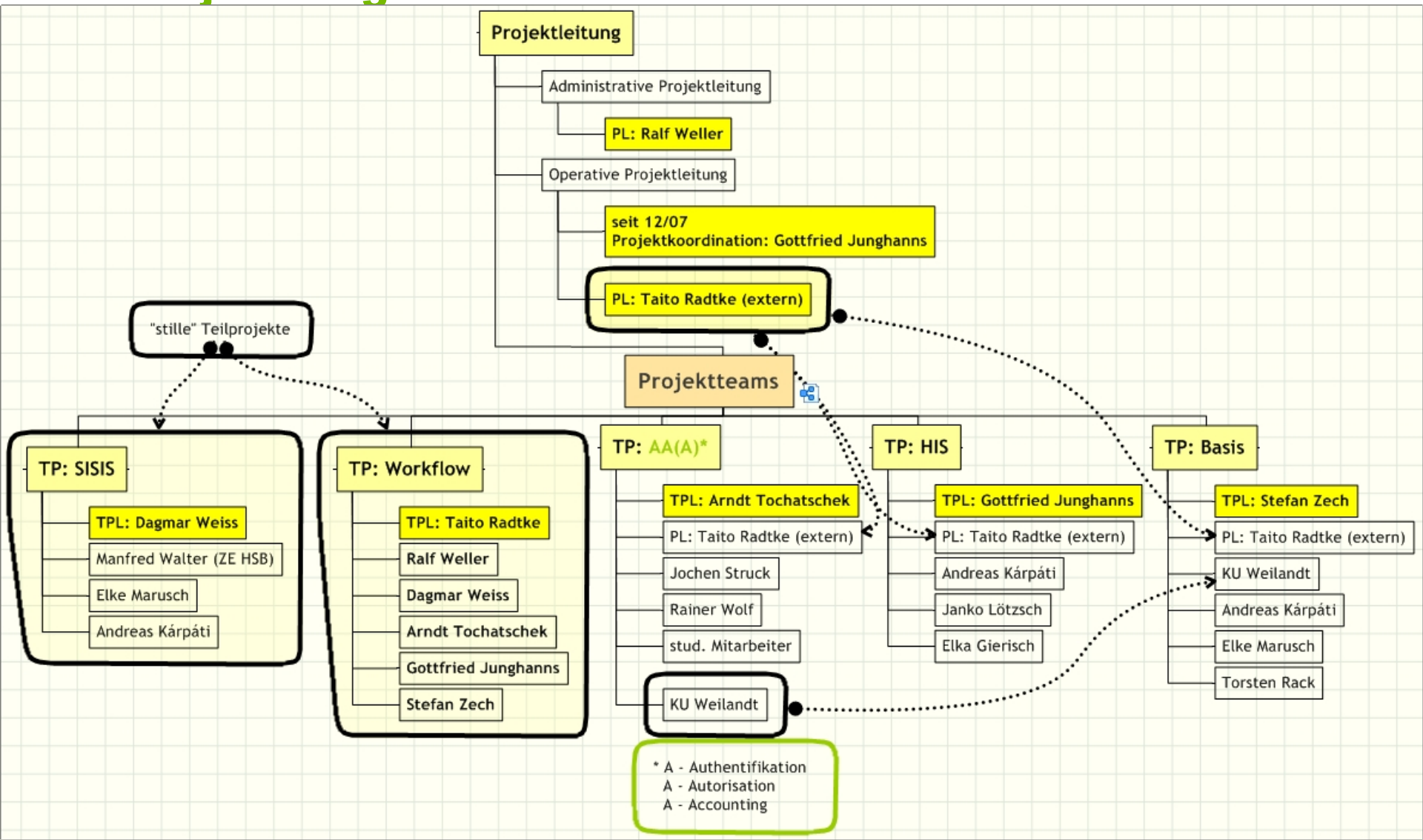
Schema für das MetaDirectory

- Schema aufbauend auf Person, inetOrgPerson, organizationalRole und eigenen Erweiterungen (fhtwEduPerson, fhtwEduRole,...)
- (!) interne Strukturen und Schema sind nur für die IDM Verarbeitung interessant
- wird durch Treiber in standardkonforme Schemata überführt => Shibboleth (eduPerson), Kerberos, possixAccount, ...
- => Möglichkeiten der Datentransformation durch IDM

IDM Driverset



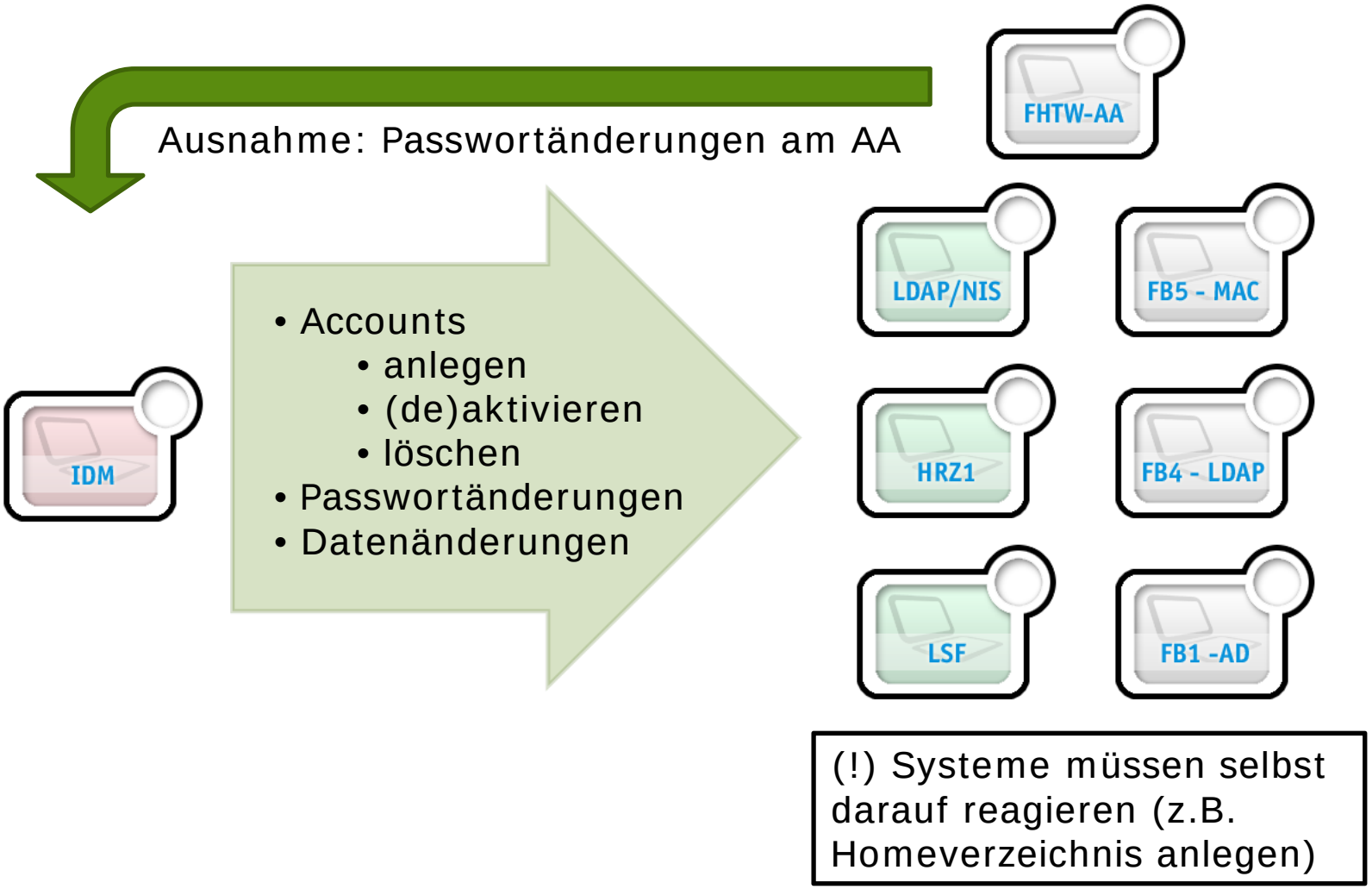
Projektorganisation



JUDIT – Funktionen des IDM-Systems

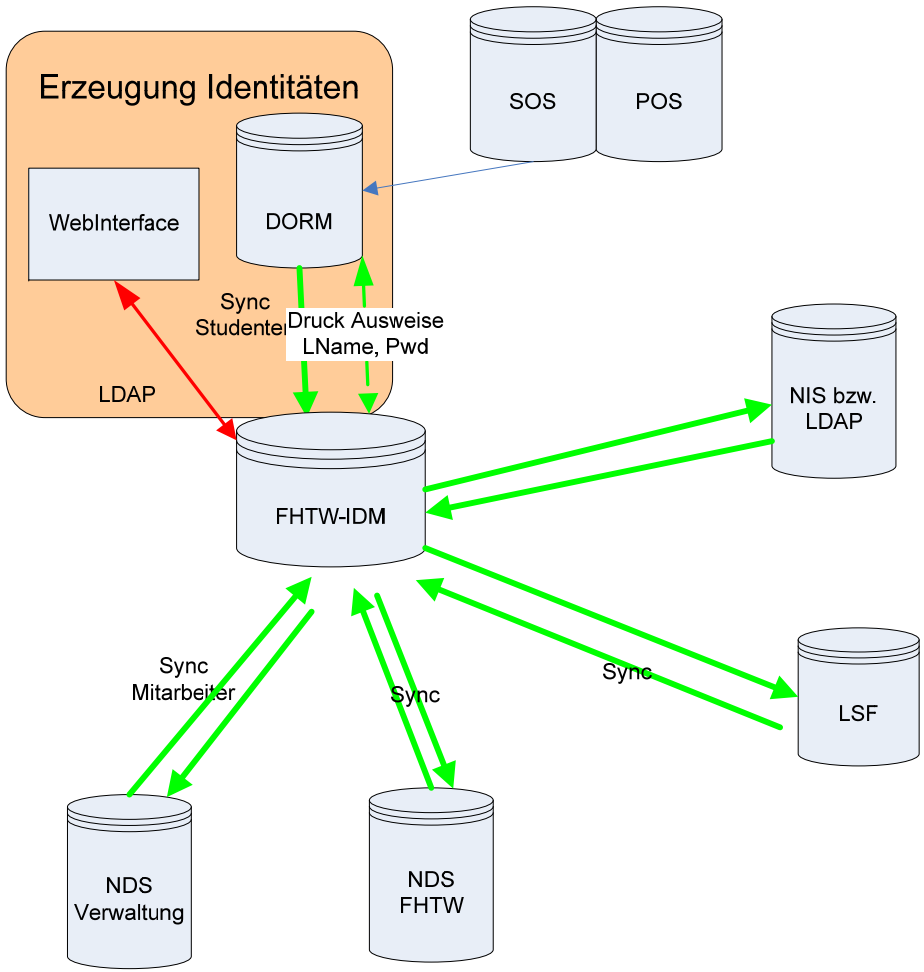
- Erzeugung des Benutzernamens
- Erzeugung Aktivierungscode
- Aktivierung der Nutzer
- Erzeugung der Ressource Account
  - Einrichtung und Löschung in den angebundenen Systemen
    - Netware, NIS/openLDAP
- Verwaltung des Passworts

JUDIT – Arbeitsweise des IDM-Systems



(!) Systeme müssen selbst darauf reagieren (z.B. Homeverzeichnis anlegen)

Istzustand


Erzeugung Identitäten
WebInterface
DORM
SOS
POS
Sync
Studenten
Druck Ausweise
LName, Pwd
LDAP
NIS bzw.
LDAP
FHTW-IDM
Sync
Mitarbeiter
Sync
Sync
LSF
NDS
Verwaltung
NDS
FHTW

Projektziele Etappe 1

1. Analyse der Abläufe zur Provisionierung von Identitätsinformationen **im Umfeld der vom HRZ betriebenen Systeme und Verfahren.**
2. Herausarbeiten der autoritativen Quellsysteme für Identitätsdaten sowie der wesentlichen Zielsysteme für Identitätsdaten.
3. Erstellen Konzept eines Identitätsmanagementsystems (IDMS).
4. Auswahl und Implementation eines Kernsystems als techn. Plattform für ein IDMS.
5. Programmierung der Treiber zwischen IDMS und Quell- und Zielsysteme.
6. Entwicklung und Test eines Verfahrens zur Zusammenführung der Identitätsdatendaten der vorhandenen autoritativen Quellsysteme und Initialbefüllung des IDMS