



**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

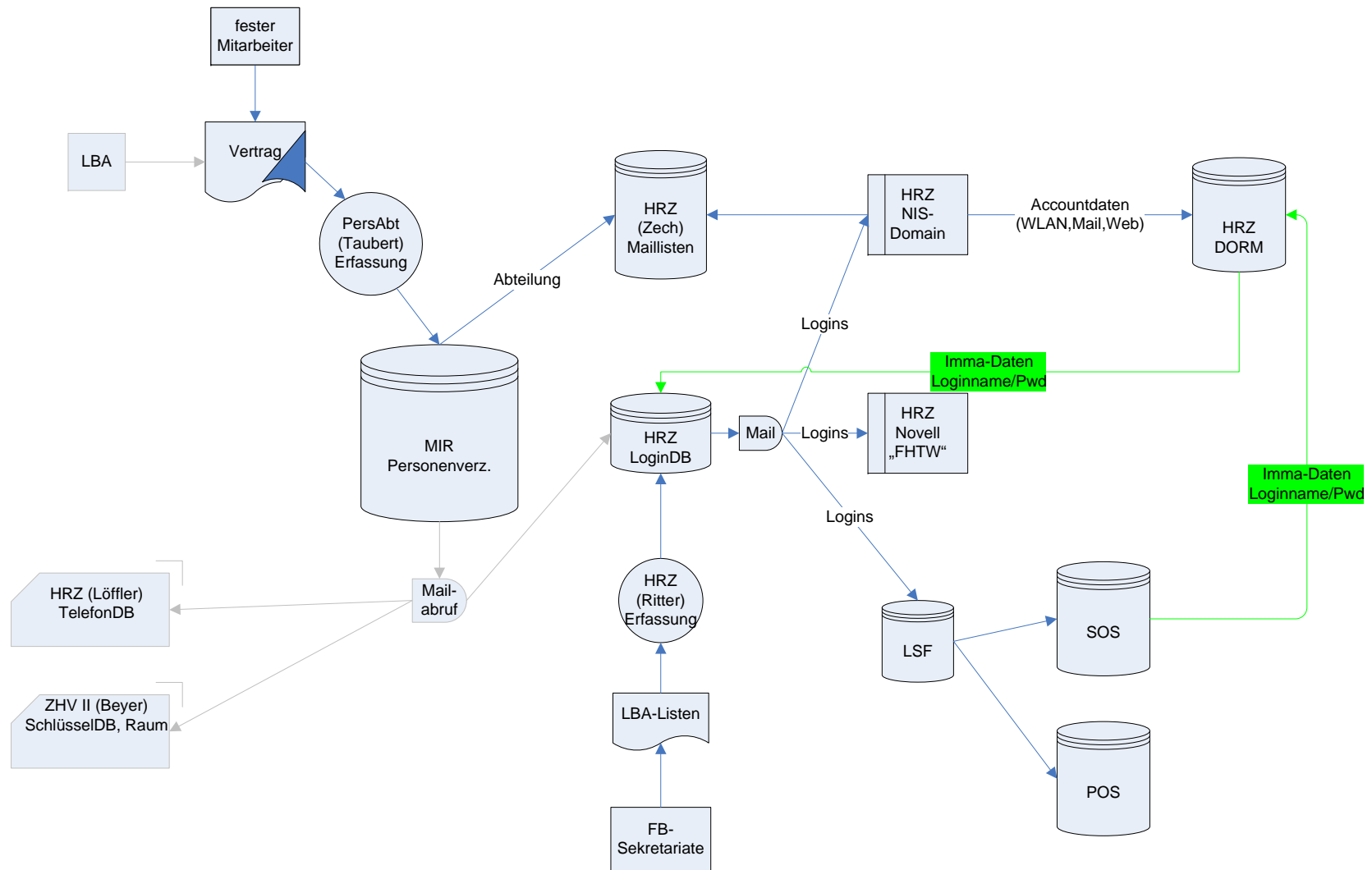
Agenda

- 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. KENOX
- 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)

[Übersicht](#) > [Rechenzentrum](#) > [Home](#) > [Projekt JUDiT](#)

Suchen

Ansehen **Bearbeiten** **Anhänge (0)** **Info**

 [Bereichsübersicht](#)  [Seite hinzufügen](#)  [News hinzufügen](#)  [Add Diagram](#)

Hinzugefügt von [Taito Radtke](#), zuletzt bearbeitet von [Taito Radtke](#) am 24. Sep 2008 ([Änderung anzeigen](#))

Stichwörter: (Keines) **BEARBEITEN**



Space Search

Searching Rechenzentrum

Table of Contents

-  1 HRZ-Gesamt
 -  Archiv
 -  Betriebskonzepte HRZ
 -  Campusmanagement (HIS)
 -  IP-Telefonie
 -  IT-Helpcenter
 -  Netzwerk+Server
 -  Projekt Groupware
 -  **Projekt JUDiT**
 -  003 Projektorganisation
 -  004 Projektplanung
 -  Judit Projektkalender
 -  Projektleitung
 -  Projektteams
 -  0100 Workflows
 -  0150 Organisationsstruktur
 -  0500 Dokumentation
 -  IN JDBC DORM
 -  J1000 Einleitung
 -  J2000 Betriebskonzept
 -  J3000 Sicherheitskonzept
 -  J4000 Architektur im Detail
 -  J5000 Programmierung
 -  J6000 Prozessabläufe
 -  JA100 Anlagen

Aufbau einer Identity Management Infrastruktur

Inhalt der Projektdokumentation

003 Projektorga- nisation	004 Projektplan- ung	0100 Workflows	0150 Organisatio- nsstruktur	0400 Test und Produktions- einführung
0500 Dokumentati- on	0600 aktuelle Tasks	B01 Links und Tools	B02 Randbemerku- ngen	B03 Materialsam- mlung

Systembereich

IDM Webinterfac- e Admin-Tool	MetaDirector- y - Judit	System andere - SISIS,Radiu- s,Telefonie	System Dorm	System FHTW AA - Novell KDC
System HIS	System LoginDB	System Mailserver	System NIS - OpenLDAP	

JUDITs Vorbereitungen

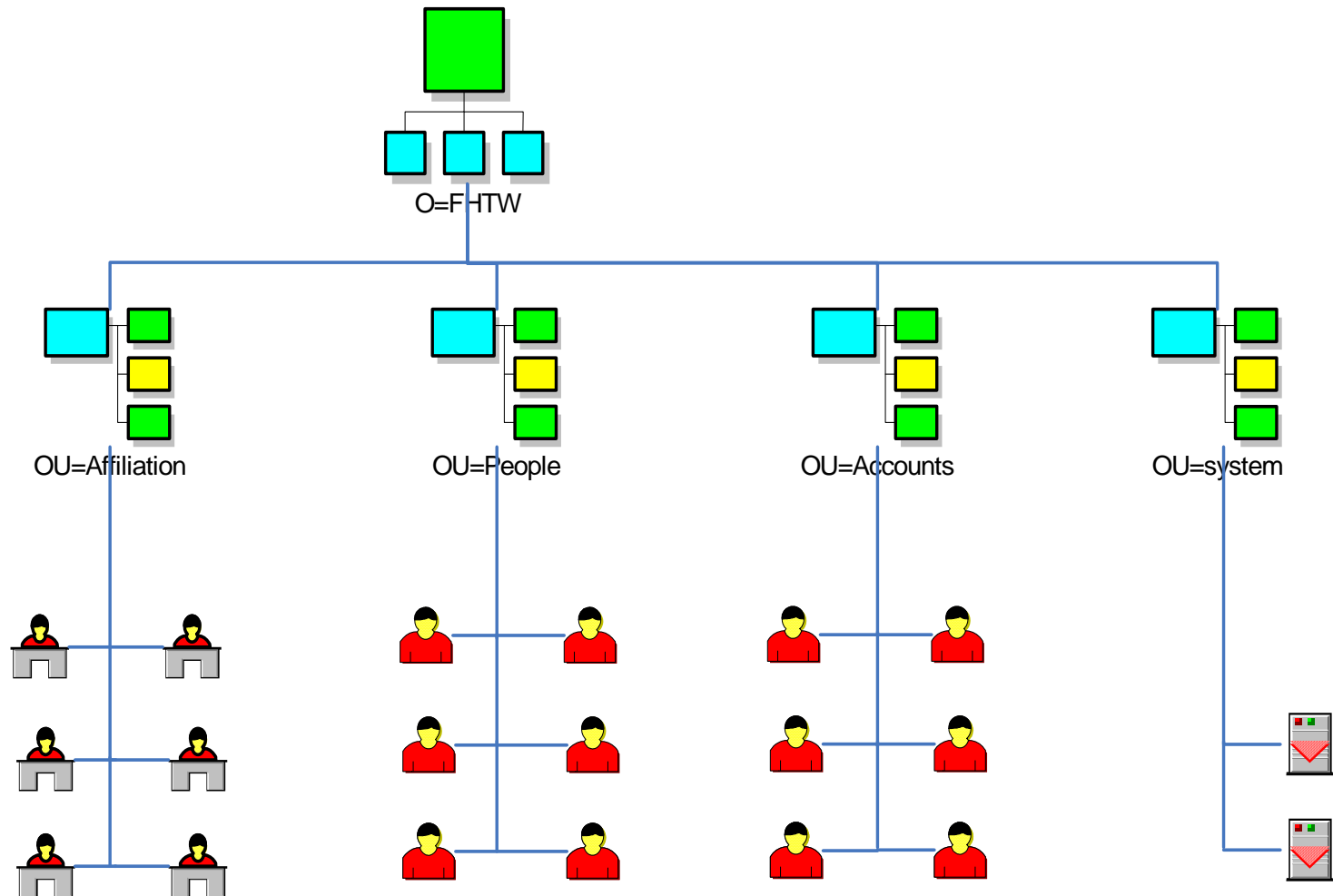
- Beobachtung größerer Universitätsprojekte (IDMOne, TUM, TUBIS...)
- Besuch CODEX-Projekt Weimar
- Entscheidung: Novell IDM (Verzeichnisbasierend)
- Schemaanalyse – wie üblich => eduPerson nicht ausreichend, andere Schemaerweiterungen komplex und nicht übertragbar
- Ergebnis: wenige(!) Schemaerweiterungen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

JUDITs Anforderungen an ein MetaDirectory

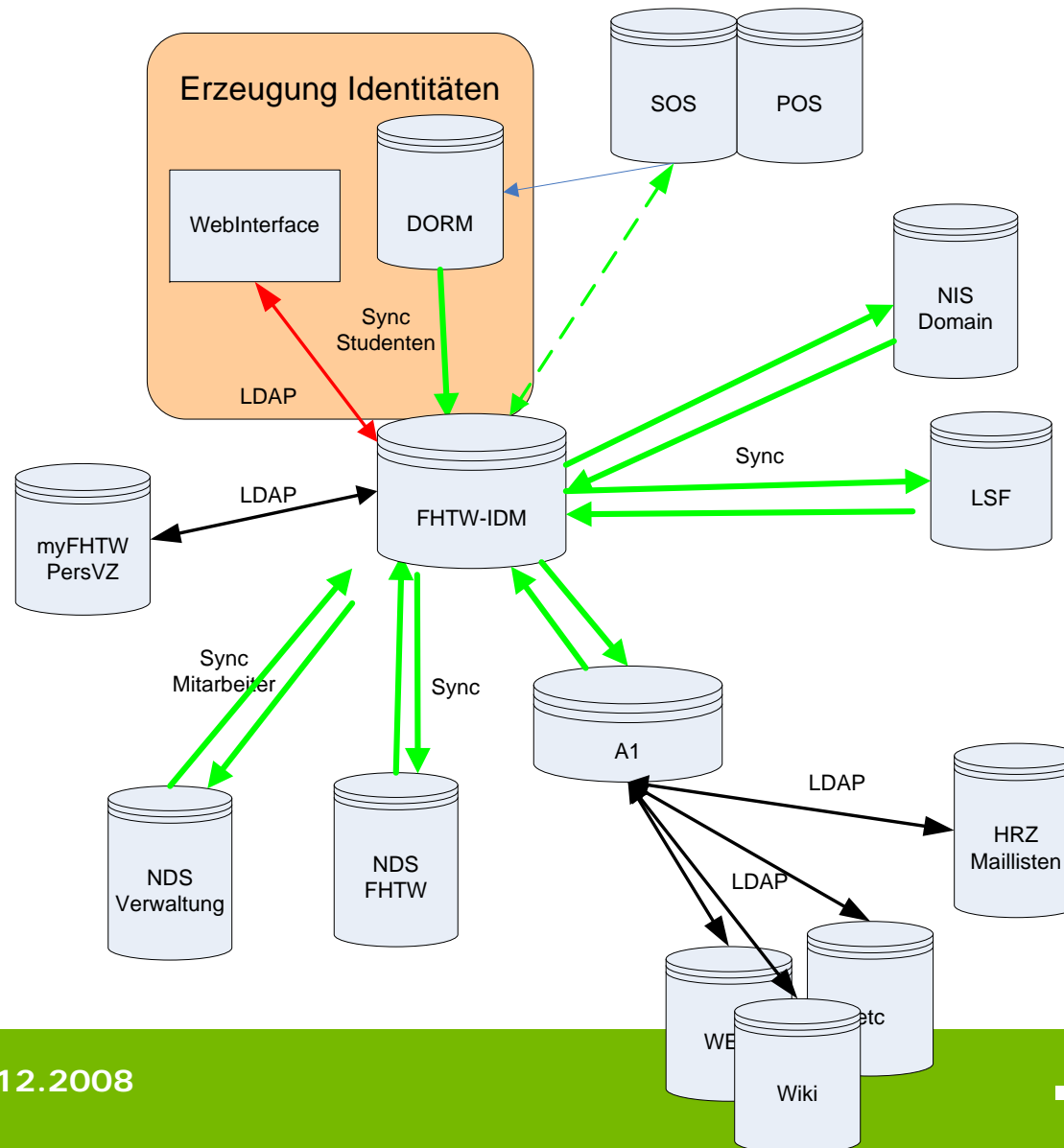
- Jede Person besitzt nur genau eine **Identität**.
- Eine Identität kann mehrere definierte **Affiliations** (Beziehungen) zur FHTW besitzen:
 - Student, Faculty, Staff & Affiliate
- Für jede Beziehung existiert innerhalb der Organisationsstruktur mindestens eine **Rolle** (Funktion)
 - Beispiel: Dekan 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

JuditWare Person Suchen Abfragen Werkzeuge System Protokolle Hilfe

← → 🏠 👤 🖨️ 🗄️ 🔑 📅 | Schnellsuche:

Stefan Zech

[Anzeigen](#)

[Bearbeiten](#)

[Rolle hinzufügen](#)

Siehe auch...

- [Sonstiges, ZE Rechenzentrum \(\)](#)
- [Mitarbeiter/in, ZE Rechenzentrum](#)
- [Student/in,](#)
- [Lehrpersonal, ZE Rechenzentrum,](#)
- [Sonstiges, ZE Rechenzentrum \(\)](#)
- [Mitarbeiter/in, FHTW - HRZ](#)
- [Sonstiges, FHTW - HRZ \(\)](#)
- [testzech](#)
- [fb1testold](#)
- [azech](#)
- [szech](#)
- [fb1testnew](#)
- [s0154370](#)

Stefan Zech
on=juditEDUPerson-422TYQ3efD5r355U,ou=People,p=FHTW

Stefan Zech (Person)

<p> Mitarbeiter/in (Sekundäre Rolle) ZE Rechenzentrum</p> <ul style="list-style-type: none">Account (OUT-LDAP)	<p> Sonstiges (Sekundäre Rolle) ZE Rechenzentrum</p> <ul style="list-style-type: none">Account (OUT-FHTW)	<p> Sonstiges (Sekundäre Rolle) FHTW - HRZ</p> <ul style="list-style-type: none">Account (OUT-FHTW)
<p> testzech (Konto)</p> <ul style="list-style-type: none">OUT-LDAP	<p> fb1testold (Konto)</p> <ul style="list-style-type: none">OUT-FHTW	<p> azech (Konto)</p> <ul style="list-style-type: none">OUT-FHTW

<p> Lehrpersonal (Sekundäre Rolle) juditEDUPRoleFaculty-IVCUT0PJFrBcPwM3J</p> <ul style="list-style-type: none">Account (OUT-LSF)	<p> Mitarbeiter/in (Primäre Rolle) FHTW - HRZ</p> <ul style="list-style-type: none">Account (OUT-FHTW, OUT-LDAP)	<p> Sonstiges (Sekundäre Rolle) ZE Rechenzentrum</p> <ul style="list-style-type: none">Account (OUT-FHTW)
<p> szech (Konto)</p> <ul style="list-style-type: none">OUT-FHTWOUT-LDAPOUT-LSF		<p> fb1testnew (Konto)</p> <ul style="list-style-type: none">OUT-FHTW

JUDIT – neuer Workflow für Accounts

Antrag auf Einrichtung eines HRZ Logins

Hinweisen:

- Füllen Sie den Antrag vollständig aus.
- Abgabe des Antrags:
 - persönlich im HRZ, per Fax oder per Briefpost an die neben stehende Anschrift/Nummer
- Die Bearbeitung des Loginantrages durch das HRZ erfolgt innerhalb von circa 5 Tagen!
- Die Ausgabe des bearbeiteten Antrages erfolgt nur gegen Vorlage eines Identitätsnachweises (Personalausweis, Pass, Studierendenausweis) und kann nur vom Antragsteller persönlich abgeholt werden.

Alle Felder sind gut lesbarlich in **Druckschrift** auszufüllen!

Nachname:

Vorname:

Registrierung

fhtw Fachhochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Online-Bewerbung

1. Einrichtung
2. Informationen
3. Bedingungen
4. Angaben zur Person
5. Fachauswahl
6. Studiengang
7. Studienjahr
8. Studiengang
9. Studiengang
10. Studienrichtung

Online-Bewerbung Time-Out in: 29:54

Angaben zur Person

Persönliche Daten:

* Nachname:

* Vorname:

* Geschlecht: (Bitte auswählen)



24. Jul 2008

Betreff: Einrichtung eines FHTW-Accounts

Sehr geehrte Benutzerin, sehr geehrter Benutzer Weller,

im Hochschulrechenzentrum (HRZ) der FHTW Berlin wurde für Sie ein FHTW-Account erstellt. Die Daten zu Ihrem Account entnehmen Sie bitte dem folgenden Benutzerausweis:

Benutzerausweis für Ralf Weller	
Benutzername:	weller
Aktivierungscode:	L33Q-B886-249W-W32P
Malladresse:	weller@fhtw-berlin.de

Bitte beachten Sie unbedingt die umseitigen Hinweise zu Ihrem FHTW-Account.

Benutzername & Aktivierungscode

Benutzerausweis HRZ

Liegen das Hochschulrechenzentrum (HRZ) erforderlich u.a. zur **Online-Bewerbung/Prüfungsanmeldung** aufzunehmen! während des gesamten Studiums aufbewahren! Austausch erfolgt nur einmalig!

Loginname: u0000001

Passwort: w0000-7id
http://www.fhtw-berlin.de/Service/Rechenzentrum/Benutzerausweis.html
Das Löschende des Studierendenausweises ist nicht gestattet. Ersatzanmeldungen sind kostenpflichtig!

Studierendenausweis fhtw

Technische 9 - 10118 Berlin
Fachhochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Vorname: Wintersemester 2006/2007

geboren am: 01.10.2006
Geburtsort: Berlin

geboren am: 31.03.2007
Geburtsort: Berlin

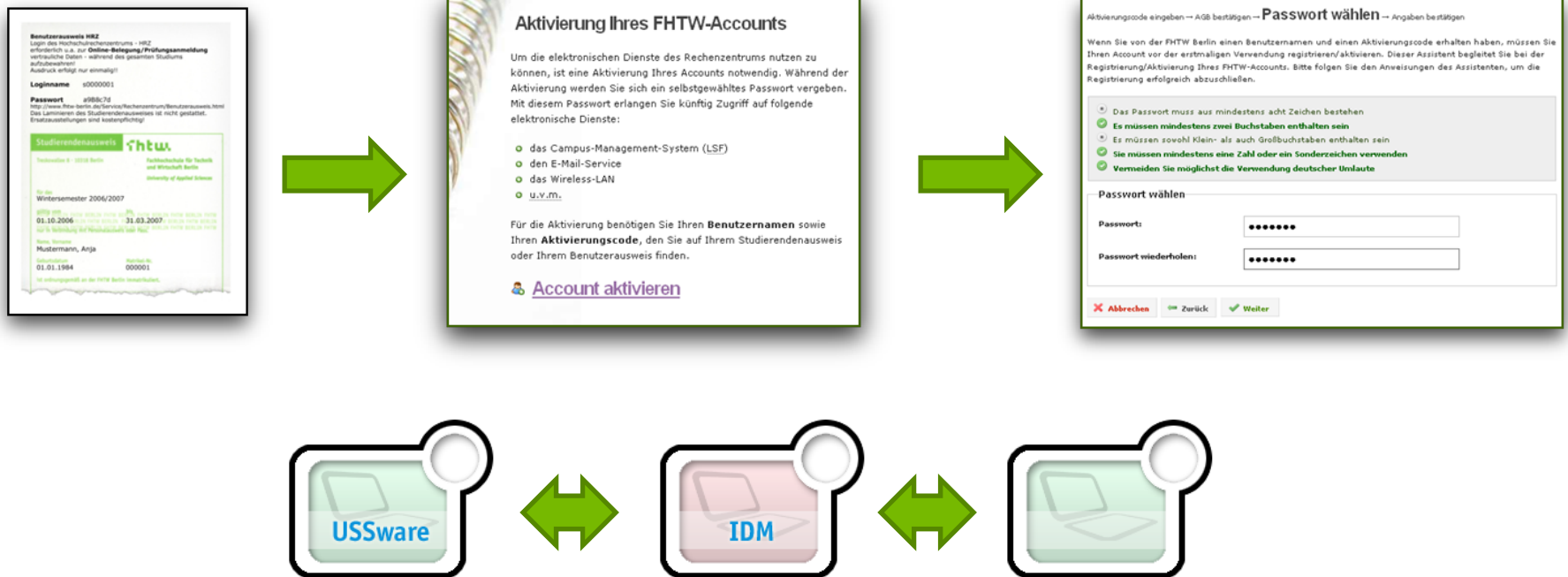
Vorname: Mittermann, Anja

geboren am: 01.01.1984
Geburtsort: Berlin

ist eingetragen bei der FHTW Berlin beantragt.

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?

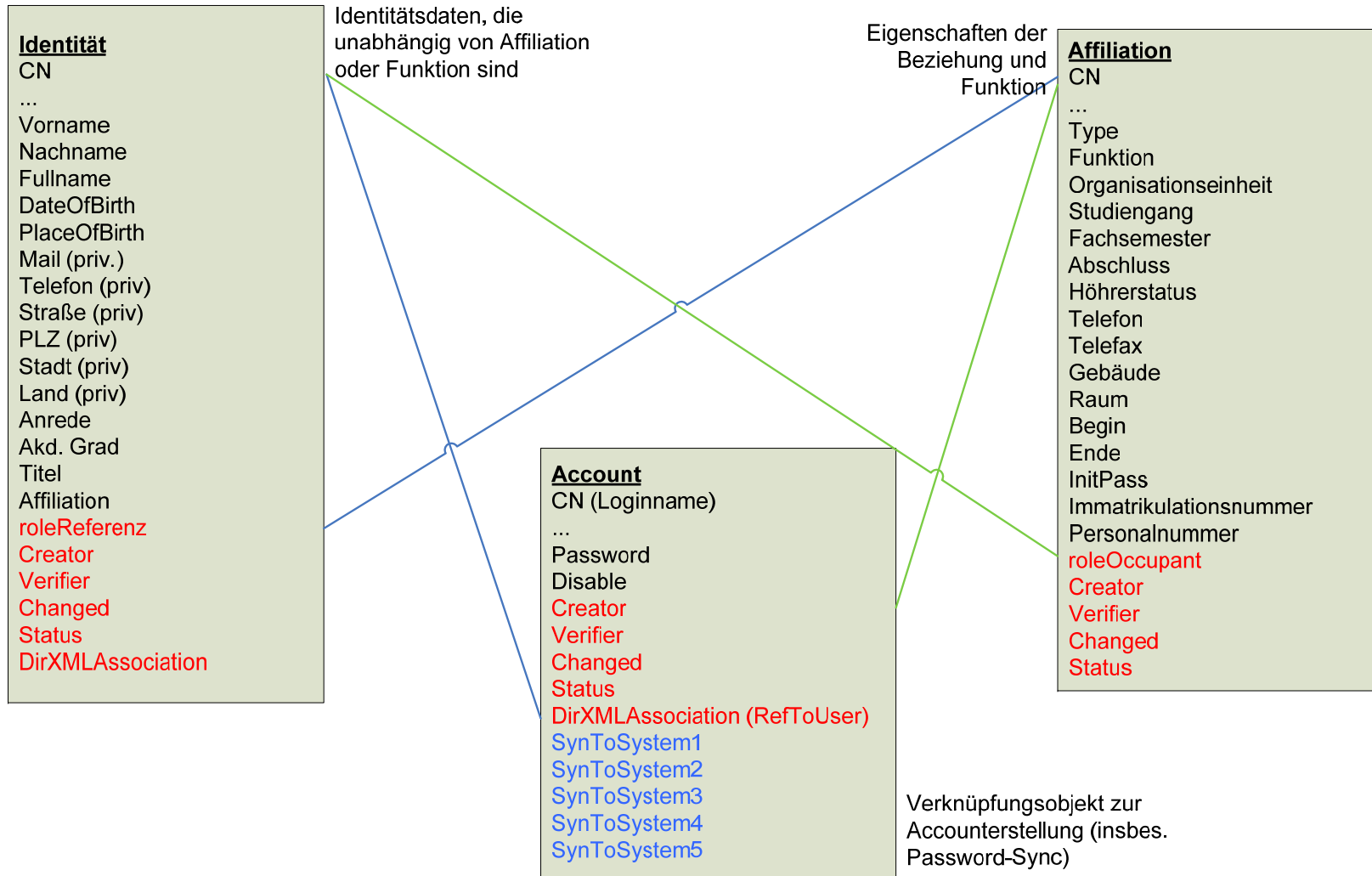


Fachhochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

**Vielen Dank für Ihre
Aufmerksamkeit!**

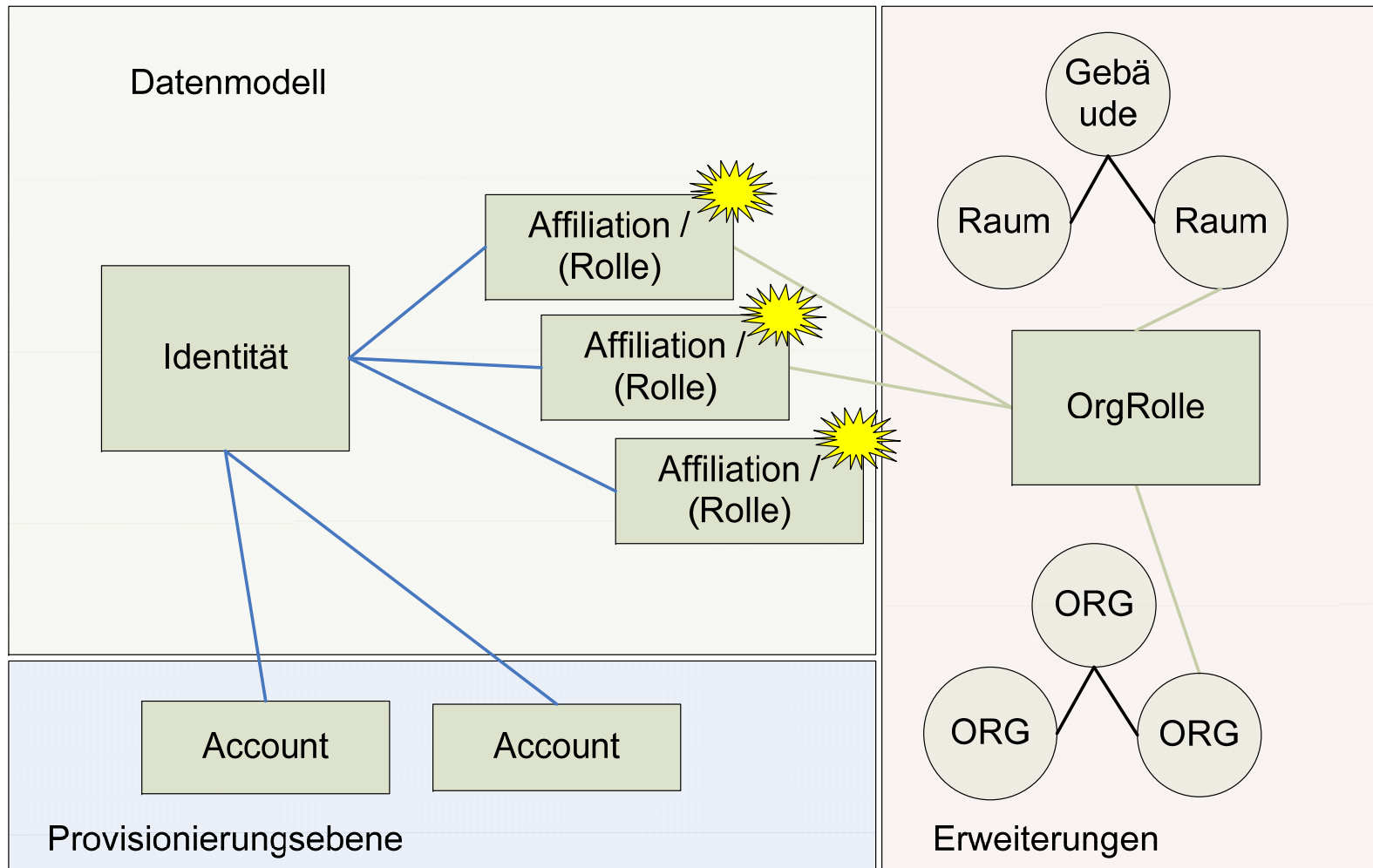
Umsetzung - Etappe 1



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, Passwörterücksetzung
- 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

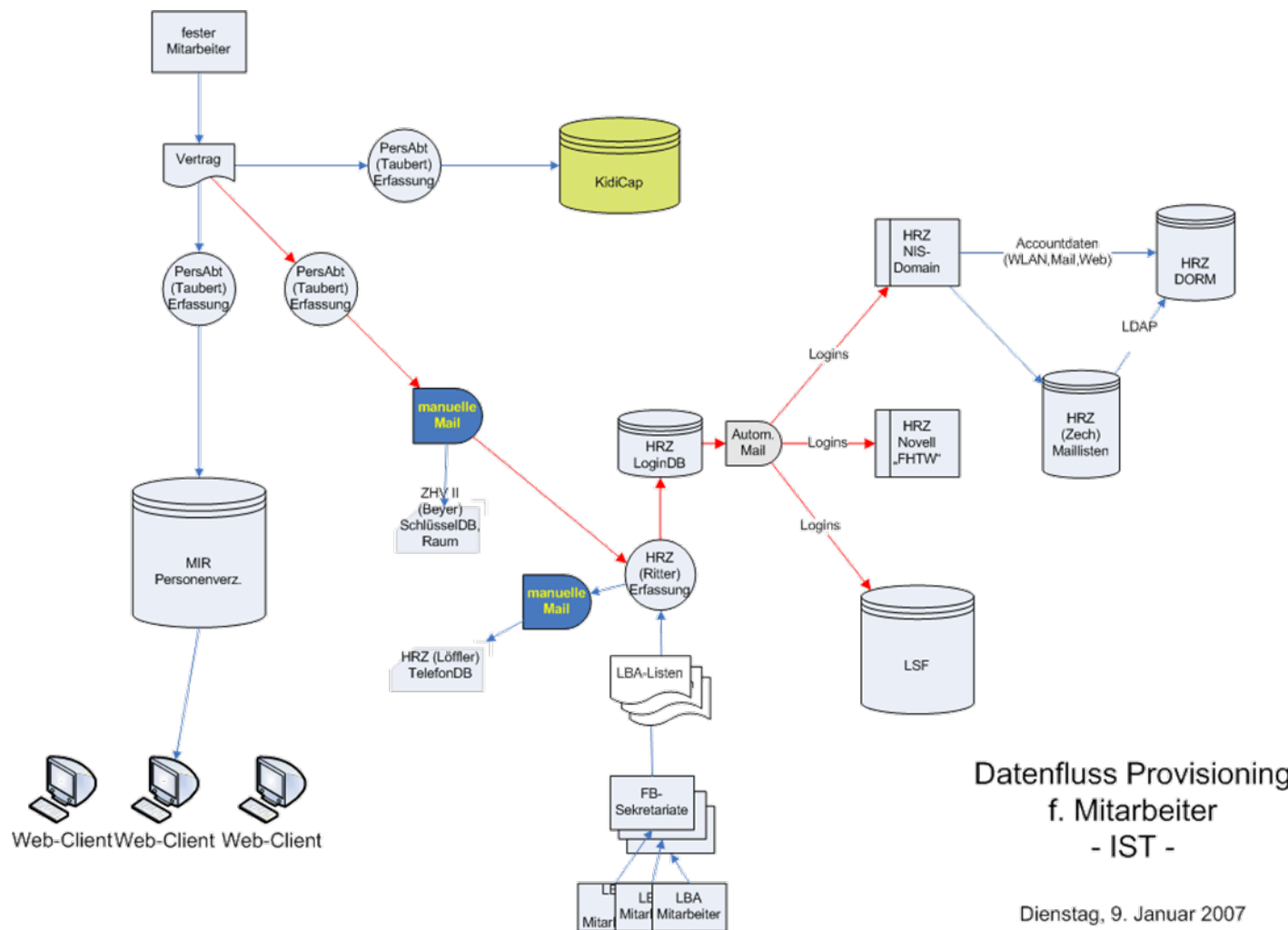
Projektorganisation

- 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)

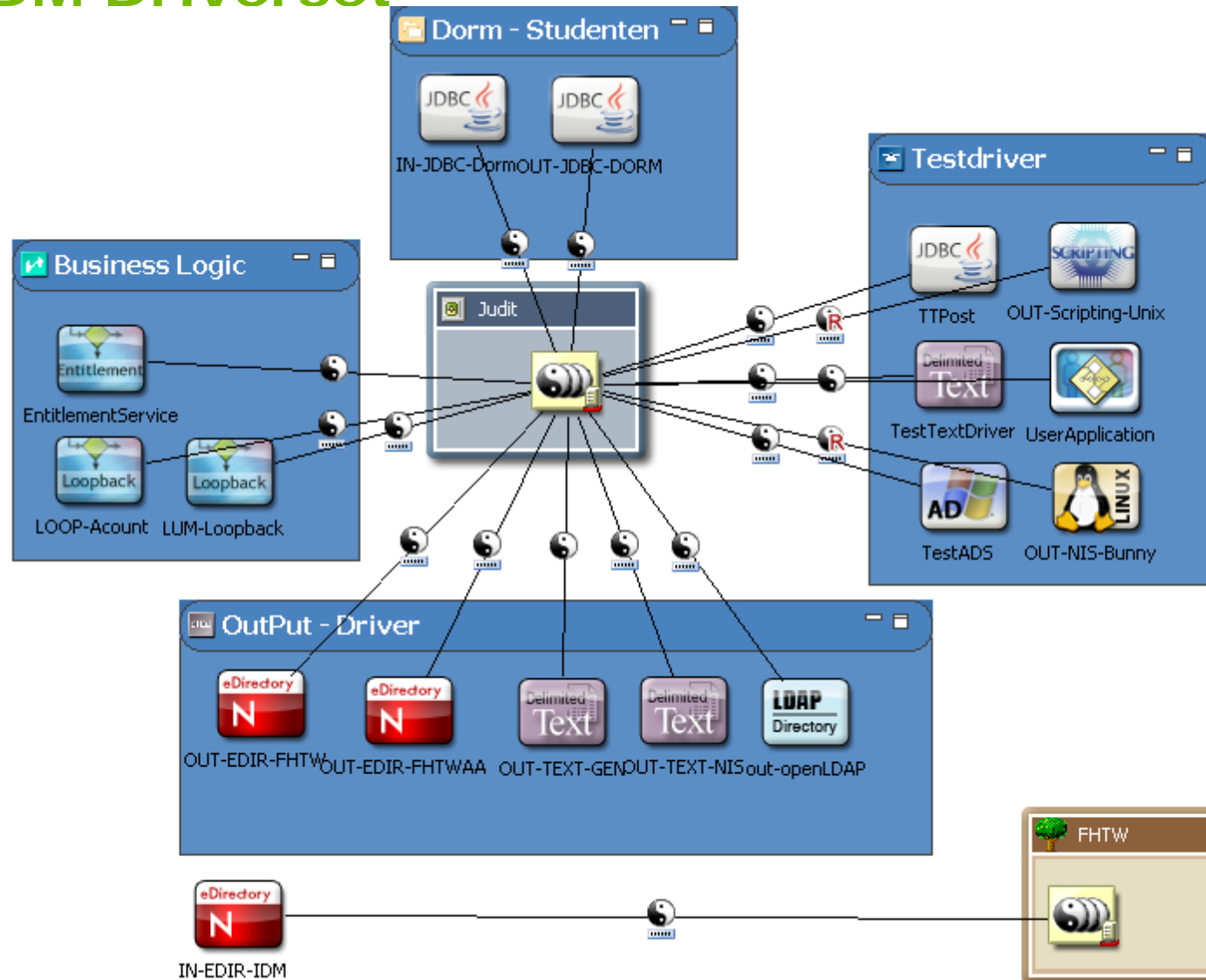
Ausgangssituation



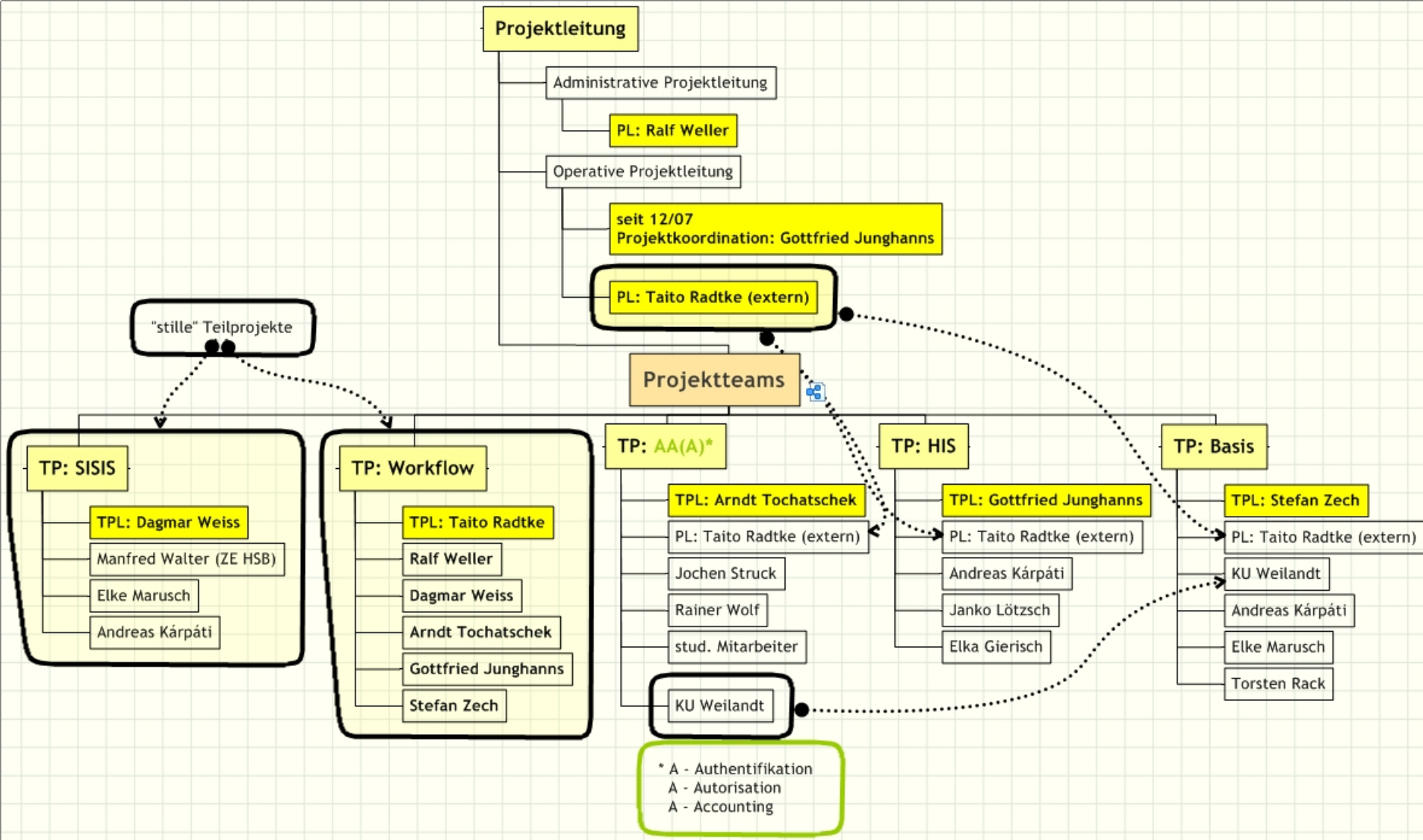
Schema für das MetaDirectory

- 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, posixAccount, ...
- => Möglichkeiten der Datentransformation durch IDM

IDM Driverset



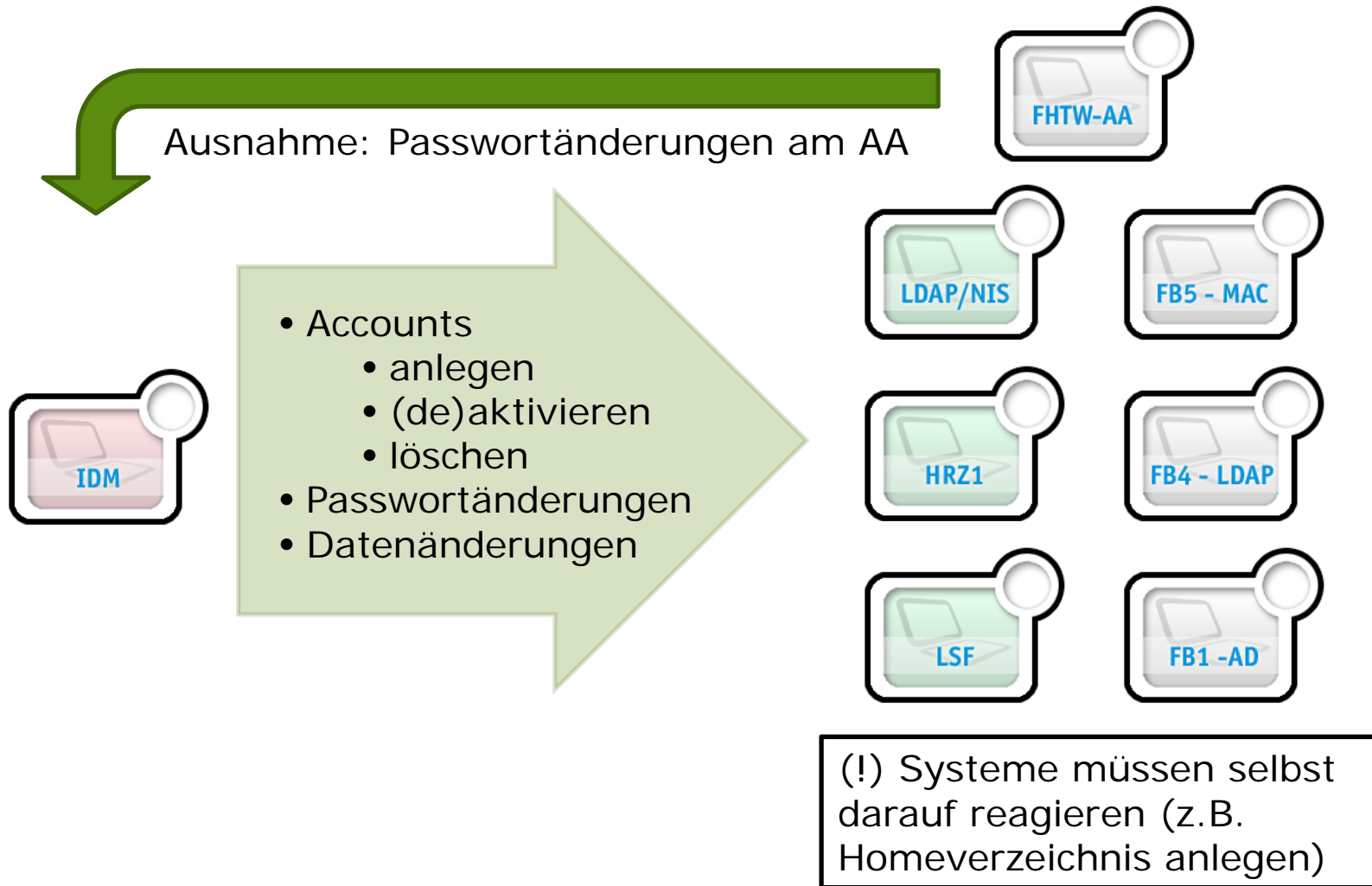
Projektorganisation



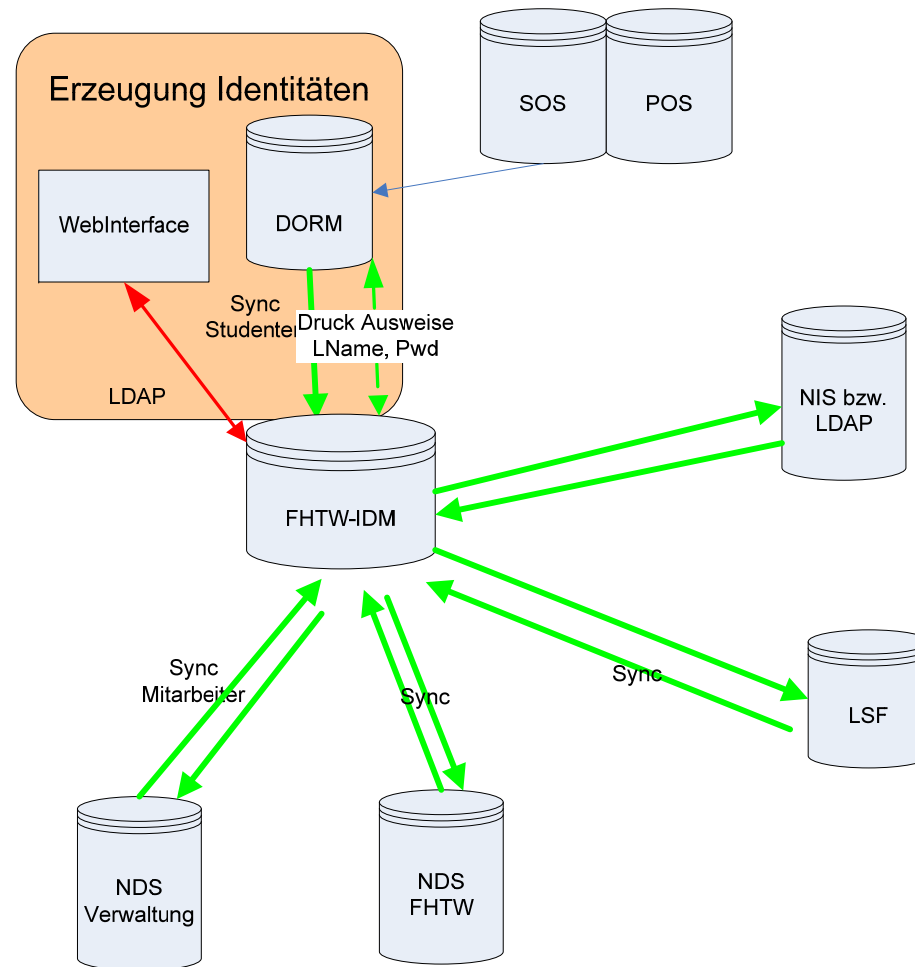
JUDIT – Funktionen des IDM-Systems

- 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



Istzustand



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