



Projektbericht

Aufbau & Implementierung eines neuen Identity & Access-
Management Systems basierend auf den Forefront Identity
Manager 2010

Daniel Löffler

E-Mail: Daniel.Loeffler@FernUni-Hagen.de

Telefon: +49 2331 987-2868

Inhalt

- Die FernUniversität in Hagen
- Identity & Access-Management an der FernUniversität
- Planung und Konzeption des „neuen“ IAM-Systems
- Projektphase I
- Herausforderungen
- Projektphase II und weitere
- Ausblick
- Benefits

Die FernUniversität in Hagen

- 1974 gegründet als Universität und Gesamthochschule des Landes Nordrhein-Westfalen
- Erste und einzige öffentlich-rechtliche Fernuniversität in Deutschland
- Mit über 84.000 Studierenden die größte Universität Deutschlands
- Vier Fakultäten
 - Fakultät für Kultur- und Sozialwissenschaften
 - Fakultät für Mathematik und Informatik
 - Fakultät für Wirtschaftswissenschaften
 - Rechtswissenschaftliche Fakultät
- 1800 Mitarbeiter

Identity & Access-Management an der FernUniversität

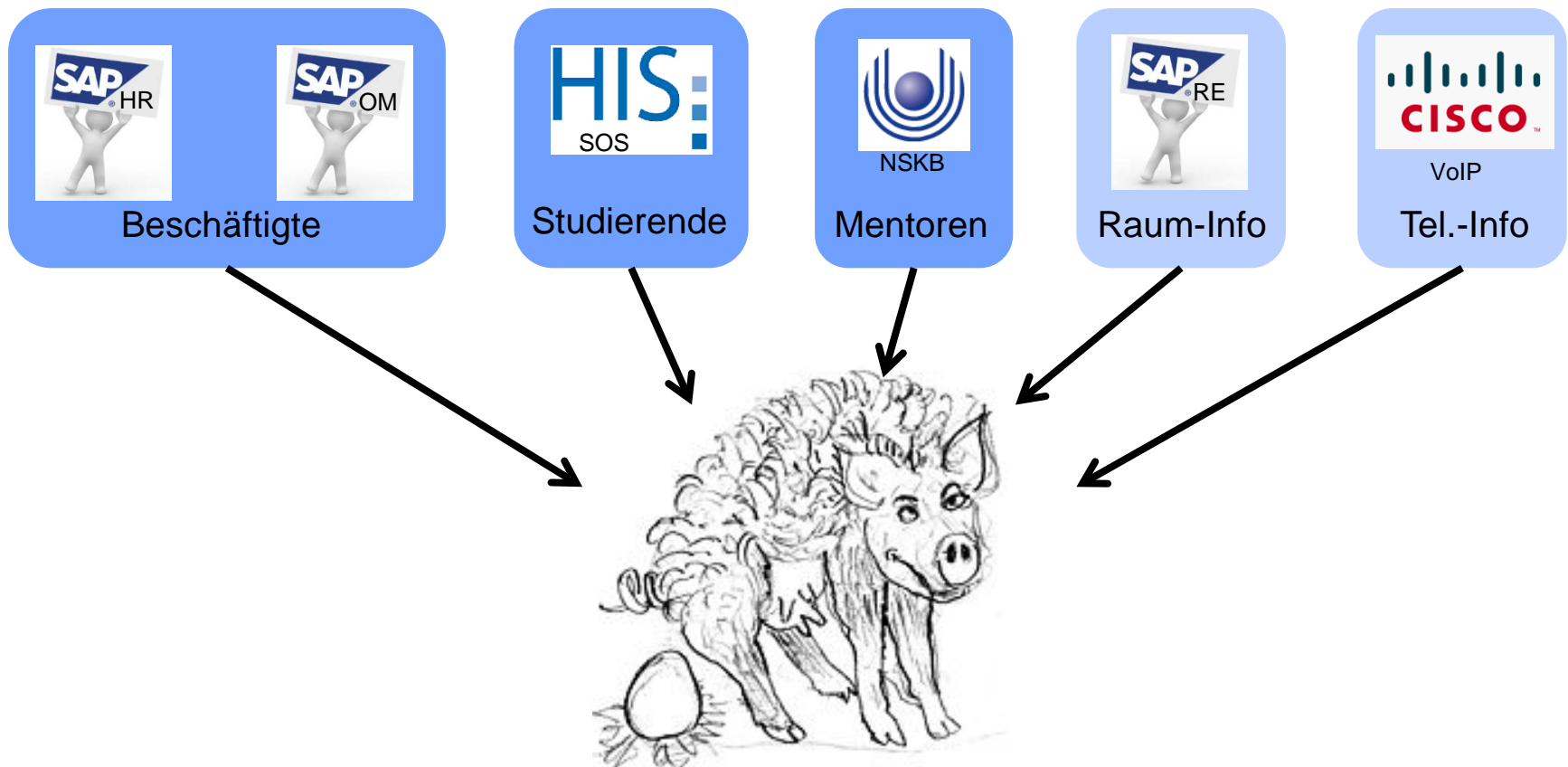
Die FernUniversität besitzt schon seit 2006 ein IAM System

- Verzeichnisdienst LDAP
 - Accounts wurden „manuell“ verwaltet
- BMC Control SA
 - Erste automatische Verwaltung von:
 - SUN LDAP-Accounts
 - UNIX-Accounts
 - Zertifikatsserver-Accounts
- Microsoft Forefront Identity Manager 2010 (FIM 2010)
 - ...



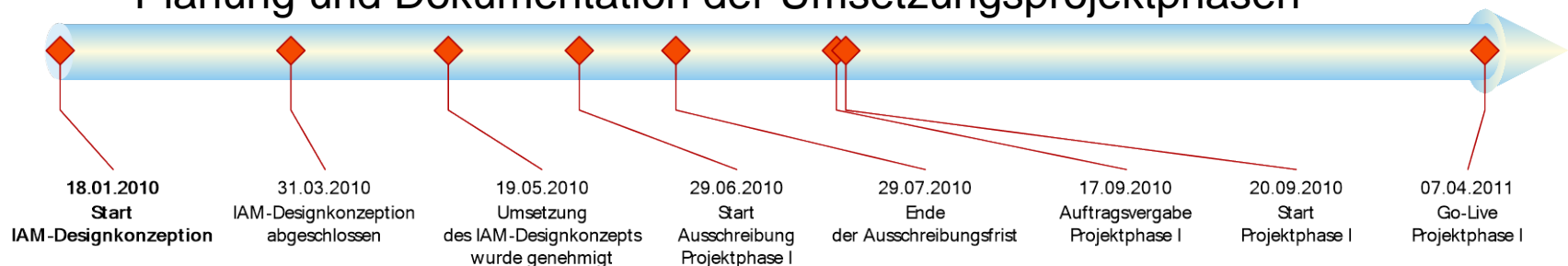
Identity & Access-Management an der FernUniversität

Das IAM System ist DAS zentrale System der FernUniversität, da es für die Verteilung sämtlicher Zugangsdaten zuständig ist



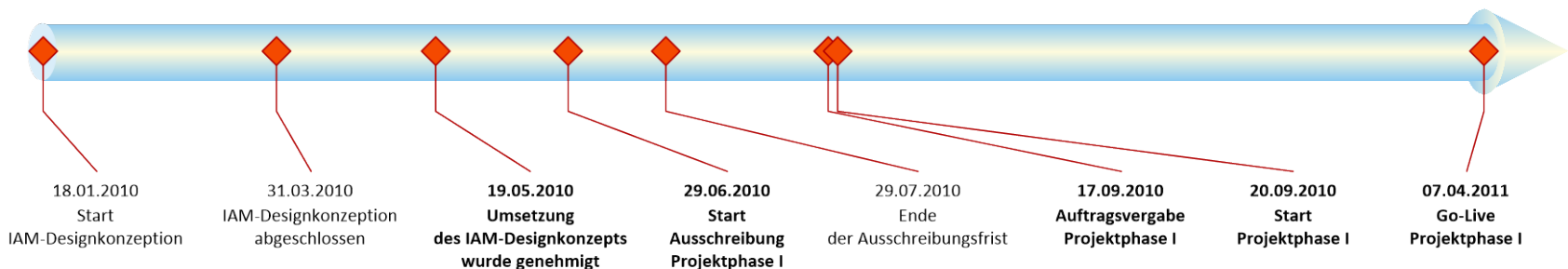
Planung und Konzeption des „neuen“ Identity & Access Management Systems

- Grobe Anforderungsanalyse
(Planungsworkshop – 4. Quartal 2009)
- Erstellung eines Identity & Access Management Design Konzepts
 - Anforderungen der FernUniversität wurden aufgenommen und vom Projektteam (FernUniversität und externe Unterstützung) bewertet und dokumentiert
 - Planung und Dokumentation der IDM-Architektur
 - Planung und Dokumentation des technischen Designs
 - Planung und Dokumentation der Umsetzungsprojektphasen

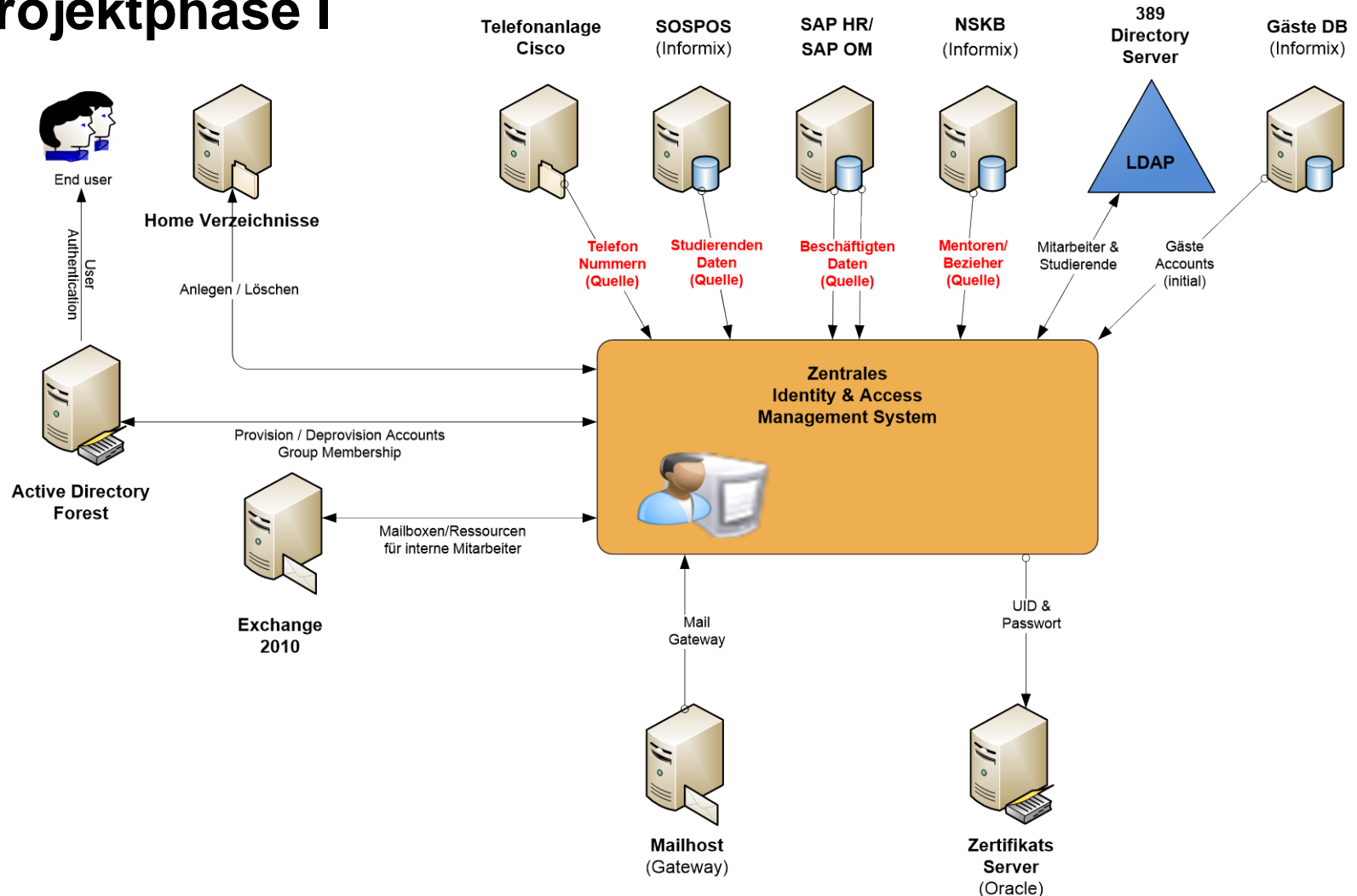


Planung und Konzeption des „neuen“ Identity & Access Management Systems

- Beschluss des Rektorats über die Umsetzung des IDM-Designkonzepts
 - Wichtig, da Identity Management von den Bereichen oft nicht angenommen wird
- Ausschreibung
- Auftragsvergabe
- Start der Projektphase I
- Go-Live der Projektphase I



Projektphase I



Herausforderungen

Die größte Herausforderung besteht darin, mit allen Beteiligten/Verantwortlichen in die konstruktive Diskussion einzusteigen

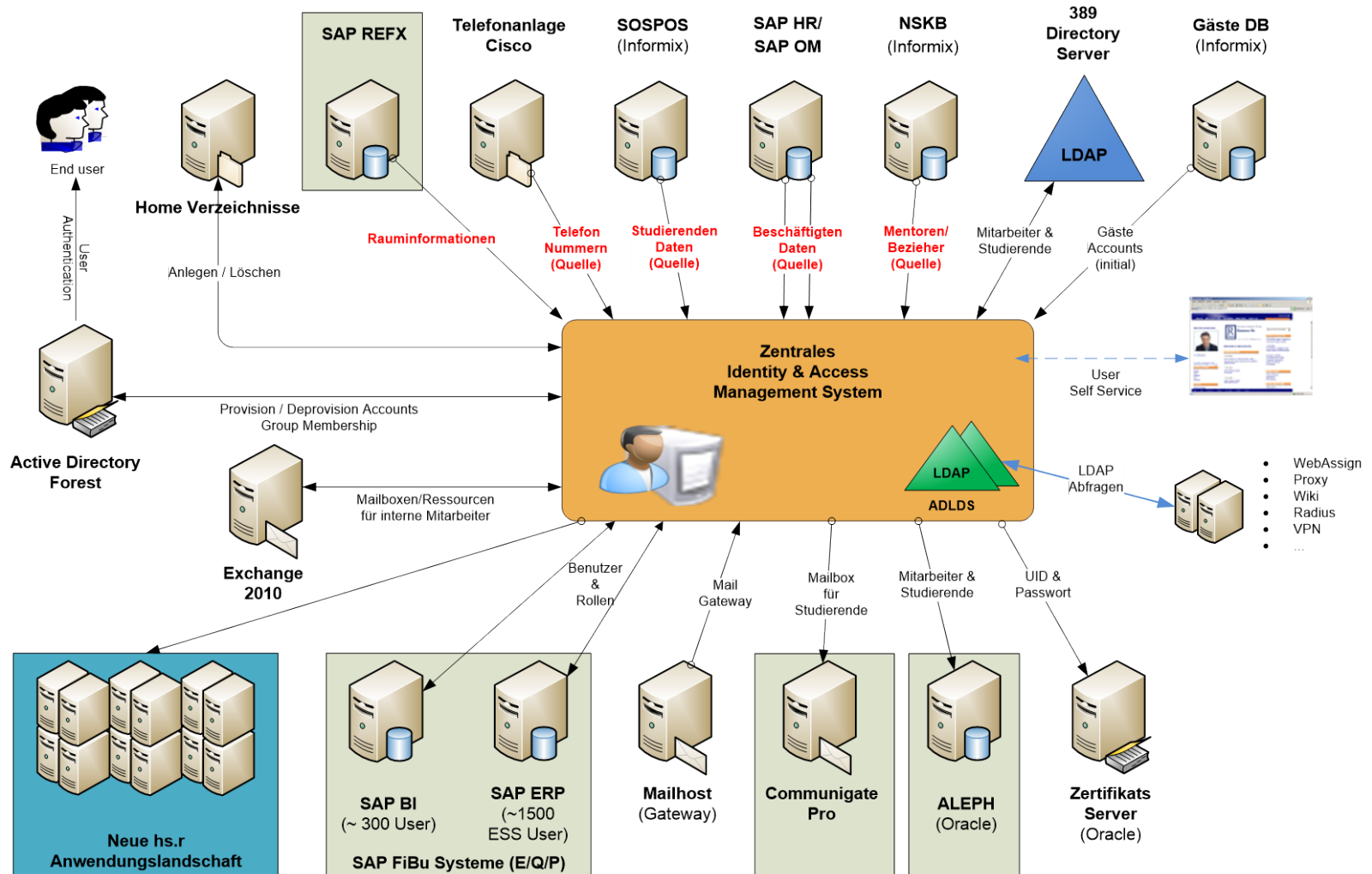
- „Alles unter einen Hut zu bekommen“
 - Integration aller Bereiche der FernUniversität (Fakultäten, Zentrale Einrichtungen, Datenschutzbeauftragte/er, usw.)
- Starke Abhängigkeiten zu anderen Projekten / Programmen
 - FiBu Projekt (Datenquellen änderten sich während des Projektes)
 - hs.r
 - Mailprojekte
- Abhängigkeiten zu allen FernUniversitäts-Anwendungen
 - Auf alte Anwendungen muss Rücksicht genommen werden
- Durchsetzung von Regeln und Prozessen
 - Datenänderungen nur in Quellsystemen möglich
 - Einführung neuer Passwortregeln

Herausforderungen

Durch die Einführung des neuen IAM Systems, wurde die Datenqualität in den IT-System deutlich verbessert

- Sehr schlechte Datenqualität, die im Vorfeld nicht absehbar war
 - Vor dem IAM-Projekt wurden keine Beschäftigten-Accounts/Daten gelöscht
 - Keine Zuordnung zu einer Datenquelle mehr möglich
 - Fehler in Datensätzen von Studierenden
 - Passwortbriefe wurden nicht korrekt adressiert
 - Falscher Name wird in Anwendungen angezeigt
- Große Teile mussten bereinigt/isoliert werden
- **Hat das Projekt mehrere Monate verzögert**

Projektphase II und weitere



Ausblick

Bei zukünftigen IT-Projekten muss immer das Identity & Access Management berücksichtigt werden

- Umsetzung einiger Portalfunktionalitäten
 - Webbasierter Passwortreset
 - Gruppenmanagement
- Anbindung eines neuen Studierendenverwaltungssystems (hs.r)
- Einführung von „Bewerber“-Accounts (hs.r)
- Anbindung eines „Alumni“-Verwaltungssystems (hs.r)
- ...
- Rollenmanagment 😊

Benefits

Es ergeben sich deutliche Benefits für die Angehörigen der FernUniversität und für die FernUniversität selbst

- Für die Angehörigen der FernUniversität (Beschäftigte, Studierenden)
 - Ein Benutzername und ein Passwort für alle Systeme
 - Passwort kann selbstständig zurückgesetzt werden (SMS, Frage-Antwort)
 - Eigenständige Verwaltung von Gruppen
 - Schnellere Bereitstellung von Accounts und Mailadresse
 - Zugriffsrechte können schneller bereitgestellt werden
- Für die FernUniversität selbst
 - Steigerung der IT-Sicherheit
 - Keine manuelle Administration von Accounts und Zugriffsrechten mehr notwendig, da vollautomatische Prozesse dies regeln