IdMS-IUBH
IAM = IdM + AM

IAM (Identity and Access Management) besteht aus 2 Bereichen:

- **Identity Management**
  - Verwalten von Identitäten, d.h. Attribute und ggf. Gruppen- resp. Rollen zuordnen, Eineindeutigkeit (systemimmanenter Identifikator) herstellen sowie die Authentifizerungsmethoden (Kennwort, biometrische Verfahren, Token etc.) festlegen
  - Authentitzität (Identifizierung), d.h. die überprüfbare Erbringung eines vertrauenwürdigen Nachweises auf Echtheit, ob ein Person oder (IT-)Ressource eine behauptete Eigenschaft besitzt
  - Provisionierung, Synchronisierung und De-Provisionierung, d.h. Kreieren und Bereitstellen von Accounts für (IT-)Ressourcen, aktuell Halten sowie (zeitnahes) Löschen (ggf. auch nur Sperren) der Accounts, wenn sie nicht mehr benötigt werden
- **Access Management**
  - Kreieren von Autorisierungsregeln sowie durchsetzen dieser
  - Authentifizierung und Autorisierung, d.h. einen Zugriff auf (IT-)Ressourcen anhand der festgelegten Policies zu erlauben oder abzulehnen

IdMS-IUBH
Provisionierung

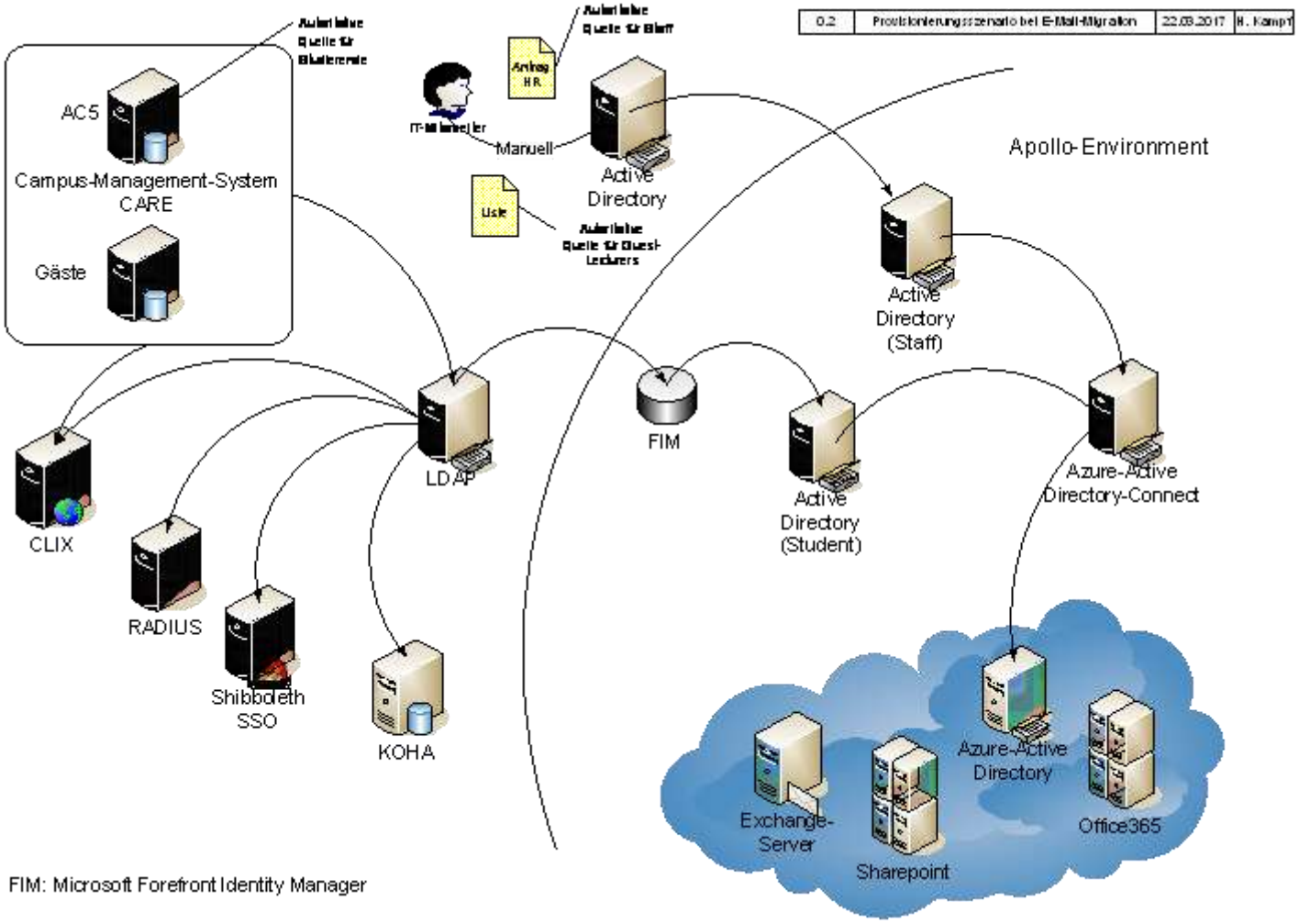
Eine wesentliche Funktion des IdMS ist die **Provisionierung**, welches dafür zuständig ist, dass angeschlossene Systeme Benutzer-Account-Informationen erhalten, um die Authentifizierungs- und Autorisierungsprozesse durchführen zu können.

Grundlage eines IdM sind sog. **autoritative Datenquellen**, in denen Identitäten – gemeint sind hier Personen – erfasst werden. Diese Datenquellen sollten in einem zentralen Repository, dem IdM-System, **konsolidiert zusammengeführt** werden. D. h. ist eine Person mit ihren Daten erfasst und von der jeweils zuständigen Organisationseinheit (Studentenverwaltung-CARE, Human Ressources, etc.) eindeutig identifiziert, so entsteht eine relevante Identität, die im IdM-System gespeichert werden sollte.

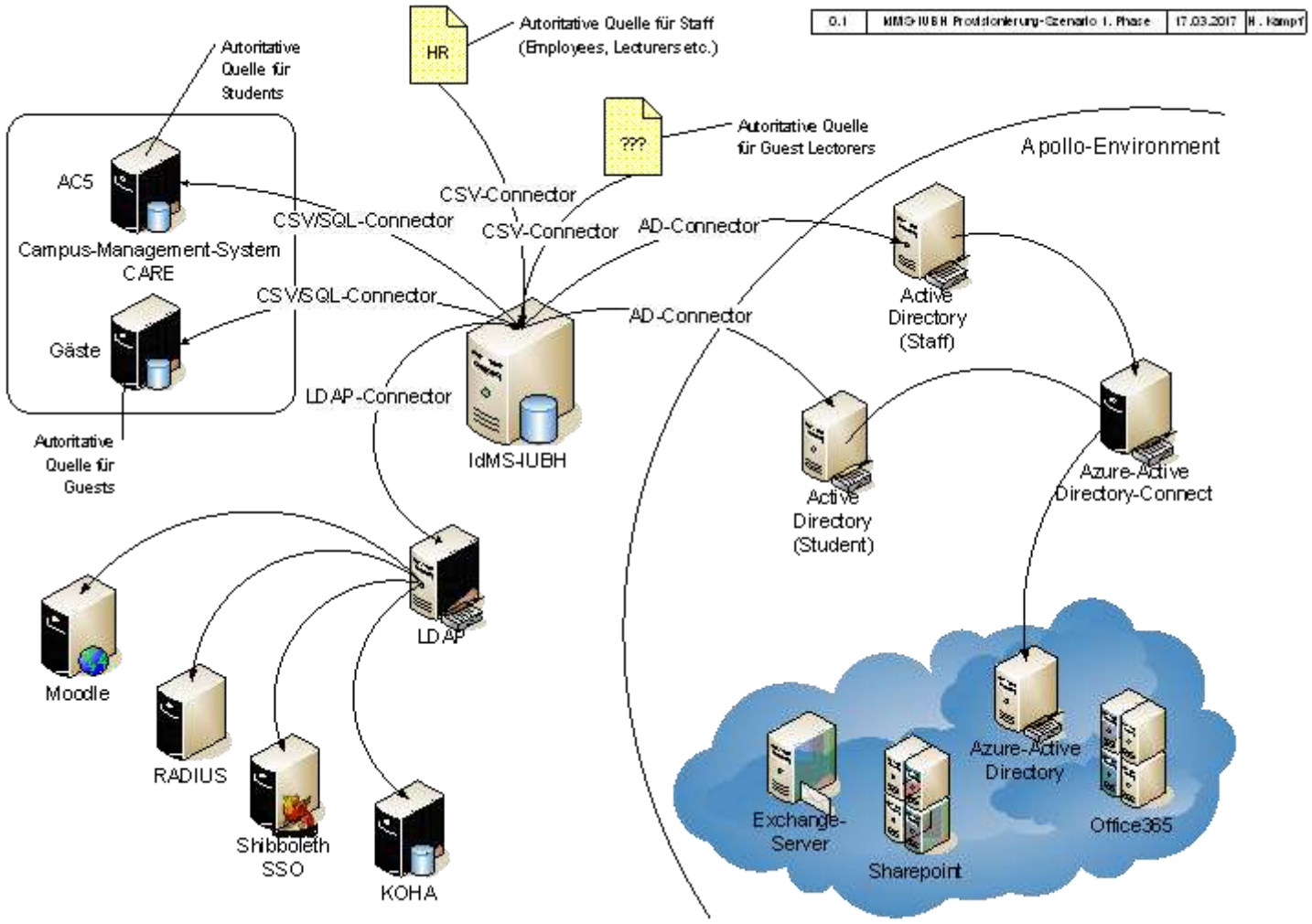
Über das IdM-System finden **keine Authentifizierungen** statt, vielmehr werden andere Systeme (LDAP, AD, Shibboleth usw.), die die jeweiligen Authentifizierungs- und Autorisierungsprozesse durchführen, über **Workflows und dedizierte Konnektoren** mit den Identitäten **regelbasiert provisioniert**. Es gibt also **Quellen**, aus denen die Identitäten stammen, und **Senken**, an die die Identitäten weitergeleitet werden.

IdMS-IUBH

Provisionierungsszenario bei E-Mail-Migration



IdMS-IUBH
Provisionierung-Szenario 1. Phase



IdMS-IUBH
Basiskomponenten

Das zentrale IdM-System der IUBH sollte aus folgenden Komponenten bestehen:

- (intuitive) Administratoroberfläche zum Einrichten und Maintainieren der Identitäten, Workflows, Konnektoren etc.
- Repository mit Benutzer- und Gruppierungsverwaltung (Gruppen, Organisationen, Rollen u. ä.)
- (frei definierbarer resp. erweiterbarer) Attributrahmen
- (vorkonfektionierte) Workflows
- (vorkonfektionierte) Konnektoren
- Logging resp. Acccess Control List für Audits

Sollten Mehrwertdienste, wie SSO, Passwordmangement, Selfservice-Funktionen in den möglichen Produktkandidaten vorhanden sein, so sollte dies auch berücksichtigt werden, um den Integrationsgrad zu erhöhen.

IdMS-IUBH
Identifizierende Attribute

Problem:

Nicht immer reichen einzelne Identifizierungsmerkmale, die eine Person resp. Identität beschreiben, in Quantität und Qualität aus, um in einem Identitätenrepository diese mit einer hohen Wahrscheinlichkeit (wieder)erkennen oder mit einer bestimmten Wahrscheinlichkeit ausschließen zu können, dass eine vermeintlich erkannte Identität, nicht die ist, für die sie gehalten wurde.

Die Eigenschaften der identifizierenden Merkmale müssen bestimmten Kriterien gehorchen:

- keine Änderungsrate und damit Zuordnung eines festen Attributwerts
- große Ausprägungsmenge und damit hoher Differenzierungsgrad

Suche nach Attributen, die einer natürlichen Person „lebenslänglich“ anhaften, und in Kombination derer eine Identität mit hoher Wahrscheinlichkeit eindeutig identifizieren, z. B.:

- Vorname
- Geburtstag
- Geburtsort

IdMS-IUBH
Dubletten

Problem:

Übernahme von Identitäten aus verschiedenen (autoritativen) Quellen, deren Attribute unterschiedliche Schreibweisen (Tippfehler, Buchstaben-, Wortdreher, Abkürzungen usw.) aufweisen.

Eine einfache Prüfung einzelner identifizierender Attribute auf Identität reicht bei Weitem nicht aus, um (ungewollte) Dubletten aufdecken zu können. Vielmehr sollten sie bei Übernahme der Identitäten ins Repository oder in einem nachfolgenden Prüfprozess aus dem Repository anhand sog. Ähnlichkeitsverfahren (z. B. Smith-Waterman, Levenshtein, Bloom-Filter u. a.) mit hoher Wahrscheinlichkeit aufgespürt und nachbearbeitet werden.

Open Source – Pro und Contrra

Kardinalfrage: Open Source oder kommerzielle Lösung?

Nur ein geringer Kostenanteil einer gesamten IdM-Suite macht die Hardware und Basissoftware aus. Der Löwenanteil der Kosten verteilt sich auf Prozesse und Architektur (Connectors, Workflows, Role-, Groupmanagement etc.), die, wenn nicht durch Eigenleistung, so durch Professional-Services (Consulting, Training, Support etc.) erzeugt werden.

Pro	Contra
Keine Kosten für den (Lizenz-)Erwerb	Kosten für Hardware, Training, Consulting sowie Implementation und Integration als auch Support bleiben (ggf. ROI- und/oder TCO-Betrachtung erforderlich)
(große) Community für Unterstützung, Bug Fixes, Weiterentwicklung	Geringere Anzahl an Anbietern (siehe z. B. www.capterra.com/identity-management-software)
KMU mit begrenzten Ressourcen und Finanzierung, aber mit der Notwendigkeit eines IdM-Service	Meist nur „on-premise“-Lösung der Anbieter, keine Komplettlösung
„Try Before You Buy“-Philosophie	Verfügbarkeit des Produkts, z. B. wenn das Unternehmen untergeht oder verkauft wird

Open Source – Auswahl (1)

OpenIDM (Fa. ForgeRock, Kalifornien, 2010)

- Registrierung notwendig
- Nur Einsicht in Dokumentation
- Kein Software-Download, da Einloggen nicht möglich
- Aggressives Vertriebs-/Marketing-Verhalten

Soffid (Fa. Soffid, Spanien, 2012)

- Registrierung notwendig
- Einfache Installation Application-Server, Console und MariaDB (zuerst MySQL-Oracle)
- 2 Konnektoren (CSV, MySQL); CSV-Konnektor nicht funktionsfähig
- Maria-DB als Zielsystem
- CSV-Datei als Quellsystem
- Unterstützung mittels guter Dokumentation und Kontakt zum CEO

IdMS-IUBH
Open Source – Auswahl (2)

midPoint (Fa. Evolveum, Slowakei, 2011)

- Einfache Installation Apache-Tomcat und midPoint-Server mit In-Memory-DB
- 2 Konnektoren (CSV, MySQL)
- Maria-DB als Zielsystem
- CSV-Datei als Quellsystem
- Unterstützung über sehr gute Dokumentation

Apache Syncope (Fa. Tirasa, Italien, 2011)

- Keine Aktivitäten

Erkenntnis

Apache Syncope, midPoint, OpenIDM nutzen ConnId-Framwork (Basis: Sun ICF) für Konnektoren; d.h. theoretische Interoperabilität scheint gegeben. Für Soffid liegen keine Erkenntnisse vor.

midPoint – Systemanforderung

lt. Evolveum-Dokumentation:

MidPoint Server	Minimal	> 5.000 user	> 10.000 user
CPU	1 core	2 cores	4 cores
Disk I/O	negligible	negligible	negligible
Disk space	2GB	10GB	10GB
RAM	4GB	4GB	8GB

Database System	Minimal	> 5.000 user	> 10.000 user
CPU	1 core	2 cores	4 cores
Disk I/O	small	medium	medium
Disk space	1GB	5GB	20GB
RAM	2GB	3GB	4GB

IdMS-IUBH
Roadmap

Vorgangsname	Anfang	Ende
IUBH IdM System	Mo 02.01.17	Mi 11.10.17
Concept Paper	Mo 02.01.17	Fr 20.01.17
Analysing Requirements	Mi 01.02.17	Fr 17.03.17
Evaluating Products	Mo 20.03.17	Fr 19.05.17
Setting up IdM-System	Mo 22.05.17	Mi 21.06.17
Setting up Connectors	Do 22.06.17	Mi 16.08.17
Connector Care (AC5) - In/Outbound	Do 22.06.17	Mi 16.08.17
Connector Care (Guests) - Outbound	Do 22.06.17	Mi 26.07.17
Connector AD (Apollo - Staff) - Outbound	Do 22.06.17	Mi 26.07.17
Connector AD (Apollo - Students) - Outbound	Do 22.06.17	Mi 26.07.17
Connector LDAP - In/Outbound	Do 22.06.17	Mi 16.08.17
Connector CSV (HR) - Inbound	Do 22.06.17	Mi 26.07.17
Connector CSV (Guest Lecturers) - Inbound	Do 22.06.17	Mi 26.07.17
System- and Integrationtest	Do 17.08.17	Mi 06.09.17
Setting up production system	Do 07.09.17	Mi 11.10.17