# IDM
# Datenarten und angeschlossene Quell- und Zielsysteme

---

**Identitätsmanagement PH-BW**

IDM Datenarten und angeschlossene Quell- und Zielsysteme

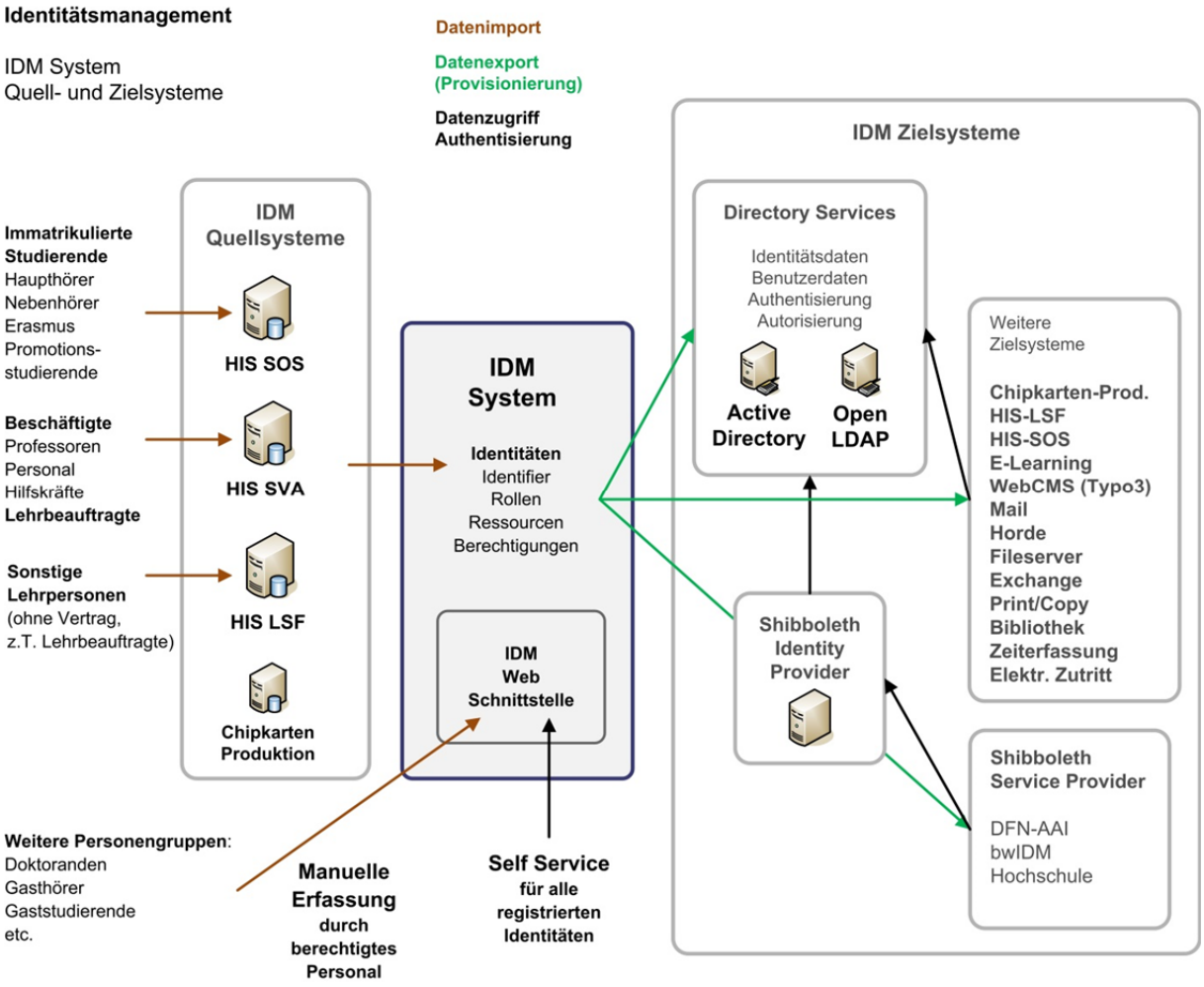
| | | |
|---|---|---|
| Kennung: | IDM_01 | |
| Version: | 1.2 | |
| Erstellt: | 09.07.2014 | PH Freiburg |
| Überarbeitet: | 22.06.2015 | PH Heidelberg |

Seite 4: Daten Campus Card – mit Universitätsrechenzentrum ist das Rechenzentrum der Universität Heidelberg (URZ) gemeint.

# 1. Übersicht IDM Datenflüsse und angebundene Systeme

Das IDM bezieht zum größten Teil die erforderlichen Daten zu den zu verwaltenden Identitäten über Schnittstellen (Konnektoren) aus den Systemen der Hochschulverwaltung (Quellsysteme). Weitere Konnektoren des IDM sorgen für eine kontrollierte Übermittlung der Daten und Berechtigungen von Identitäten an die an das IDM angeschlossenen Anwendungen und Dienste (Zielsysteme), die letztendlich von der im IDM erfassten Person mittels seiner wiederum vom IDM generierten Zugangsressourcen (Account, Chipkarte) und seinen Berechtigungen entsprechend genutzt werden.

Folgende Übersichtsgrafik veranschaulicht die Datenflüsse im Rahmen des Identitätsmanagement und die am IDM angeschlossenen Quell- und Zielsysteme (jedoch ohne Anspruch auf Vollständigkeit, die vollständige Angabe der am IDM angebundenen Systeme erfolgt in den Kapiteln 2 und 4).



# 2. Quellsysteme des IDM

In diesem Kapitel werden die an das IDM angeschlossenen Quellsysteme dargestellt und die Schnittstellen und Verfahren für den Datenimport in das IDM beschrieben. Die genaue Spezifikation der aus den Quellsystemen bezogenen Daten sowie deren Begründung zur Verwendung im IDM erfolgt im nachfolgenden Kapitel 3 zu den Datenfeldern des IDM.

## 2.1. Datenquellen für Identitäten

**Datenbank Studierendenverwaltung**

Die im IDM benötigten Daten der eingeschriebenen Studierenden werden durch automatisierte Prozesse aus dem Studierendenverwaltungssystem HIS-SOS in das IDM gespeist. Der Import der Daten und deren Aktualisierung erfolgt mindestens einmal täglich auf Grundlage eines aus HIS-SOS generierten Datenexports und dessen Verarbeitung durch einen Importprozess des IDM. Die Pflege der Stammdaten der Identitäten von Studierenden wird somit durch Personal der Studierendenverwaltung vorgenommen.

Am Hochschulservicezentrum Reutlingen, das die Verwaltungssysteme der Hochschule im Auftrag betreibt, wird jede Nacht durch einen automatisierten Prozess mittels Datenbankabfrage eine Exportdatei generiert. Diese wird über eine verschlüsselte Verbindung auf ein Transfersystem der Hochschule übertragen, von welchem aus sie vom IDM zum Datenabgleich weiterverarbeitet wird.

**Datenbank Personalverwaltung**

Der Abgleich der Identitätsdaten der Beschäftigten der Hochschule in das IDM erfolgt analog zum Verfahren der Studierendendaten (Exportdatei, Schnittstelle) durch automatisierte Prozesse einmal täglich aus dem Personalverwaltungssystem HIS-SVA. Die Pflege der Stammdaten der Identitäten von Beschäftigten liegt somit bei der Personalverwaltung als verantwortliche Hochschuleinrichtung.

**Datenbank Campusmanagement („Lehre, Studium und Forschung“)**

Das Verwaltungssystem für Lehre und Studium der Hochschule HIS-LSF ist einerseits Zielsystem des IDM (Provisionierung der benötigten Beschäftigtendaten), dient aber auch als Quellsystem für die Identitäten externer Lehrpersonen ohne Beschäftigungsverhältnis (z.B. Gastdozierende und nicht im Personalverwaltungssystem geführte Lehrbeauftragte). Deren Stammdaten werden dort durch verantwortliches Personal der Fakultäten für das Vorlesungsverzeichnis eingepflegt. Der Datenabgleich wird durch das IDM mittels direktem Zugriffs über die Webservice-Schnittstelle von HIS-LSF (SOAP/XML) realisiert. Der Import erfolgt, nur bei Bedarf der Nutzung von IT-Diensten der Hochschule (z.B. E-Learning), durch berechtigtes Personal manuell über die IDM Webschnittstelle angestoßen. Die weitere Aktualisierung der importierten Identitäten wird einmal täglich durch einen automatisierten Prozess des IDM durchgeführt.

**Manuelle Eingabe und Pflege im IDM**

Alle weiteren Identitäten von Personengruppen, die zur Nutzung von IT-Diensten der Hochschule berechtigt sind, werden durch autorisiertes Personal der verantwortlichen Einrichtungen (z.B. Rechenzentrum, Fakultäten, Institute, Bibliothek) manuell über die webbasierte Schnittstelle des IDM erfasst und gepflegt. Erfassung im IDM und mögliche Statusverlängerungen erfolgen auf Grundlage

einer Beantragung durch die betreffende Person sowie der Erbringung eines der Personengruppe entsprechenden Statusnachweises (vgl. Anlage A IDM Berechtigungskonzept zur Nutzung der IT-Dienste der Hochschule). Zu den manuell im IDM gepflegten Personengruppen zählen derzeit z.B. nicht eingeschriebene Doktoranden und weitere nicht in den Quellsystemen erfasste Hochschulmitglieder, Gasthörer und nicht eingeschriebene Gaststudierende, Gastwissenschaftler und andere berechtigte, etwa an Forschungsprojekten der Hochschule beteiligte, externe Personen.

**Konsolidierung der IDM Datenquellen**

Im Zuge der Weiterentwicklung des Identitätsmanagements wird die weitere Reduzierung der manuell im IDM erfassten Personengruppen angestrebt, durch sukzessive Integration der Verwaltung ihrer Stammdaten in die vorhandenen Quellsysteme der Hochschulverwaltung und deren Import in das IDM über entsprechende Schnittstellen und automatisierte Verfahren. Ebenso ist eine Konsolidierung durch Reduzierung und Integration der Datenquellen insgesamt geplant, etwa mittels der Erfassung der Gasthörer im Studierendenverwaltungssystem HIS-SOS.

**Daten Campus Card**

Die bei der Produktion von Hochschulausweisen  der Studierenden generierten und in bestimmten IDM Zielsystemen benötigten Daten werden vom IDM aus den Identitätsdaten des Universitätsrechenzentrums bezogen, den entsprechenden Identitäten zugeordnet und fortlaufend aktualisiert.

# 3. Im IDM verarbeitete Daten

## 3.1. Klassifizierung in Datenarten

Vor der detaillierten Auflistung der im IDM verarbeiteten personenbezogenen Daten erfolgt zunächst eine Klassifizierung nach Datenarten hinsichtlich ihres Zwecks bzw. ihrer Begründung zur Verwendung im IDM:

**Identifizierung:** Daten zur eindeutigen, fehlerfreien Identifizierung einer Person (Identität) als Grundlage für zuverlässige und automatisierte IDM-gestützte Verfahren:

- Kriterien zur eindeutigen Identifizierung bei Namensgleichheit
- Automatisierte Zuweisung und Aktualisierung von Quelldaten
- Konsolidierung von Daten einer Person aus unterschiedlichen Quellen
- Rechtevergabe und Provisionierung von Zielsystemen
- Berechtigte Nutzung von Ressourcen (z.B. Accounts, Passwörter)
- Fehlerfreie Aushändigung von Ressourcen (z.B. Account, Chipkarte)
- Fehlerfreie elektronische Adressierung von Personen bei Übermittlung vertraulicher Informationen (z.B. per Email)

**Offizielles Merkmal:** Daten mit offiziellem Charakter und entsprechend hohen Anforderungen an Korrektheit und Aktualität. Insbesondere in elektronischen, offiziellen Verzeichnissen der Hochschule (z.B. Personen-, Kontaktdaten-, Vorlesungsverzeichnisse und Webportale) veröffentlichte, öffentlich oder authentisierte berechtigte Personen zugängliche Identitätsmerkmale (z.B. Namen, Titel und akademischer Grad, Art der Hochschulzugehörigkeit, Zugehörigkeit zu Hochschuleinrichtungen und dienstliche Kontaktdaten).

**Rechtevergabe:** Daten zur fehlerfreien, effizienten (z.T. automatisierten) und zeitlich gesteuerten Vergabe von Berechtigungen und Ressourcen durch bzw. über das IDM, sowie zu deren Entzug.
Neben Kennungen zur Identifizierung, sind dies Daten zu den im IDM den Identitäten zugewiesenen Rollen und Berechtigungsgruppen. Ferner gehören dazu auch Daten aus den Quellsystemen, die Rollen- und Gruppenmitgliedschaften begründen, sowie deren Status bzw. Gültigkeitsdauer bestimmen.

**Zielsystemrelevanz:** Daten, die für den Betrieb bzw. die Nutzung von Zielsystemen notwendig sind, etwa zur eindeutigen Identifizierung von Nutzern oder zur Kennzeichnung ihrer Rollen in den Zielsystemen. Diese Daten werden vom IDM in mindestens ein Zielsystem provisioniert, d.h. das IDM sorgt für deren Korrektheit und Aktualität in den betreffenden Zielsystemen.

## 3.2. Datenfelder des IDM-Systems

Nachfolgende Tabelle listet die einzelnen im IDM verarbeiteten personenbezogenen Daten unter Angabe der Begründung für ihre Verwendung im IDM sowie ihrer Quellen auf. Daten ohne Angabe einer Quelle werden vom IDM generiert.

Alle Identitätsmerkmale, die für mindestens ein Zielsystem als relevant gekennzeichnet sind, sind für die Weitergabe an angeschlossene Zielsysteme durch das IDM vorgesehen (Provisionierung). Die detaillierte Darstellung im Einzelnen, d.h. welche Daten vom IDM an welche Zielsysteme übermittelt werden, erfolgt in Kapitel 4 zu den Zielsystemen des IDM.

| Datenfeld | Beschreibung und Zweck | Begründung | | | | Quellen | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Identifizierung | Offizielles Merkmal | Rechtevergabe | Zielsystemrelevanz | HIS SOS | HIS SVA | HIS LSF | Manuelle Eingabe | UniID-System |
| Name | Identifizierung, Generierung Basisdaten | X | X | X | X | X | X | X | X | |
| Vorname | Identifizierung, Generierung Basisdaten | X | X | X | X | X | X | X | X | |
| Namenszusätze | Identifizierung, Generierung Basisdaten | X | X | | X | X | X | X | X | |
| Geburtsname | Identifizierung (bei Namensänderungen) | X | | | | X | X | | X | |
| Geburtsdatum | Identifizierung (bei Namensgleichheit) | X | | | X | X | X | X | X | |
| Geburtsort | Identifizierung (bei Namensgleichheit) | X | | | | X | X | | X | |
| Titel | Identifizierung, Erstellung Anzeigenamen | X | X | | X | X | X | X | X | |
| Akademischer Grad | Identifizierung, Erstellung Anzeigenamen | X | X | | X | X | X | X | X | |
| Daten Studierende | | | | | | | | | | |
| Matrikelnummer (SOS) | Eindeutige Kennung eines Studierenden (Zuordnung Quelle) | X | | | X | X | | | | |
| Datum Immatrikulation<br>Datum Exmatrikulation | Gültigkeitsdauer Studierendenstatus, Zuordnung Rollen, Vergabe Berechtigungen | | | X | | X | | | | |
| Semesterstatus | Steuerung spezifischer Berechtigungen (z.B. bei Urlaubssemester) | | | X | X | X | | | | |
| Studierendenkategorie (Hörerstatus) | z.B. Haupt-/Nebenhörer, Austauschstud.<br>Vergabe spezifischer Berechtigungen | X | X | X | | X | | | | |
| Studiengang, Fächer, Fachsemester | Vergabe spezifischer Berechtigungen | | | X | X | X | | | | |
| Daten Beschäftigte | | | | | | | | | | |
| Personalnummer (SVA) | Eindeutige Kennung eines Beschäftigten (Zuordnung Quelle) | X | | | X | | X | | | |
| Beschäftigungsnummer | Zuordnung Rollen/Berechtigungen bei mehreren Beschäftigungsverhältnissen | | | X | | | X | | | |
| Beschäftigungsbeginn<br>Beschäftigungsende | Gültigkeitsdauer Beschäftigtenstatus, Zuordnung Rollen, Vergabe Berechtigungen | | | X | X | | X | | | |
| Personalkategorie (Beschäftigungs- und Dienstart) | z.B. Professoren, Beschäftigte (Wissen., Verwaltung), Lehrbeauftragte, Hilfskräfte<br>Vergabe spezifischer Berechtigungen | X | X | X | | | X | | | |
| Hochschuleinrichtung | Vergabe spezifischer Berechtigungen für Angehörige einer bestimmten Einrichtung | X | X | X | X | | X | | X | |
| Kostenstellen | Kostenabrechnung bestimmter Dienste | | | X | X | | X | | X | |
| PVS Matrikelnummer | Bei studentischem Personal hinterlegte Matrikelnummer (Zusammenführung der Identitäten aus beiden Quellen) | X | | | | | X | | | |
| Weitere Daten | | | | | | | | | | |
| Quellsystem (Kennung) | Interne Zuordnung Quellsysteme | X | | | | X | X | X | | |
| Typisierte Art der Hochschulzugehörigkeit | Affiliation (EduPerson Schema, z.B. student, employee, member, affiliate),<br>Vergabe von Berechtigungen | X | X | X | X | * | * | * | X | |
| Rollen | Vergabe von Berechtigungen | | | X | X | * | * | * | X | |
| Gruppenzugehörigkeiten | Vergabe von Berechtigungen | | | X | X | * | * | * | X | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Identitätskennung | Eindeutige ID einer Identität (Zuordnung Ressourcen) | X | | X | X | | | | | |
| Benutzerkennung | Eindeutige ID eines Benutzeraccounts, mehrere Accounts pro Identität möglich (Authentisierung, Zuordnung Ressourcen) | X | | X | X | | | | | X |
| Passwort | Passwort eines Benutzeraccounts (Authentisierung) | X | | X | X | | | | | X |
| E-Mail Adresse | IDM-generierte Hochschul-Mailadresse | X | X | | X | | | | | |
| Dienstliche Adresse | Kontaktdaten innerhalb der Hochschule (Raum, Gebäude, Telefonnummer) | X | X | | X | | | X | X | |
| Private Adresse | Privater Kontakt durch berechtigte Einrichtungen | X | | | X | X | X | | X | |

* Im IDM regelbasiert zugeordnet auf Basis von Quelldaten (z.B. Art Hochschulzugehörigkeit, Rollen, Gruppen)

# 4. Zielsysteme des IDM

## 4.1. Übersicht Zielsysteme und Weitergabe IDM Daten

Folgende im IDM verarbeitete Daten werden vom IDM an Zielsysteme provisioniert. Eine genauere Beschreibung nach einzelnen Zielsystemen erfolgt in den nachfolgenden Abschnitten dieses Kapitels.

| **IDM Daten** | Directory Services | Shibboleth IDP | HIS LSF | HIS SOS | E-Learning Systeme | Web-CMS Typo3 | Mail | Windows Domain | RAS WLAN / VPN | Service Prov. DFN-AAI |
|---|---|---|---|---|---|---|---|---|---|---|
| Anbindung OpenLDAP | | X | X | | X | X | X | | X | |
| Anbindung Active Directory | | | | | | | | X | X | |
| Name | X | X | X | | X | X | X | X | | + |
| Vorname | X | X | X | | X | X | X | X | | + |
| Namenszusätze | X | X | X | | X | X | X | X | | + |
| Geburtsdatum | X | | | | | | | | | |
| Titel, akad. Grad | X | | X | | X | X | | X | | |
| Matrikelnummer (SOS) | X | | X | | X | | | | | |
| Datum Im-/Exmatrikulation | | | | | | | | | | |
| Semesterstatus | | | | | | | | | | |
| Studierendenkategorie | | | | | | | | | | |
| Studiengang, Fächer, Fachsemester | X | | | | X | | | | | |
| Personalnummer (SVA) | X | | | | | | | | | |
| Beschäftigungsbeginn/-ende | X | | | | | | | | | |
| Personalkategorie | | | X | | | | | | | |
| Hochschuleinrichtung | X | | X | | X | X | | | | |
| Kostenstellen | X | | | | | | | | | |
| Typisierte Art der Hochschulzugehörigkeit | X | X | | | | | | | | X |
| Rollen (inkl. Gültigkeitdauer) | X | X | X | | X | X | X | X | X | |
| Gruppenzugehörigkeiten | X | X | | | X | X | X | X | X | |
| Identitätskennung | X | | X | | X | X | | X | | |
| Benutzerkennung | X | X | X | | X | X | X | X | X | */+ |
| Email-Adresse | X | X | X | X | X | X | X | X | | + |
| Dienstliche Adresse | X | | X | | X | X | | | | |
| Private Adresse | X | | | | | | | | | |

## 4.2. Primäre Zielsysteme mit IDM Funktionalität

Die folgenden primären Zielsysteme des IDM Systems realisieren wichtige Funktionen des gesamten Identitätsmanagements als Schnittstellen-Systeme des IDM zu angeschlossenen Zielsystemen und

Diensten, sowie zur Implementierung zentraler IDM-gestützter Authentisierungs- und Autorisierungsverfahren.

**Directory Services**

Als LDAP-basierte Schnittstelle zwischen dem IDM und nachgeordneten Zielsystemen werden als Verzeichnisdienste eingesetzt und direkt vom IDM mit Daten provisioniert:

- OpenLDAP (OLDAP)
- Active Directory (AD): lokale Windows Domain (Zugriff nur durch lokale Zielsysteme)

Diese implementieren zentrale, IDM-gestützte Verzeichnisse zur Speicherung:

- Aktiver Ressourcen zur Authentisierung (PH Account: Benutzerkennung, Passwort) und Autorisierung (Berechtigungsinformationen, Gruppenmitgliedschaften).
- Personenbezogener Daten von Identitäten (z.B. Namen, Email-Adressen).
- Zielsystem-relevanter Benutzerdaten.

Der LDAP-Zugriff durch die Zielsysteme wird mittels systemspezifischer LDAP-Nutzerobjekte (sog. Bind-User) realisiert und deren Zugriffsberechtigungen per Zugriffskontrolle in den Directory Services (ACL) kontrolliert auf die notwendigen Daten eingeschränkt.

LDAP-basierte Authentisierungen der Zielsysteme erfolgen ohne direkten Zugriff auf die hinterlegten Passwort-Hashes, sondern durch einen Authentisierungsversuch mit der Benutzerkennung und er Passwortangabe des Benutzers (LDAP Bind). Zielsysteme speichern daher keine Passwörter.

**Shibboleth Identity Provider (IDP)**

Webbasierte Schnittstelle (Protokolle HTTPS, SAML) zwischen IDM und berechtigten nachgeordneten Zielsystemen, den sogenannten Shibboleth Service Providern (SP), als Authentisierungs- und Autorisierungsdienst sowie – nach erfolgreicher Authentisierung durch den Benutzer – zur kontrollierten Weitergabe vom SP benötigter Benutzerdaten.

Der IDP speichert in einer eigenen Datenbank lediglich persistente, anonymisierte SP-spezifische Benutzer-ID's (Hashwerte). Alle weiteren an SP übermittelten Benutzerdaten werden vom IDP aus dem angebundenen Directory Service (OLDAP) via LDAP bezogen oder aus dort hinterlegten Informationen regelbasiert generiert. Genauso erfolgt die Authentisierung am IDP über eine indirekte Authentisierung durch den IDP gegen den LDAP Directory Service. Zugriffsberechtigte SP sind in der Konfiguration des IDP hinterlegt. Genauso die für jeden SP spezifisch freigegebenen zu übermittelnden Daten (Attribut-Filter).

Der am IDM angeschlossene IDP ist in der Shibboleth Föderation der DFN-AAI registriert, so dass alle SP der Föderation berechtigt sind den IDP zur Authentisierung zu nutzen, sowie grundlegende anonyme Informationen zum Benutzer erhalten. Das Verfahren ist jedoch immer durch den Benutzer gesteuert, d.h. dieser möchten einen SP nutzen, der wiederum den Benutzer zunächst an den IDP seiner Hochschule zur Authentisierung weiterleitet, welcher bei Erfolg den SP mit Daten beliefert.

Grundsätzlich ist der Shibboleth-Dienst der DFN-AAI auf möglichst anonyme Nutzung von Diensten ausgelegt. Bestimmte in der Föderation angebotene Dienste erfordern jedoch zur Nutzung weitere, nicht-anonyme Benutzerdaten (z.B. Namen, Email-Adressen). In diesem Fall wird der Benutzer vom

IDP nach erfolgreicher Authentisierung um die explizite Freigabe für einen bestimmten SP gebeten, bevor einer Weitergabe der Daten an den SP erfolgt und damit die Nutzung des Dienstes möglich ist (Attribut-Freigaben werden ebenfalls in der Datenbank des IDP gespeichert).

Für den IDP freigegebene IDM Daten und Weitergabe an SP der DFN-AAI:

| **Benutzerattribut** | **Quelle** | **Weitergabe an SP der DFN-AAI** | **Nutzer-freigabe** |
|---|---|---|---|
| Benutzerkennung | Directory Service | Nur bestimmte | Ja |
| Anonyme Benutzer-ID:<br>• Targeted-ID<br>• Persistent-ID | IDP<br>• Zufällig generierter Hashwert<br>• Persistenter Hashwert generiert auf Basis der Benutzerkennung | Alle | - |
| Typisierte Art d. Hochschul-zugehörigkeit (Affiliation) | Directory Service | Alle<br>(nur member/affiliate) | - |
| Rollen | Directory Service | - | - |
| Gruppenzugehörigkeiten | Directory Service | - | - |
| Berechtigungen | z.T. IDP (generiert auf Basis von Affiliation, Rollen, Gruppen)<br>z.T. Directory Service | Alle / nur bestimmte<br>(je nach Berechtigung) | - |
| Namen | Directory Service | Nur bestimmte | Ja |
| Email-Adresse | Directory Service | Nur bestimmte | Ja |

Die Nutzung des IDP für Hochschul-interne webbasierte Dienste erfolgt derzeit nicht, wird aber angestrebt (z.B. für den Webdienst des Bibliotheksystems der Hochschule).

## 4.3. Weitere Zielsysteme der Hochschule

**HIS LSF Campus Management System („Lehre, Studium & Forschung“)**

- Authentifizierung gegen Directory Service
- Persistente Speicherung von Identitätsdaten in eigener Datenbank
- Provisionierung von HIS LSF erfolgt über dessen Webservice-Schnittstelle (SOAP).

Weitergabe IDM Daten (betrifft lediglich Beschäftigte und sonstige Lehrpersonen, bei Studierenden greift LSF direkt auf die HIS SOS Datenbank zu):

- Identitäts-/Benutzerkennung, Namen, Titel, akad. Grad, Email-Adresse
- Personalkategorie (Beschäftigte), Hochschuleinrichtung
- Rollen für Zuweisung von Berechtigungen (z.B. Lehrende)

**HIS SOS Studierendenverwaltungssystem**

Die Self Services der Studierendenverwaltung werden über HIS LSF realisiert, dass im Rahmen der HIS Campusmanagement Systeme direkt auf die SOS Studierendendatenbank zugreift (QIS-Module). Die

HIS LSF Webservice-Schnittstelle wird vom IDM genutzt um die Hochschul-Email-Adresse der Studierenden nach HIS SOS zu provisionieren und für die Hochschulverwaltung verfügbar zu machen.

- Authentifizierung gegen Directory Service
- Persistente Speicherung von Identitätsdaten in eigener Datenbank (SOS)
- Weitergabe IDM Daten: Email-Adresse (Studierende)

**E-Learning Systeme (Stud.IP, Moodle, Mahara)**

- Authentifizierung gegen Directory Service
- Persistente Speicherung von Identitätsdaten in eigener Datenbank

Weitergabe IDM Daten:

- Identitäts-/Benutzerkennung, Namen, Titel, akad. Grad, Email-Adresse, Dienstl. Adresse, Hochschuleinrichtung, Rollen für Zuweisung von Berechtigungen (z.B. Autor, Dozent, Gast)
- Matrikelnummer, Studiengang, Fachsemester (Studierende)

**Web Content Management System (Typo3)**

Das System implementiert derzeit den offiziellen Webauftritts der Hochschule. Geschützte Bereiche für angemeldete Hochmitglieder (Konto in Typo3) zur Bearbeitung von Inhalten. Webbasiertes Personenverzeichnis (dienstliche Kontaktdaten der Beschäftigten und sonstigen Lehrpersonen).

- Authentifizierung gegen Directory Service (OLDAP)
- Persistente Speicherung von Identitätsdaten in eigener Datenbank
- Provisionierung durch Benutzer gesteuert, bei Anmeldung werden die benötigten Daten aus dem Directory Service importiert und ein Konto angelegt (IDM aktualisiert nachfolgend).

Weitergabe IDM Daten (Beschäftigte, sonstige Lehrpersonen):

- Identitäts-/Benutzerkennung, Namen, Titel, akad. Grad,
- Email-Adresse, Dienstliche Adresse, Hochschuleinrichtung

**Mail**

- Der Mail-Dienst umfasst in seiner Gesamtheit eine Reihe unterschiedlicher Dienste:
    - IMAP Mailserver *Cyrus* (Mailkonto-ID entspricht der Benutzerkennung)
    - SMTP Zustellungsdienst *Postfix*
    - Webmail/Groupware *Horde* (Studierende, Beschäftigte und sonstige Hochschulmitglieder)
    - 
    - Mailing-Listen *Mailman*
- Authentifizierung gegen Directory Service
- Zustellbare Email-Adressen sind in den Directory Services hinterlegt (AD, Primäre Email-Adresse und weitere Aliase). So ermittelt der Postfix-SMTP für die Zustellung von Emails anhand der Mailadresse per LDAP-Abfrage das Mailkonto des adressierten Benutzers.

Weitergabe IDM Daten:

- Benutzerkennung an: Cyrus-IMAP, Horde, Postfix-SMTP (hier nur LDAP-Zugriff zur Ermittlung Mailkonto)
- Primäre Email-Adresse an: Horde, Mailman, Postfix-SMTP (auch Aliase, hier nur LDAP-Zugriff zur Ermittlung Mailkonto)
- Namen an: Horde

**Windows Domain Dienste**

Integrierte Dienste innerhalb der lokalen Windows-Domain der Hochschule über persönlichen Benutzeraccount. Systeme u.a. Domain Controller (Active Directory, Fileserver).

- Nutzung von Windows Arbeitsplatzrechners und PC-Pools
- Zugriff Netzlaufwerke auf den Fileservern (persönliches Home-Laufwerk und Gruppenlaufwerke bei entsprechender Gruppenmitgliedschaft),
- Groupware
- Integrierte Domain für F&L und Verwaltung. Zugriffsschutz bzgl. Ressourcen auf Basis getrennter Organisational Units (ou), Gruppenmitgliedschaften und GPO's implementiert.

Weitergabe IDM Daten:

- Identitätskennung, Benutzerkennung, Namen, Titel, akad. Grad, Email-Adresse,
- Rollen, Gruppenzugehörigkeiten

**Remote Access Services (RAS): WLAN, VPN**

- Authentifizierung via Radius-Server gegen Directory Service, Autorisierung über Berechtigungsinformation im Directory Service (Radius-Gruppe)
- Keine persistente Datenspeicherung

### 4.4. Externe Zielsysteme außerhalb der Hochschule

**Service Provider der Shibboleth Föderation DFN-AAI**

Das Angebot umfasst vorwiegend Dienste aus dem Bibliotheks- und Verlagsbereich, aber auch Dienste die im Rahmen der *bwIDM* Kooperation der Hochschulen des Landes BW genutzt werden können (z.B. bwSync&Share und bwFileStorage).

Die Datenübertragung wird durch Benutzer direkt gesteuert, d.h. sobald dieser auf eine geschützte Ressource eines Anbieters zugreifen möchte, muss er sich zunächst am IDP der eigenen Hochschule authentifizieren. Die im Fall einer erfolgreichen Anmeldung vom IDP an den Anbieter übertragenen Daten wurden bereits in Abschnitt 4.2 dargestellt.

## 5. Anlagen

A. IDM Berechtigungskonzept zur Nutzung der IT-Dienste der Hochschule (Übersicht zu den im IDM erfassten Personengruppen, Dokument: IDM_06_Berechtigungskonzept-IT-Nutzung_PHHD)