IDM
Administrations- und Berechtigungskonzept

Identitätsmanagement PH-BW

IDM Administrations- und Berechtigungskonzept

Kennung:	IDM_02	
Version:	1.1	
Erstellt:	15.07.2014	PH Freiburg
Überabeitet:	22.06.15	PH Heidelberg

1. IDM Systemarchitektur

Das zentrale Identitätsmanagement wird in seiner Gesamtheit durch eine Reihe von Systemen realisiert, die darin unterschiedliche Funktionen übernehmen und Dienste (IDM Services) für das Identitätsmanagement bereitstellen.

1.1. IDM Systeme

Folgende Systeme realisieren als Kernkomponenten und Subsysteme das IDM System.

IDM Core System

- IDM Core Applikation, diese implementiert als Kernanwendung des IDM
  - Funktionen und Prozesse zur Verwaltung von Identitäten und Ressourcen
  - Webservices zu definierten IDM Funktionen (ID Management, Self Service)
  - Schnittstellen zu Quellsystemen und Zielanwendungen
- IDM Datenbank zur Speicherung von
  - Daten zu Identitäten (Personen, Identifier, Rollen)
  - Daten zu Ressourcen und Berechtigungen
  - IDM Prozessdaten
- IDM Self Service Applikation
  - Implementiert Webmasken für die ID Selbstverwaltung
  - Zugriff auf entsprechende Webservices der Core Applikation

IDM Audit System

Datenbankanwendung zur Protokollierung der ID Management Prozesse und damit zur Prüfung aller im IDM durchgeführten Änderungen (Auditing).

IDM Webserver Systeme

Webserver Dienste zur Bereitstellung der Webbasierten Funktionen (Webservices) des IDM Core Systems. Für die Webschnittstellen IDM Admin (ID Management) und IDM Self Service werden getrennte Webhosts (Apache Virtualhosts) mit unterschiedlichen Funktionen und Zugriffsklassen betrieben.

IDM Print Server

System und Anwendung als Schnittstelle des IDM Core zu Druckern der Hochschule für die Generierung von Ausdrucken (z.B. Account-Handouts, Formulare).

HSZ Transfer Server

System zum Transfer der Datenexporte der beim HSZ Reutlingen gehosteten Quellsysteme für Studierenden- und Beschäftigtendaten (HIS SOS und SVA).

Backup Service

Externes am *Steinbuch Center for Computing* (*SCC,* am *Karlsruher Institut of Technology*) betriebenes Backupsystem mit Anwendung für die Sicherung der IDM Core Daten und Systeme. Dieser Dienst

wird von den Pädagogischen Hochschulen des Landes BW bereits für Sicherungen anderer Serverdienste genutzt.

Die nachfolgenden Systeme sind primäre Zielsysteme des IDM Systems, realisieren aber als Bestandteil des gesamten Identitätsmanagements wichtige Funktionen als Schnittstellen des IDM zu angeschlossenen Zielsystemen und Zielanwendungen und in der Implementierung zentraler, IDM-gestützter Authentisierungs- und Autorisierungsverfahren.

Directory Services

An das IDM angeschlossene LDAP Verzeichnisdienste dienen durch Speicherung der aktiven Daten und Ressourcen von Identitäten (Accounts, Berechtigungen, etc.) als LDAP-basierte Schnittstellen zu Zielsystemen und Diensten der Authentisierung und Autorisierung, sowie dem kontrollierten Bezug von Nutzerdaten. Die Darstellung und Beschreibung der konkret am IDM angeschlossenen Verzeichnisdienste (Active Directory und OpenLDAP) sowie der vom IDM in diese übertragenen Daten erfolgt in der Dokumentation der verarbeiteten Datenarten und Zielsysteme des IDM (Dokument: IDM_01_Übersicht_DatenQuellenZiele).

Shibboleth Identity Provider

Dieser Dienst dient als Webbasierte Schnittstelle des IDM (SAML, Security Assertion Markup Language) für Webbasierte Zielsysteme und Dienste zur Authentisierung, Autorisierung und bei entsprechender Freigabe bzgl. der Zielanwendung zum kontrollierten Bezug von Nutzerdaten. An diese Schnittstelle angeschlossene Systeme verfügen über einen sogenannten *Shibboleth Service Provider*. Die Darstellung der konkret über diese Schnittstelle angeschlossenen Zielsysteme und vom IDM übermittelten Daten erfolgt ebenfalls im Dokument *IDM_01_Übersicht_DatenQuellenZiele*.

1.2. Schnittstellen und Zugriffe

Zugriffe auf Systeme, Anwendungen und Funktionen des IDM und die darin verarbeiteten Daten durch Systeme, Anwendungsprozesse und berechtigte Personen erfolgen kontrolliert über definierte Schnittstellen. Eine grafische Übersicht der IDM Systemarchitektur samt Beschreibung der Schnittstellen, Netzstruktur und Zugriffswege ist in Anlage A dokumentiert.

Die Provisionierung der Ressourcen und Berechtigungen von Identitäten in die angeschlossenen Zielsysteme, LDAP Dienste und andere Anwendungen, erfolgt durch die IDM Applikation mittels Konnektoren und IDM Nutzerkonten in den betreffenden Systemen mit entsprechenden Zugriffs-berechtigungen.

Der Zugriff auf Daten des IDM durch Zielanwendungen wird nur über die definierten Schnittstellen (LDAP Directory Services, Shibboleth IDP) und lediglich lesend auf die jeweils für die Anwendung freigegebenen, für ihren Betrieb notwendigen Daten gewährt. Die Zugriffskontrolle wird mittels sogenannter Access Control Lists in den Schnittstellensystemen realisiert. Die genaue Beschreibung der Schnittstellen und Zugriffsberechtigungen der einzelnen Zielsysteme ist dem Dokument *IDM_01_Übersicht_DatenQuellenZiele* zu entnehmen.

Die konkreten Maßnahmen zur Implementierung und Sicherstellung der Zugriffsberechtigungen werden in Kapitel 4 im Detail beschrieben.

2. Administrations- und Berechtigungskonzept

Die im Rahmen des Identitätsmanagements durchzuführenden administrativen Aufgaben, werden zur weiteren Beschreibung ihrer konkreten Umsetzung im IDM, sowie der für ihre Durchführung notwendigen Zugriffsberechtigungen für das administrative Personal mittels des IDM Systems auf im IDM und Zielsystemen gespeicherte Daten, in folgende Kategorien unterteilt:

- ID Management
- ID Self Management
- System Management

2.1. ID Management

Als ID Management werden alle im IDM durchgeführten Verwaltungsvorgänge bezeichnet, die Daten zu Identitäten (Personen, Rollen, Identifier) und ihren Ressourcen (Nutzerkonten, Berechtigungen, Nutzerdaten) verarbeiten. Zum Teil werden diese durch automatisierte Prozesse im IDM System realisiert. Alle weiteren durchgeführten Vorgänge erfolgen manuell durch berechtigte Personen kontrolliert über die Web-basierten Management Funktionen des IDM Core.

Automatisiertes ID Management

Bestimmte Aufgaben des ID Managements werden durch automatisierte Prozesse der IDM Core Applikation auf Grundlage von im IDM hinterlegten Regeln und Konfigurationen realisiert.

Hierbei wird unterschieden zwischen vollautomatisierten Prozessen, die zu festgelegten Zeiten (z.B. einmal täglich) oder nach bestimmten Ereignissen (z.B. Statusende einer Identität) durchgeführt werden, und teilautomatisierten Prozessen, die zwar manuell angestoßen werden müssen, dann aber nach dem im IDM für den jeweiligen Vorgang definierten Schema bzw. Regelwerk ablaufen.

Mittels der Teilautomatisierung von Prozessen, etwa kritischer Prozesse, die die Sperrung und Löschung von Ressourcen betreffen, lassen sich Kontrollmechanismen für das manuelle Identitätsmanagement über die IDM Webschnittstelle realisieren, um betroffene Datensätze vorab zu prüfen oder den Prozess gezielt für eine Auswahl von Datensätzen auszuführen. Dies impliziert jedoch eine gewissenhafte und rechtzeitige manuelle Durchführung der Prozesse durch das für das ID Management verantwortliche Personal.

Ferner können berechtigte Identitätsverwalter im Einzel- bzw. Ausnahmefall in automatisierte Prozesse eingreifen. So können Identitäten, durch entsprechende Markierung über die IDM Webschnittstelle, vorab und zeitlich befristet, von automatisierten Prozessen zur Sperrung von Berechtigungen oder Ressourcen ausgenommen werden (d.h. Verzögerung der automatischen Sperrung bis zur Statusklärung). Damit lassen sich Ausnahmesituationen abfangen, die etwa bei zeitlichen Verzögerungen der Statusverlängerung im Quellsystem durch die verantwortliche Einrichtung entstehen können (z.B. Vertragsverlängerung Beschäftigte).

Sämtliche im IDM ausgeführten Prozesse, ob automatisiert oder manuell angestoßen, sowie die durch sie erfolgten Änderungen im IDM und den Zielsystemen, werden unter Aufzeichnung des Zeitpunktes, der betroffenen Datensätze (Identifier) und der jeweils durchgeführten Aktion, im IDM Audit protokolliert.

Import aus den Quellsystemen

Die Neuanlage und die Aktualisierung von Identitäten aus den angeschlossenen Quellsystemen erfolgen durch vollautomatisierte Prozesse (z.B. Studierende und Beschäftigte). Die aus den Quellsystemen stammenden Daten einer Identität zur Person, sowie zu Rolle und Status, können nur durch entsprechende Pflege in den Quellsystemen nachträglich verändert werden. Damit wird ein wesentlicher Teil des ID Managements dieser Personengruppen von den jeweils verantwortlichen Hochschuleinrichtungen (Studierenden-/Personalabteilung) erbracht.

Eine Erweiterung der in den Quellsystemen der Hochschulverwaltung erfassten Personengruppen (z.B. auf Doktoranden, Gasthörer und Gaststudierende), verbunden mit ihrer Pflege durch die verantwortlichen Hochschuleinrichtungen in diesen Systemen, wird im Zuge der Weiterentwicklung des Identitätsmanagements angestrebt.

Umsetzungen in die Zielsysteme

Automatisierte Prozesse übernehmen die Provisionierung, d.h. Anlage, Aktualisierung und Löschung, definierter Daten und Ressourcen in den angeschlossenen Zielsystemen, in dem sie nach automatisiert oder manuell erfolgten Änderungen von Daten oder Bedingungen im IDM, automatisch durchgeführt werden:

- Generierung von Ressourcen und Vergabe von Berechtigungen bei Neuregistrierung einer Identität oder Zuordnung einer neuen Rolle (z.B. Hochschul-Account, Mailkonto bei Studierenden). Welche Ressourcen und Berechtigungen bei welchen Rollen automatisch vergeben werden, wird im IDM konfiguriert.
- Sperrung von Berechtigungen oder Ressourcen bei Verlust der im IDM definierten Voraussetzungen. Z.B. Sperrung des Accounts bei Statusende (z.B. Exmatrikulation, Beschäftigungsende), oder Entzug rollenabhängiger Berechtigungen bei Gültigkeitsende der zugrunde liegenden Rolle (selbst wenn andere Rollen noch aktiv bleiben). Eine zeitliche Verzögerung der Sperrung (z.B. erst zwei Wochen nach Statusende) ist konfigurierbar.
- Löschung gesperrter Ressourcen sowie gespeicherter Nutzerdaten aus den Zielsystemen nach einem festgelegten Zeitraum.

Umsetzungen innerhalb des IDM

Automatisierte Prozesse sorgen für die Sperrung der im IDM gespeicherten Daten von Identitäten in einer definierten Frist nach ihrem Statusende, d.h. nach Ablauf aller zugeordneten Rollen. Genauso erfolgt deren endgültige Löschung aus dem IDM Datenbestand nach einem weiteren festgelegten Zeitraum automatisiert. Die Details zu den Zeiträumen und den genauen Umsetzungen sind im Kapitel 3 zum Löschkonzept aufgeführt.

Manuelles ID Management

Manuelle bzw. manuell angestoßene Administrationsvorgänge des Identitätsmanagement werden über die Webbasierte Schnittstelle des IDM durch autorisierte und mittels persönlichem Account authentisierte Personen durchgeführt. Zum Zweck des ID Managements erfolgt kein direkter Zugriff auf die in der IDM Core Datenbank oder in den angebundenen Zielsystemen gespeicherten Daten.

Zu den manuellen ID Management Tätigkeiten zählen z.B. die Registrierung neuer Identitäten von nicht in den Quellsystemen geführten berechtigten Personen, die Zuweisung von Rollen und Ressourcen, die Durchführung teilautomatisierter Prozesse, sowie die regelmäßige Kontrolle der Auswirkungen automatisierter Prozesse (Auditing).

Rollenbasiertes Berechtigungskonzept

Die Vergabe der zur Durchführung des ID Managements notwendigen Berechtigungen zur Einsicht und zur Verarbeitung gespeicherter Identitäts- und Ressourcendaten, sowie zur Ausführung bestimmter Prozesse, erfolgt auf Grundlage eines gestuften rollenbasierten Berechtigungsmodells.

Bestimmte Management Funktionen und Verantwortlichkeiten werden in differenzierten ID Management-Rollen mit entsprechenden Berechtigungen zusammengefasst. Diese sind von den im IDM Identitäten zugeordneten Statusrollen (ID-Rollen, z.B. Studierende, Beschäftigte, Doktoranden, Gäste) zu unterscheiden.

Management-Rollen werden realen, mit entsprechenden Aufgaben betrauten Personen zur Ausübung ihrer Verwaltungstätigkeit zugewiesen. Die Rollen werden nur an bereits im IDM als Beschäftigte der Hochschule geführte Identitäten zugewiesen. Die Zuweisung der Rollen und Berechtigungen endet automatisch mit Statusende der Identität (Beschäftigungsende), sie kann aber auch von vorne herein zeitlich befristet und jederzeit vorab wieder entzogen werden.

Die aktuell im IDM vergebenen Management-Rollen und administrativen Berechtigungen können jederzeit samt Bezug der für die Zuweisung verantwortlichen Person nachvollzogen werden. Gleiches gilt für die Historie solcher Zuweisungen, da jede Zuordnung bzw. Entziehung dieser Rollen im IDM Audit protokolliert wird.

Management Rollen

Im IDM Core wird folgender Grundstock von ID Management Rollen mit den beschriebenen Funktionen und Berechtigungen implementiert:

ID Management Rolle	Übersicht zu Funktionen und Berechtigungen
Admin	Grundlegende Administration (u.a. Zuweisung der weiteren Management Rollen). Einsicht in alle im IDM gespeicherten Daten, Durchführung aller im Webfrontend implementierten Funktionen.
IDManager	Verwaltung von Identitäten (Registrierung, Aktualisierung, ID-Rollen Zuweisung) Einsicht und Bearbeitung nahezu aller Daten von Identitäten und ihrer Ressourcen (ausgenommen sind die Einsicht gesperrter Daten, sowie die Bearbeitung aus der Quellsystemen stammenden Daten) Auditing von Änderungen an Identitäten
RessourceManager	Verwaltung der Ressourcen und Berechtigungen von Identitäten (z.B. Accounts) Einsicht in notwendige Daten von Identitäten (Identifizierung, Statusfeststellung) Einsicht und Bearbeitung von zugeordneten Ressourcen und Berechtigungen Auditing von Änderungen an Ressourcen und Berechtigungen

Admin

Die Rolle dient vor allem der Durchführung übergeordneter, über die Webschnittstelle freigegebener Administrationsaufgaben:

- Zuweisung und Entzug der weiteren spezifischeren Management-Rollen.
- Konfiguration bestimmter Parameter von Systemmodulen, Konnektoren und Prozessen.
- Steuerung und Parametrisierung automatisierter Prozesse, sowie Prüfung bzw. Kontrolle ihrer ordnungsgemäßen Ausführung.
- Vollständige Einsicht in sämtliche Auditing Protokolle.

Mit dieser Rolle ausgestattete Personen können sämtliche im IDM gespeicherten Daten einsehen, auch für andere ID Management Rollen gesperrte Daten und verfügen über alle in der IDM Admin Webanwendung implementierten Berechtigungen.

IDManager

Diese Rolle ist für die grundlegende Verwaltung von Identitäten vorgesehen und umfasst Berechtigungen zur Durchführung folgender Aufgaben:

- Registrierung von Identitäten, die nicht aus Quellsystemen bezogen werden.
- Validierung von Identitäten, die eine explizite Freigabe zur weiteren Zuordnung von Ressourcen und Berechtigungen erfordern.[1]
- Konsolidierung von Identitäten: Zusammenführung mehrfach erfasster Identitäten einer Person, d.h. Bereinigung von möglichen „Duplikat-Identitäten", die über getrennte Registrierungswege entstehen können (z.B. Studierende, die noch Hilfskraft werden, oder manuell erfasste Doktorandin wird später noch Beschäftigte).
- Zuweisung und Entziehung von ID-Rollen, Ressourcen (z.B. Zugehörigkeit zu einer Hochschuleinrichtung) und Berechtigungen, die nicht aus Quellsystemen bezogen werden (auch bei primär aus den Quellsystemen stammenden Identitäten, z.B. zusätzliche Rolle Doktorand bei einem Beschäftigten).
- Kontrolle (Auditing) der automatisierten Prozesse, d.h. der durchgeführten Importe und Aktualisierungen von Identitäten aus Quellsystemen, sowie der Verarbeitungen von Ressourcen und Berechtigungen.

Zur Ausübung der beschriebenen Aufgaben erhalten mit dieser Rolle ausgestattete Personen Einsicht in alle Identitätsdaten (Person, zugeordnete ID-Rollen und Ressourcen), sowie auf Protokolldaten des IDM Audit zu Änderungen von Identitäten, ihrer ID-Rollen und Ressourcen.

Eine Ausnahme bildet das Geburtsdatum von Identitäten. Dieses ist nicht direkt einsehbar, sondern bei der Validierung oder Zusammenführung von Identitäten, Zwecks einer eindeutigen Identifizierung, nur in Form eines Vergleichs, d.h. es wird angezeigt, ob das Geburtsdatum zweier Identitäten gleich, ungleich, oder ein Vergleich aufgrund eines fehlenden Datums nicht möglich ist.

Um die Verwaltung bestimmter Unterkategorien von Identitäten, die noch nicht aus den Quellsystemen der Verwaltung bezogen werden, an die verantwortlichen Hochschuleinrichtungen delegieren zu können, sind abgeleitete Rollen mit entsprechend eingeschränkten Zugriffs- und Administrationsrechten geplant (z.B. *IDManager:Gasthörer*, *IDManager:BIBExterne*).

RessourceManager

Für die IDM gestützte Zuteilung von Ressourcen und Berechtigungen an Identitäten werden verschiedene unter dieser Kategorie zusammengefasste Rollen bereitgestellt.

[1] Noch „zu validieren" sind Identitäten, bei deren Registrierung das IDM auf Basis von Namensgleichheit oder Ähnlichkeit eine Duplikats-Erfassung vermutet. Über diesen Marker wird eine manuelle Prüfung erzwungen, die entweder zur Bestätigung als neue Identität (Validierung) oder zur Zusammenführung mit einer vorhandenen Identität (Erfassung einer zusätzlichen Rolle) führt. Nur für valide Identitäten können Ressourcen generiert und Berechtigungen erteilt werden (bei automatisierten Prozessen wird dieses mit der Validierung nachgeholt).

Implementiert sind bereits *RessourceManager* Rollen für die

- Verwaltung von Accounts:
  Erstellung und Sperrung von Accounts und daran geknüpfter weiterer Nutzerressourcen wie Mail, Netzwerkspeicher, Nutzerkonto Dienst „X“, etc., oder das Zurücksetzen des Passworts.
- Zuweisung von Identitäten zu Status- oder Berechtigungsgruppen:
  Z.B. Ressourcen und Berechtigungen, die abhängig von der Zugehörigkeit zu bestimmten Hochschuleinrichtungen, Instituten, Abteilungen sind (Gruppenlaufwerke, Mailinglisten), oder von der Zuordnung von Kostenstellen zur Abrechnung bei kostenpflichtigen Diensten.
- Abfrage von Statusinformationen einer Identität:
  Etwa für Ressourcen, deren Vergabe nicht über im IDM realisierte Prozesse erfolgt, die aber zumindest die zuverlässige Überprüfung bestimmter Kriterien aus dem Referenzsystem IDM erfordert (d.h. lediglich Leserechte auf entsprechende Identitätsdaten).

Um das Treffen korrekter Entscheidungen bei der Berechtigungsvergabe zu ermöglichen, dürfen mit diesen Rollen ausgestattete Personen die dazu notwendigen Identitätsdaten einsehen. Dies umfasst Namen und Identifier zur eindeutigen Identifizierung (wem wird eine Berechtigung erteilt) und Daten zu ID-Rollen und Status (sind die Voraussetzungen erfüllt oder ist die angeforderte Berechtigung abzulehnen). Protokolldaten zu Änderungen der verantworteten Ressourcen sind ebenfalls einsehbar.

Die Rollen haben keine Berechtigung zur Registrierung und Änderung von Identitäten und Rollenzuordnungen. Zudem kann durch im IDM hinterlegte Regeln die Zuweisung bestimmter Ressourcen an bestimmte Voraussetzungen bzgl. der Identität (z.B. Status, ID-Rolle) geknüpft sein, sodass manche Zuweisungen nicht durchgeführt werden können.

Erweiterungen der Management Rollen

Eine Implementierung weiterer Rollen, bzw. eine weitere Ausdifferenzierung, kann sich aus zukünftigen neuen Anforderungen an weitere IDM gestützte Verfahren zur Vergabe von Ressourcen und Berechtigungen ergeben (z.B. durch die Anbindung neuer Zielsysteme). Bei einer Erweiterung oder Anpassung des Management Rollenkonzepts ist dann jeweils festzulegen, zu begründen und zu dokumentieren auf welchen Kreis von Identitäten und auf welche Identitätsdaten die Rolle Zugriffrechte erhält.

2.2. ID Self Management

Jede im IDM registrierte Identität kann sich mit ihrem persönlichen Account am webbasierten IDM Self Service anmelden und erhält damit Zugriff auf folgende Selbstverwaltungsfunktionen:

- Informationen zu eigenen im IDM gespeicherten personenbezogenen Daten, sowie zu Berechtigungen in Zielanwendungen einholen.
- Änderung eigener Account-Passwörter.
- Freischaltung oder Deaktivierung bestimmter Ressourcen und Berechtigungen beantragen oder falls berechtigt selbst durchführen (welche genau, hängt von Rollen und Status ab).
- Änderung bestimmter Kontaktdaten (sofern sie nicht aus einem Quellsystem stammen).

2.3. System Management

Administrative Aufgaben aus diesem Bereich dienen der Sicherstellung der technischen Funktionalität und des Betriebs der IDM Dienste.

Zu diesem Zweck erhalten namentlich benannte Personen als Systemadministratoren Zugriffsberechtigungen auf die IDM Systeme. Diese sind durch zum sicherheitsbewussten Umgang mit den Systemen und den darin verarbeiteten Daten angehalten, sowie zur Einhaltung der geltenden gesetzlichen Vorgaben des Datenschutzes verpflichtet.

Der Zugang erfolgt persönlich authentisiert, mittels auf den Systemen eingerichteter Systemnutzerkonten, und über die spezifizierten Schnittstellen (SSH, VM-Konsole) von definierten, freigegebenen Arbeitsplatzrechnern.

Zu den definierten Aufgaben mit entsprechenden Berechtigungen gehören:

- Überwachung (Monitoring), Wartung und Aktualisierung der Server, Betriebssysteme und Anwendungen.
- Konfiguration der IDM Applikation und Schnittstellen zu Quell- und Zielsystemen.
- Im Bedarfsfall Identifikation und Behebung von Fehlern.
- Testen und technische Inbetriebnahme von Erweiterungen, Aktualisierungen der IDM Anwendungen
- Dokumentation von Systemeinstellungen und deren Änderungen

3. Löschkonzept

Im IDM geführte Identitäten erreichen ihr Statusende mit Ablauf der Gültigkeit ihrer letzten zugeordneten ID-Rolle. Damit verfügen sie über keinen gültigen Status mehr, der die Berechtigung zur Nutzung von IT-Ressourcen der Hochschule begründet.

In der Regel wird das Statusende bereits mit Registrierung einer Identität als Befristung im IDM erfasst und bei Erfüllung entsprechender Voraussetzungen laufend verlängert.[2] Auch wenn für jede im IDM erfasste Identität ihr Statusende bekannt sein sollte, so ist dieses jederzeit über den IDM Self Service einsehbar, wird die betreffende Person rechtzeitig (mind. zwei Wochen) vorab von einem automatisierten IDM Prozess per Email an des bevorstehende Statusende und dessen Auswirkung auf bestehende Berechtigungen erinnert.[3]

Nach Statusende sorgt das IDM durch automatisierte bzw. teilautomatisierte Prozesse, zu definierten Zeitpunkten, für folgende Umsetzungen bis hin zur Bereinigung nahezu aller Daten und Berechtigungen einer vormals registrierten Identität:

Zeitpunkt nach Statusende	**Vorgänge im bzw. durch das IDM**
Umgehend	Ressourcen und Berechtigungen, die aufgrund rechtlicher Vorgaben auf den Tag genau nicht mehr bestehen dürfen, werden umgehend gesperrt (im Sinne der Deaktivierung der Zugriffsrechte/Funktionalität). Dies können z.B. arbeitsrechtliche Vorgaben bzgl. der Zugriffsrechte von Beschäftigten nach Vertragsende sein, oder vertragsrechtliche Verpflichtungen der Hochschule (z.B. Berechtigungen bzgl. lizensierten Medien im Bibliotheksbereich oder Vergünstigungen aufgrund eines bestimmten Status). Die Sperrungen erfolgen automatisiert durch Prozesse des IDM.
Maximal 8 Monate	Verbleibende aktive Ressourcen und Berechtigungen der Identität in den Zielsystemen werden gesperrt (im Sinne der Deaktivierung der Zugriffsrechte/Funktionalität). Z.B. Sperrung des Hochschul-Accounts und anderer Nutzerkonten, oder der Mailadresse. Die Sperrungen erfolgen automatisiert durch Prozesse des IDM. In begründeten Einzelfällen können diese zeitlich befristet hinausgezögert werden (vgl. dazu Abschnitt 2.1. zum Automatisierten ID Management).
1 Jahr	Im IDM gespeicherte Daten der Identität werden „gesperrt“ (im Sinne der Sichtbarkeit für ID Management Rollen). Die Sperrung erfolgt automatisiert durch das IDM. Die Einsicht in gesperrte IDM Daten wird jedoch gestattet: • Der Rolle Admin zur Wahrnehmung von Auskunftspflichten. • Dem IDM Prozess zur Registrierung von Identitäten (Importe aus Quellsystemen oder manuelle Eingabe), um die notwendige Konsolidierung mit einer in diesem Fall „gesperrten“ aber nachweislich

[2] Das Statusende von Studierenden oder Beschäftigten wird durch die automatisierten Importprozesse aus den entsprechenden Quellsystemen übernommen und aktualisiert.

[3] Ausnahmen in denen nur eine kurzfristigere Erinnerung möglich ist, sind frühzeitige Beendigungen des Status, wie z.B. die vorzeitige Exmatrikulation im laufenden Semester, ein vorzeitiges Beschäftigungsende oder der Abbruch einer Promotion.

	gleichen Identität zu ermöglichen. (Vergleichskriterien: Namen, Geburtsdaten, Quellsystem-ID). Damit wird auch im Sinne der Nutzerfreundlichkeit die Reaktivierung einer Identität mit ihren vormaligen Kennungen ermöglicht. Ressourcen und Nutzerdaten werden vom IDM mittels automatisierter Prozesse aus den Zielsystemen gelöscht, insofern die Zielsystemanbindung eine Löschung durch das IDM vorsieht.
2 Jahre	Im IDM gespeicherte personenbezogene Daten der Identität werden dauerhaft gelöscht. Die Löschung erfolgt teilautomatisiert nach vorhergehender Freigabe zur Löschung durch berechtigte Administratoren (Rolle Admin) über die IDM Admin Webschnittstelle. Ausgenommen von der Löschung sind folgende Daten: • Identitäts- und Benutzerkennungen werden zur Verhinderung einer erneuten Vergabe an eine andere Person dauerhaft als „gesperrt“ archiviert. • Email-Adressen werden in begründeten Fällen (z.B. aufgrund ihrer Verwendung in wissenschaftlichen Publikationen) für einen längeren vertretbaren Zeitraum für die Wiederverwendung gesperrt.

Hinsichtlich der zu einer Identität gespeicherten Protokolldaten greift folgendes Löschkonzept (vgl. Angaben zur Protokollierung in Kapitel 4.5):

5 Jahre	Löschung der im IDM Audit zur IDM Verfahrensdokumentation gespeicherten Protokolldaten (Vergabe, Änderung, Entzug von Ressourcen und Berechtigungen). Die Löschung erfolgt teilautomatisiert nach vorhergehender Freigabe zur Löschung durch berechtigte Administratoren (Rolle Admin) über die IDM Admin Webschnittstelle.

4. Maßnahmen zum Schutz der IDM Systeme und verarbeiteten Daten

Aufgrund der zentralen Rolle des IDM als führendem System für Identitätsdaten und für die Vergabe von Berechtigungen in den angeschlossenen Zielsystemen, sowie den daraus resultierenden Zugriffsberechtigungen in diesen Systemen, kommt dem Schutz der IDM Systeme und dem Schutz der von ihnen verarbeiteten Daten vor Ausspähung und Manipulation eine große Bedeutung zu.

Dazu werden die im Folgenden beschriebenen Maßnahmen getroffen. Eine detaillierte Auflistung ist in der Verfahrensbeschreibung des IDM Systems dokumentiert.

4.1. Zugriffskontrolle auf Netzebene

Die IDM Serversysteme werden in einem geschützten Netzwerkbereich (Servernetz) betrieben. Netzwerkzugriffe werden mittels des zentralen *Firewall* und *Routing* Dienstes der Hochschule kontrolliert und zugelassen. Dort hinterlegte Zugriffsregeln (Access Control Lists) schränken die erlaubten Zugriffe auf die IDM Systeme und die dort laufenden Anwendungen auf das definierte notwendige Minimum ein.

Auf Netzwerkebene werden folgende Zugriffe auf die IDM Systeme und die darin laufenden Anwendungen mittels Freigaben in der zentralen Firewall sowie in den Schnittstellen der Anwendungen gewährt:

System	**Schnittstelle**	**Zugriff von Systemen bzw. Netzbereichen**
IDM Core	Datenbank (sql) Datenbank (sql + ssl) Webservice ID Management (fcgi) Webservice Self Service (fcgi) SSH VM-Admin-Konsole	IDM Core (Localhost) Admin-Subnetz (befristete Freigabe) Webserver IDM Admin Webserver IDM Self Service Admin-Subnetz Admin-Subnetz
IDM Audit	Datenbank (sql + ssl) SSH	IDM Core Admin-Subnetz
Webserver IDM Admin	Web (https) SSH	Arbeitsplatz-Subnetze Admin-Subnetz
Webserver IDM Self Service	Web (https) SSH	Zunächst nur Hochschulnetze Admin-Subnetz
HSZ Transfer	SSH (SCP) SSH (SCP) SSH (SCP)	Export Server HSZ IDM Core Admin-Subnetz
IDM Print	SSH SSH	IDM Core Admin-Subnetz
Backup Service	TSM (tcp + ssl)	IDM Core, IDM Audit (TSM Client)
LDAP Directory Services	LDAP (SSL/TLS) LDAP (SSL/TLS) SSH	IDM Core Berechtigte Zielsysteme Admin-Subnetz
Shibboleth IDP	Web (https + SAML) SSH	Berechtigte Zielsysteme (Shib. Service Provider) Admin-Subnetz

Berechtigte Systemadministratoren erhalten zu allen IDM Systemen über die Secure Shell (SSH) Zugang auf Systemebene. Dieser ist lediglich für ein Subnetz freigegeben, in dem sich Arbeitsplatzrechner von berechtigter Administratoren befinden (Administratorennetz des technischen RZ Personals). Zusätzlich können authentisierte und autorisierte Administratoren auf die

virtualisierten Systemen (IDM Core) über die Administrationsschnittstelle der Virtualisierungsumgebung per Konsole zugreifen (etwa bei einem Ausfall des SSH Dienstes).

Zugriffe auf die IDM Core Datenbank erfolgen nur lokal auf dem IDM Core System durch die IDM Applikation sowie durch Administrationsprogramme der Datenbankanwendung. Datenbankzugriffe aus dem Netzwerk sind regulär gesperrt, können aber für Wartungsarbeiten durch Systemadministratoren aus dem Administratorennetz (bzw. von einzelnen IP Adressen) für einen limitierten Zeitraum in der Schnittstellenkonfiguration der Datenbankanwendung freigeben werden.

Der Zugriff auf die webbasierten Funktionen des IDM Core wird mittels Webserver realisiert, die, um die direkten Netzwerkschnittstellen des IDM Core Systems minimal zu halten, auf einem separaten System betrieben werden. Der Webzugriff erfolgt ausschließlich verschlüsselt mittels HTTPS Protokoll. Durch den Einsatz zweier unterschiedlicher Webserver (Virtual Hosts, die unter separaten IP Adressen erreichbar sind) für das ID Management und den IDM Self Service werden bereits auf Netzwerkebene getrennte Zugriffsberechtigungen auf die webbasierten Funktionen des IDM realisiert:

- Die Web-Schnittstelle für die ID Management Funktionen ist nur aus definierten hochschulinternen Subnetzen erreichbar (Arbeitsplatzrechner der Beschäftigten der Hochschule).
- Der Zugriff auf die IDM Self Service Web-Schnittstelle ist zunächst nur aus dem Hochschulnetz möglich (aus dem Internet nach erfolgter Einwahl via VPN). Mittelfristig wird eine freie Erreichbarkeit aus dem Internet angestrebt, um weitere, diese erfordernde Self Service Funktionen anbieten zu können (z.B. „Passwort-Zurücksetzung“).

Die Webserver greifen wiederum auf die entsprechenden Webservices der IDM Core Applikation für das ID Management und den Self Service mittels einer separaten Schnittstelle (z.B. FastCGI, HTTPS Reverse Proxy, etc.) zu (s. Anlage A).

Die automatisierten Prozesse des IDM Core, regelmäßiger Import und Abgleich der Daten aus den angeschlossenen Quellsystemen sowie die Umsetzung von Ressourcen und Berechtigungen in die Zielsysteme, werden durch einen entsprechenden Systemnutzer („idm“) ausgeführt. Dieser hat Berechtigungen die entsprechenden Skripte anzustoßen und auf die Quellsystem-Daten (lesend, je nach Quellsystem direkt oder per SCP auf die auf dem HSZ Transfersystem vorliegenden Exportdateien) sowie IDM-/Zielsystem-Daten (lesend und schreibend) zuzugreifen.

4.2. Authentisierung und Autorisierung

Zugriffe zur Verwaltung von Identitäten und ihrer Ressourcen, auf IDM Anwendungen, sowie zur Administration der Systeme erfolgen ausschließlich über die spezifizierten Schnittstellen und immer authentisiert durch Anmeldung mit einem persönlichen Account und qualifiziertem Passwort[4]. Zugriffsberechtigungen werden differenziert vergeben, d.h. entsprechend auf die für die Ausübung der jeweiligen Funktion als Identitätsverwalter oder Systemadministrator notwendigen Datenzugriffe beschränkt.

Die Systemadministration via SSH erfolgt immer authentisiert über entsprechend auf den IDM Systemen für berechtigte Administratoren eingerichtete persönliche Systemnutzerkonten.

[4] Mindestens 8 Zeichen, darunter mindestens jeweils ein Großbuchstabe, eine Ziffer und ein Sonderzeichen.

Genauso werden Zugriffe auf die IDM Core Datenbank und die IDM Audit Datenbank nur authentisiert mittels dazu eingerichteter Datenbanknutzerkonten gewährt. Die IDM Applikation verwendet eigene Nutzerkonten mit entsprechenden Zugriffsberechtigungen. Zur Datenbank-administration berechtigte Systemadministratoren erhalten in den Datenbanken eigene Nutzerkonten mit entsprechenden Berechtigungen.

Auf die Webservices der IDM Applikation kann nur nach Authentisierung mittels eines durch das IDM System verwalteten persönlichen Hochschul-Account zugegriffen werden. Dies gilt abschließend für die IDM Self Services. Der Zugriff auf ID Management Funktionen hingegen erfordert zusätzlich eine Autorisierung mittels Zuordnung einer der im vorhergehenden Kapitel zum Berechtigungskonzept beschriebenen ID Management Rollen.

Das Hochschulservicezentrum Reutlingen verfügt zur Übertragung der Datenexporte aus den Quellsystemen über ein eigenes Nutzerkonto auf dem HSZ Transfer Server. Ein dort eingerichtetes Nutzerkonto für die IDM Applikation gewährt dieser die Abholung der Dateien zur weiteren Verarbeitung. Genauso erhält die IDM Applikation mittels eines eigenen Nutzerkontos Zugriff auf den IDM Print Server, um die Ausgabe von Dokumenten anzustoßen.

4.3. IDM Systeme

Für den IDM Core und das IDM Audit System wird ein um Sicherheitsmodule erweitertes Linux Betriebssystem (*Security Enhanced*) eingesetzt. Beide Systeme werden als virtuelle Maschinen in der Virtualisierungsinfrastruktur der Hochschule (Produkt *VMware*) betrieben. Sicherheitsaktualisier-ungen der Betriebssysteme und Anwendungen werden regelmäßig und zeitnah durchgeführt.

4.4. Verschlüsselte Kommunikation

Zum Schutz der über Netzwerkverbindungen übertragenen Daten erfolgt die Kommunikation zwischen den IDM Systemen, sowie zwischen diesen und den angeschlossenen Quell- und Zielsystemen, ausnahmslos über verschlüsselte Verbindungen.

4.5. Sicherung von Daten und Systemen

Um im Bedarfsfall, z.B. bei einem Systemausfall oder einer festgestellten Kompromittierung, einen möglichst aktuellen und konsistenten Zustand wiederherstellen zu können, werden durch einen IDM Core Systemprozess automatische Sicherungen der IDM Datenbank auf einem separaten Backupsystem gespeichert. Die Datensicherung erfolgt einmal pro Nacht, bei Bedarf auch in kürzeren Zeitintervallen. Die Backups werden für einen Zeitraum von zwei Wochen aufbewahrt.

Für die Datensicherung wird der den PHs zur Verfügung stehende zentrale *Backup- und Archiv-Dienst* des SCC genutzt. Der Backup-Dienst setzt derzeit das IBM Produkt *Tivoli Storage Manager* (TSM) ein. Auf dem IDM Core und dem IDM Audit System wird der entsprechende TSM-Client installiert, welcher authentisiert (Sytem-ID, Passwort) über eine verschlüsselte Netzverbindung Datensicherungen zu definierten Zeitpunkten automatisch überträgt oder im Bedarfsfall dort gesicherte Daten wiederherstellt.

Zusätzlich werden in regelmäßigen Abständen, spätestens vor Systemaktualisierungen, Sicherungskopien des virtualisierten IDM Core erstellt (inkrementelle Snapshots, Klone der virtuellen Maschine), so dass dieser im Bedarfsfall schnell wieder verfügbar gemacht bzw. auf einen gewünschten vorherigen Zustand zurückgesetzt werden kann.

4.6. Protokollierung

Sämtliche automatisierte oder manuell über Webschnittstellen durchgeführte ID Management Prozesse, die gespeicherte Identitätsdaten und Zuordnungen von Ressourcen verändern, werden zum Zweck der Nachvollziehbarkeit samt Zeitpunkt und Urheber der Änderung im IDM Audit protokolliert. Dies betrifft insbesondere auch die Vorgänge zur Vergabe von administrativen Berechtigungen im IDM selbst.

Die IDM Audit Datenbank wird zum zusätzlichen Schutz der Protokolldaten vor Manipulation auf einem vom IDM Core getrennten System betrieben. IDM Core Prozesse dürfen, über einen dazu eingerichteten Datenbanknutzer, der Audit Datenbank nur weitere Daten zuführen sowie diese lesen, jedoch keine bereits gespeicherten Protokolldaten nachträglich verändern oder löschen.

IDM Core Systemprozesse (System- und Datenbankzugriffe, Datensicherungen, Anwendungen etc.) werden in System-Logdateien auf dem IDM Core und dem Audit System (per Syslog-ng) protokolliert.

Insgesamt werden folgende Vorgänge im IDM protokolliert:

Zweck der Protokollierung	**Umfang der Protokollierung**	**Rechtsgrundlage**	**Aufbewahrungs-dauer**
Nachweis über den Datenimport ins IDM	Erfolg, Misserfolg und Umfang des Imports von Daten aus den Quellsystemen.	Eingabekontrolle nach §9 Abs. 3 Nr. 7 LDSG, Transportkontrolle nach §9 Abs. 3 Nr. 9 LDSG.	2 Wochen (Störfall- / Changemanagement)
Nachweis über die Rechteverwaltung im IDM	Vergabe, Modifikation, Entzug von Zugangs- und Zugriffsrechten zur Ausführung von Tätigkeiten im IDM selbst.	Speicherkontrolle nach §9 Abs. 3 Nr. 3 LDSG, Zugriffskontrolle nach §9 Abs. 3 Nr. 5 LDSG.	5 Jahre (Verfahrens-dokumentation)
Nachweis über die Rechteverwaltung mittels IDM	Vergabe, Modifikation, Entzug von Zugangs- und Zugriffsrechten für die Zielsysteme des IDM, sowohl bzgl. der automatisierten als auch der manuellen Vorgänge.	Speicherkontrolle nach §9 Abs. 3 Nr. 3 LDSG, Benutzerkontrolle nach §9 Abs. 3 Nr. 4 LDSG.	5 Jahre (Verfahrens-dokumentation)
Nachweis über die Datensicherung	Automatische und manuell vorgenommene Daten-sicherungen (Zeitpunkt, Umfang, Erfolg), Erfolg vorgenommener Rückein-spielungen (sowie Tests).	Verfügbarkeitskontroll e nach §9 Abs. 3 Nr. 10 LDSG.	2 Wochen (Störfall- / Changemanagement)

Nachweis über systemtechnische Änderungen	Änderungen an den IDM Systemen (Zeitpunkt, Umfang, Art der Änderung)	Datenträgerkontrolle nach §9 Abs. 3 Nr. 2 LDSG.	2 Wochen (Störfall- / Changemanagement)

Diese Protokolldaten unterliegen der besonderen Zweckbindung aus § 15 Abs. 4 LDSG. Über die Protokolldaten besteht keine Auskunftspflicht nach § 21 Abs. 1 Satz 2 LDSG.

5. Anlagen

A. Grafische Übersicht zu IDM Systemen und Schnittstellen