Technische Universität Bergakademie Freiberg
Fakultät für Wirtschaftswissenschaft
Universitätsrechenzentrum

Anlage 1 zur Dienstvereinbarung Identitätsmanagement

Systembeschreibung und Datenfelder des Identity Management Systems

TU Bergakademie Freiberg
Akademiestraße 6
D–09599 Freiberg

Inhalt

1 Identitätsmanagementsystem (IDMS)

1.1 Begriffserklärung / Eingesetzte Software

Unter dem Begriff „Identitätsmanagement“ (IDM) versteht man die Verwaltung von personenbezogenen Daten einer Person. Je nach Zusammenstellung dieser Daten definiert sich eine Identität dieser Person. Eine Person kann mehrere Identitäten besitzen, wobei eine Identität jedoch immer genau einer Person zugeordnet wird. Beispielsweise kann eine Person an der TUBAF sowohl als Student als auch als Mitarbeiter geführt werden, was zwei Identitäten im jeweiligen Kontext der Verwaltung entspricht, aber die gleiche Person referenziert. Ein System zur Verwaltung verschiedener Personen und deren Identitäten wird als Identitätsmanagementsystem (IDMS) bezeichnet. Das IDMS hinterlegt die Informationen jeder Identität mit einem sogenannten Vertrag. Jede Identität wird zudem einer Organisationseinheit in einem hinterlegten Organigramm zugeordnet. Dieses enthält Beziehungen zwischen den einzelnen an der TUBAF vorhandenen Organisationseinheiten. Somit werden mittels der Informationen aus einer Identität sowie deren Zugehörigkeit zu einer Verwaltungseinheit Zugriffsrechte und weitere Attribute abgeleitet. So wird beispielsweise im Rahmen der Vergabe eines Logins für die IT-Dienste aus dem Vor- und Nachnamen einer Person deren E-Mail-Adresse abgeleitet.

Die Für die Einführung eines IDMS an der TUBAF hat sich die durch den beteiligten Dienstleister Maintainet AG im Zuge einer Rahmenvereinbarung angebotene Lösung auf Basis der Software „Novell Identity Managers 4.0 Advanced Edition“ mit den Komponenten „Integration Module 4.0 for Database“ und „Integration Module 4.0 for Tools“ sowohl aus technischer wie auch funktioneller Sicht klar durchgesetzt.

1.2 Anforderungen an ein IDMS für die TUBAF

Um der Anforderung gerecht zu werden, einen effizienten, sicheren und gemäß dem Datenschutz stattfindenden Informationsfluss zwischen unterschiedlichen und teils inkompatiblen IT-Systemen zu gewährleisten, wird ein über alle Teilsysteme übergreifendes IDMS geschaffen, welches die für die jeweiligen Verwal-

tungsaufgaben relevanten Daten zentral zur Verfügung stellt. Hierbei werden lediglich vorher definierte Daten aus den nachfolgend dargestellten Systemen gesammelt, gegebenenfalls aktualisiert (modifiziert) und anschließend für die Weiterverarbeitung bereitgestellt. Eine Aufschlüsselung dieser Daten (Attribute) wird in Abschnitt 2 gegeben. Es sind hierbei „Quellsysteme“ und „Zielsysteme“ zu unterscheiden:

- Quellsysteme stellen Daten für das IDMS bereit
- Zielsysteme erhalten Daten aus dem IDMS

Die an der TUBAF eingesetzten und für eine Integration in ein IDMS vorgesehenen IT-Systeme lassen sich hierbei wie folgt in Quell- und Zielsysteme einteilen:

Quellsysteme:

- HIS-COB – Kostenstelle (Daten ohne Personenbezug)
- Kartenmanagement

sowohl Quell- als auch Zielsysteme:

- HIS-SOS – Studentenverwaltung
- HIS-SVA – Personalverwaltung
- User Application (UA) – Nutzeroberfläche des IDMS (Verwaltung anderer Universitätsidentitäten (Gäste/Externe/Walk-In Kunden Bibliothek))
- Telefonie (indirekt)

Zielsysteme:

- Zentrale Nutzerdatenbank, u.a. zur Realisierung des Shibboleth-Dienstes – Authentifizierung für Zugriff auf (gesicherte, interne und externe) Webdienste
- HIS-POS (Prüfungsverwaltung)
- Libero – Bibliothek (Ausleihe)
- Siport – Zugriffskontrollsystem der Fa. Siemens
- Zeiterfassung CTI Leancom
- E-Mail
- Microsoft Active Directory / Microsoft Exchange

Der Zugriff auf die im IDMS gehaltenen Daten erfolgt über die oben genannte „User Application“. Dies ist das Modul des Systems, welches die grafische Benutzeroberfläche bereitstellt (Funktionsbeschreibung siehe auch Kapitel 3.1). Stammdaten können nur von (autorisierten) Mitarbeitern geändert werden. In der UA wird dem Nutzer zudem die Möglichkeit gegeben, sein Passwort zu ändern.

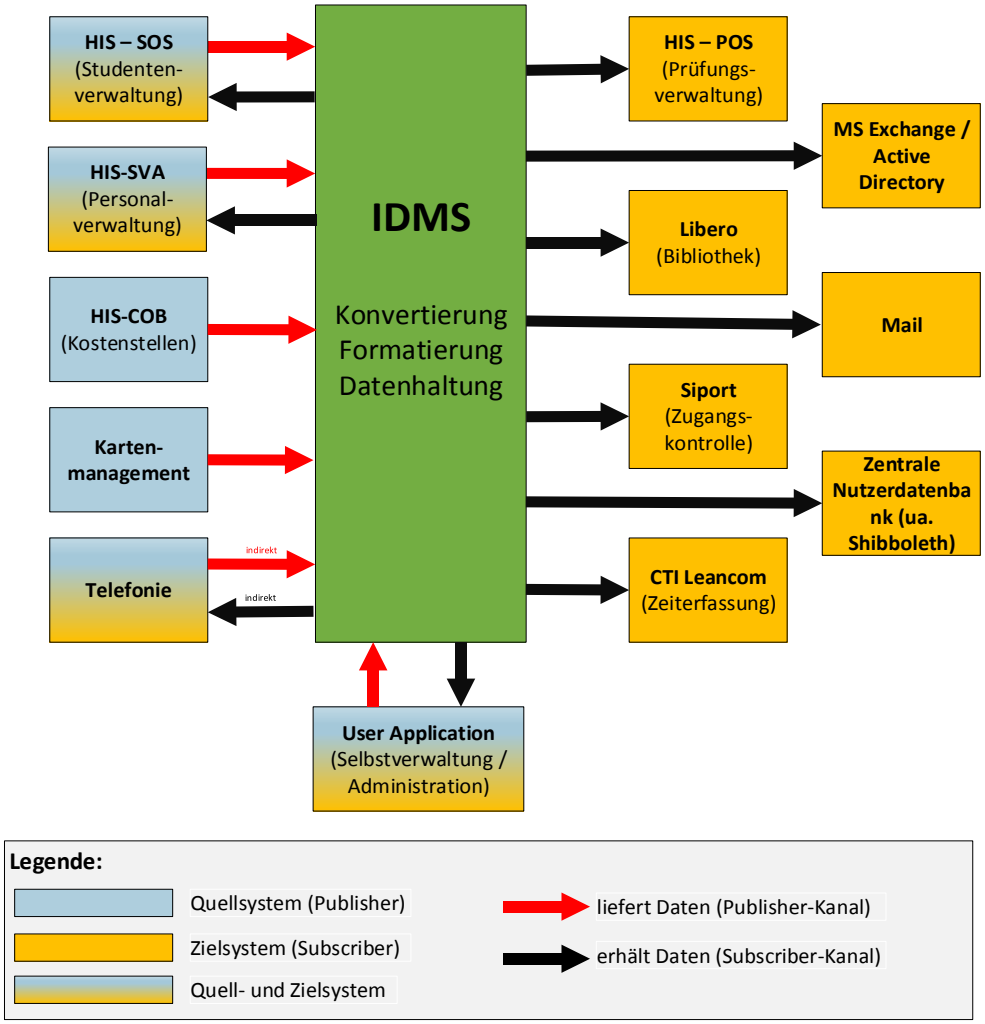

Abbildung 1 Quell- und Zielsysteme (Publisher-Subscriber-Modell)

1.3 Datenaustausch zwischen Verwaltungssystemen und IDMS

Um eine konsistente Datenhaltung über alle Teilsysteme hinweg zu organisieren, muss das IDMS in folgende verwaltungstechnische Vorgänge integriert werden:

- Neuen Datensatz in einem Quellsystem anlegen
- Vorhandenen Datensatz in einem Quellsystem ändern
- Vorhandenen Datensatz aus einem Quellsystem löschen

Um dies realisieren zu können, muss ein stetiger Informationsfluss zwischen Quellsystemen, IDMS und Zielsystemen gewährleistet werden. Sämtliche Datenübergaben erfolgen ausschließlich im Universitätsnetz unter Nutzung anerkannter verschlüsselter Übermittlungsverfahren wie SSH und LDAPS.

2 Personenbezogene Attribute im IDMS

Für jedes der Quell- und Zielsysteme wurde eine umfangreiche Analyse der zu verarbeitenden Daten vorgenommen, dies geschah in Abstimmung mit dem für Datenschutzfragen zuständigen Justiziariat der TUBAF. Dabei wurden zwei grundsätzliche Gründe für eine Datenhaltung im IDMS ausgewertet – Zum einen die unbedingte Notwendigkeit zum ordnungsgemäßen Betrieb der angeschlossenen Zielsysteme, zum anderen Attribute, die eine im IDMS verwaltete Person rollenunabhängig identifizieren. Dies ist notwendig, da eine Person, welche mehrere Rollen innerhalb der TUBAF inne hat (z.B. gleichzeitig Student und Mitarbeiter) eindeutig zu einer einzigen Identität im IDMS zugeordnet werden muss. Die folgende Tabelle 2 zeigt übersichtsweise die verwendeten Attribute und aus welchen Quellsystemen diese bezogen werden. Anschließend wird für jedes Attribut kurz beschrieben, warum die Aufnahme in das IDM-System erfolgt. Die Übergabe der Attribute an die Zielsysteme, welche datenschutzrechtlich durch entsprechende Verfahrensverzeichnisse untersetzt ist, wird in der Anlage 2 je Zielsystem erläutert.

Nr.	Datenfeld	Mitarbeiter – HIS-SVA	Studenten – HIS-SOS	Kartenmanagement	Kostenstellen – HIS-	Telefonie	UA - Gäste/Externe	UA - Externe Bibliothek	IDM-System
1	Nachname	x	x				x	x	x
2	Vorname(n)	x	x				x	x	x
3	Namenszusätze	x	x						x
4	Titel	x	x				x		x
5	Geburtsname		x						x
6	Geburtsdatum	x	x				x		x
7	Geburtsort	x	x						x
8	Geschlecht	x	x						x
9	Personalnummer	x							x
10	Matrikelnummer		x						x
11	Vertrags-Nr./Beschäftigungsverhältnisnummer	x							x
12	Vertragsbeginn	x	x				x	x	x
13	Vertragsende	x	x				x	x	x

Nr.	Datenfeld	Mitarbeiter – HIS-SVA	Studenten – HIS-SOS	Kartenmanagement	Kostenstellen – HIS-	Telefonie	UA - Gäste/Externe	UA - Externe Bibliothek	IDM-System
14	Abteilung/Organisationszugehörigkeit (Inhalt auch Kostenstelle)	x							x
15	Dienstart	x							x
16	Personalkategorie	x							x
17	Ident Nummer HIS		x						x
18	Fakultät		x						x
19	Studiengang		x						x
20	Vertiefung		x						x
21	Hörerstatus (Gast- / Haupt- / Nebenhörer)		x						x
22	Studienstatus		x						x
23	Studienart		x						x
24	Fachsemester		x						x
25	Aktuelles Semester		x						x
26	Nächstes Semester		x						x
27	Abschluss (angestrebter)		x						x
28	Bibliotheksnummer		x	x					x
29	Private Anschrift		x						x
30	Login-Name - Benutzername								x
31	Passwort								x
32	Kartennummer					x			x
33	Telefonnummer(n) (TUBAF)								x
34	E-Mail-Adresse(n) (TUBAF)								x
35	Full Name								x
36	E-Mail-Adresse (privat)							x	x
37	Vorname (internationalisiert)								x
38	Nachname (internationalisiert)								x
39	Gastverantwortlicher TUBAF						x		x
40	Zulassungsgrundlage Gast						x		x
41	Bereich/Mail-Subdomain								x
42	Status Account								x
43	Kostenstellenverantwortlichkeit								x

Nr.	Datenfeld	Mitarbeiter – HIS-SVA	Studenten – HIS-SOS	Kartenmanagement	Kostenstellen – HIS-	Telefonie	UA - Gäste/Externe	UA - Externe Bibliothek	IDM-System
44	Kostenstelle (Nummer)				x				x
45	Kostenstelle (Bezeichnung)				x				x
46	Übergeordnete Kostenstelle				x				x
47	Kostenstelle Bezeichnung - Langform				x				x
48	Benutzergruppe nach DFN AAI								x
49	Login Disabled /Sperrvermerk /Loginstatus								x
50	Berechtigungen						x		x

Tabelle 1: Personenbezogene Attribute IDM - Quellsystemsicht

Anmerkung: Für die Erstellung der Chipkarten (Kartenmanagement) müssen ebenfalls Attribute aus den Personal- und Studentenquellsystemen verarbeitet werden. Diese werden dem Kartenmanagementsystem über sogenannte Views (Einsicht in streng definierte Teile der Datenbanken) zur Verfügung gestellt, welche nicht Teil des IDMS sind. Das diesbezügliche Verfahrensverzeichnis und Datenschutzkonzept liegen neben der Dienstvereinbarung zur Nutzung einer multifunktionalen Universitätschipkarte an der TUBAF vor.

Nr. 1-3: Nachname, Vorname(n), Namenszusätze

Nachname, Vornamen und Namenszusätze dienen der Identifizierung einer Person beim Eintragen in das IDMS sowie der Generierung von Basisdaten wie Email- Adresse und Login-Name. Die Datenfelder Nachname, Vornamen, Namenszusätze und besitzen für die eindeutige Identifizierung einer Person beim Eintragen ihrer Daten in das IDMS eine Schlüsselfunktion.

Nr. 4: Titel

Ein Datenfeld für akademische Titel bzw. akademische Grade einer Person ist von Seiten der akademischen Anwendungen notwendig. Außerdem soll der Titel im Telefonverzeichnis angezeigt werden.

Nr. 5: Geburtsname

Der Geburtsname dient der eindeutigen Identifizierung einer Person beim Auftreten von Namenskonflikten. Im Falle einer Heirat im Zeitraum des Arbeitsvertrages kann sich der Nachname eines Nutzers ändern, obwohl es sich um ein und dieselbe Person handelt. Da auf einem bestehenden Verfahrensverzeichnis aufsetzend der Geburtsname der Mitarbeiter nicht gespeichert, wird, wird dieser Ablauf nicht für Mitarbeiter implementiert.

Nr. 6-7: Geburtsdatum/-ort

Geburtsdatum und -ort dienen der eindeutigen Identifizierung einer Person beim Auftreten von Namenskonflikten. So können z.B. die in der Personalverwaltung verwalteten Beschäftigten gleichzeitig als Studierende eingeschrieben sein. In diesem Fall muss überprüft werden, ob es sich um ein und dieselbe Person handelt.

Nr. 8: Geschlecht

Aus dem Geschlecht wird die korrekte Anrede einer Person abgeleitet (Herr bzw. Frau).

Nr. 9: Personalnummer

Die Personalnummer identifiziert einen Beschäftigten an der Universität eindeutig. Die hier verwendete Personalnummer entspricht nicht der durch die zentrale Gehaltstelle vergebenen Personalnummer. Innerhalb der operationellen Datenbank der Personalverwaltung sind Beschäftigte über ihre interne Personalnummer lebenslang eindeutig identifizierbar. Für einige universitätsinterne Arbeitsabläufe ist die interne Personalnummer unverzichtbar.

Nr. 10: Matrikelnummer

Die Matrikelnummer identifiziert einen Studierenden an der Universität eindeutig und ist lebenslang gültig. Innerhalb der operationellen Datenbank der Studentenverwaltung sind Studierende über ihre Matrikelnummer eindeutig identifizierbar.

Für viele universitätsinterne Arbeitsabläufe ist die Matrikelnummer unverzichtbar, wie z.B. bei der Eintragung von Prüfungsergebnissen.

Nr. 11: Vertrags-Nr./Beschäftigungsverhältnisnummer

Es gibt an der TUBAF nicht nur Studierdende, die parallel auch Mitarbeiter tätig sind, es haben auch viele Mitarbeiter gleichzeitig mehrere Arbeitsverträge, teilweise in unterschiedlichen Bereichen. Es wird allerdings immer nur eine Personalnummer vergeben. Die Beschäftigungsverhältnisnummer dient dazu, die aus den verschiedenen Arbeitsverträgen gesandten Attribute in einer Identität zu aggregieren und eine Zuordnung zum jeweiligen Arbeitsvertrag herstellen zu können.

Nr. 12/13: Vertragsbeginn/Vertragsende

Die Datenfelder spezifizieren für alle Personengruppen das Datum, an dem die Gültigkeit der Zugehörigkeit zur Universität beginnt bzw. abläuft. Diese Daten steuern Prozesse wie die Änderung der Organisationszugehörigkeit, Aktivierung und Deaktivierung von IT-Rechten sowie Zuteilung und Freigabe der an eine Person vergebenen Ressourcen.

Nr. 14: Abteilung/Organisationszugehörigkeit (Inhalt auch Kostenstelle)

Die Datenfelder für die Organisationszugehörigkeit enthalten die Nummer einer Organisationseinheit der Universität. Aus der Organisationszugehörigkeit sind vor allem Rechte und notwendige Ressourcen in den jeweiligen Organisationseinheiten ableitbar. Außerdem werden auf Basis dieses Attributes der Bereich und die Mail-Subdomain abgeleitet.

Nr. 15: Dienstart

Dienstart gibt Auskunft über den Charakter der Beschäftigung an der Universität. So ist zum Beispiel ein Studierender, der gleichzeitig als Beschäftigter der Personalkategorie „Wissenschaftliche Hilfskraft“ tätig ist, primär als Studierender anzusehen.

Nr. 16: Personalkategorie

Die Personalkategorie wird für die (transformierte) Übergabe an das Bibliotheksystem aufgenommen. Von der Personalkategorie hängen die detaillierten Nutzungsbedingungen (Ausleihfristen, Gültigkeiten) der Bibliothek ab.

Nr. 17: Ident Nummer HIS

Die Ident Nummer HIS wird von HIS bei der Bewerbung von Studenten generiert. Sie wird in das IDM-System aufgenommen, damit bei der Rückübergabe des Login-Namens und der E-Mailadresse eine Zuordnung des Login-Namens zur richtigen Ident-Nummer möglich wird. Nach Übergabe des Login-Namens kann die Person (Studierender) sich am Selbstbedienungsportal des HIS-Systems anmelden, um u.a. Rückmeldungen und Prüfungsanmeldungen vorzunehmen.

Nr. 18-27: Fakultät, Studiengang, -nummer, -art, Fachsemester, Vertiefung angestrebter Abschluss und Studienstatus

Die betreffenden Datenfelder dienen der Einordnung von Studierenden. Jeder Studierende kann in mehreren Studiengängen eingeschrieben sein. Jedem Studiengang ist ein Fachsemester zugeordnet, in dem sich der Studierende bezogen auf den betreffenden Studiengang gerade befindet. Angestrebter Abschluss und Immatrikulationsstatus sind ebenfalls damit verknüpft. Der Studienstatus ermöglicht darüber hinaus auch die Erkennung von Beurlaubung und Exmatrikulation von Studierenden. Die Informationen werden mit jeder Einschreibung und Rückmeldung aktualisiert. Damit existiert die Möglichkeit, Sonderrechte für Studierende abhängig von Studiengang, Fachsemester, angestrebtem Abschluss und Studienstatus zu vergeben. Außerdem sind die Attribute sind für den Bereich eLearning relevant, um die Berechtigungen für den Zugang zu den konkreten Lehrmaterialien via Shibboleth zu gewährleisten.

Nr. 28: Bibliotheksnummer

Die Bibliotheksbenutzernummer wird für den Bibliotheksbetrieb benötigt. Für Studierende wird diese im Studierendenverwaltungs- System HIS-SOS erfasst, für alle anderen Personengruppen wird sie initial im Kartenmanagementsystem generiert. Die Bibliotheksnummer wird über das IDM-System gemeinsam mit weiteren benötigen Attributen an die Bibliothek übermittelt. Personen mit Gast-Status erhalten keine Bibliotheksnummer.

Nr. 29: Private Anschrift

Die Anschrift besteht aus den Feldern Straße, Adresszusatz, Postleitzahl, Ort und Land. Sie dient der Abspeicherung der amtlich gemeldeten Postadresse einer Person. Im IDM-System wird lediglich die Privatadresse der Studierenden und Externen der Bibliothek gespeichert, mit dem ausschließlichen Zweck, diese an die Universitätsbibliothek weiterzuleiten. Dort wird diese für die Abwicklung von Mahnungsvorgängen benötigt. Aufgrund der vergleichsweise geringen Fallzahl wurde intern entschieden, die Mitarbeiteradresse für diesen Vorgang nicht vorzusehen.

Nr.30: Login-Name - Benutzername

Der Benutzername spezifiziert den Login-Namen einer Person für die Benutzung von IT-Diensten der Universität. Der Benutzername wird beim ersten Eintragen einer Person in das IDMS generiert (bzw. bei Studierenden bei der Einschreibung). Die Bildungsvorschrift des Login-Namen setzt sich aus den Anfangsbuchstaben von Vor- und Nachnamen, vier zufällig generierten Zahlen und vier Buchstaben (Konsonant und Vokal im Wechsel) zusammen. Beispiel Max Mustermann – Login-Name: mm4376nima

Nr. 31: Passwort

Das Passwort wird initial im IDM-System generiert und dort reversibel gespeichert. Durch die reversible Speicherung kann es dem Microsoft Active Directory sicher übergeben werden und dort für Authentifizierungsvorgänge u.a. am

Mailserver, dem Libero-System und den in der Domäne verwalteten Benutzerkonten für Mitarbeiter genutzt werden.

Nr. 32: Kartennummer

Die Kartennummer entspricht der Seriennummer der Karte, die vom Hersteller vergeben wurde. Diese wird an der TUBAF für verschiedene Anwendungen benötigt. Der direkte Bezug zum IDM-System und die damit verbundene Pflege ergeben sich durch die Verwendung der Kartennummer im Zeiterfassungs- und Zutrittskontrollsystem der TUBAF. Beide Systeme erhalten die Nummer vom IDMS.

Nr. 33: Telefonnummer(n) (TUBAF)

Das Datenfeld enthält die dienstlichen Telefonnummern, unter denen ein Beschäftigter zu erreichen ist. Hauptanwendung für diese Daten ist das hochschulinterne elektronische Telefonbuch.

Nr. 34: E-Mail-Adresse(n) (dienstlich) (TUBAF)

Das Datenfeld E-Mail-Adresse enthält die an der Universität gültige E-Mail-Adresse einer Person. Die E-Mail-Adresse wird beim ersten Eintragen einer Person generiert. Die bereits jetzt an Personen vergebenen E-Mail-Adressen müssen übernommen und der entsprechenden Identität im IDMS zugeordnet werden. Eine an der Universität gültige E-Mail-Adresse ist die Voraussetzung für den Nachrichtenaustausch zur Organisation des Arbeits- und Studienalltags sowie zur Inanspruchnahme der portalgestützten Dienste.

Nr. 35: Full Name

Der Full Name besteht aus dem vollständigen Vor- und Nachnamen der Person. Er wird vom Microsoft Active Directory verwendet, um bei universitätsinternen Telefonaten Anrufer nicht nur mit ihrer Nummer, sondern auch mit vollständigem Namen anzuzeigen.

Nr. 36: E-Mail-Adresse (privat)

Bei Externen der Bibliothek wird auf die Vergabe einer dienstlichen E-Mail-Adresse verzichtet, stattdessen wird die private E-Mail-Adresse der Person für die Kommunikation verwendet.

Nr. 37: Vorname (internationalisiert)

Der um Umlaute bereinigte (internationalisierte) Vorname wird für die E-Mail-Adressgenerierung benötigt.

Nr. 38: Nachname (internationalisiert)

Der um Umlaute bereinigte (internationalisierte) Nachname wird für die E-Mail-Adressgenerierung benötigt.

Nr. 39: Gastverantwortlicher TUBAF

Ein Gast-Konto wird von dem Mitarbeiter eingerichtet, der den Gast eingeladen hat. Dieser dient dem inhaltlichen Administrator als Ansprechpartner für alle ggf. mit dem Gast-Konto entstehenden Probleme.

Nr. 40: Zulassungsgrundlage Gast

Das Attribut wird im IDM von den Gast-Konto einrichtenden Mitarbeitern für den inhaltlichen Administrator gepflegt. Hier werden grundsätzliche Informationen über die Notwendigkeit der Anlage des Gast-Kontos gepflegt. Im Zweifelsfall kann so die Anlage eines Gast-Kontos vermieden werden.

Nr. 41: Bereich/Mail-Subdomain

Die Attribute werden an der TUBAF aus mehreren Gründen für eine Identität gepflegt. Zum einen werden die Bereiche (Beispiel: F6-BWL) im Web-Telefonverzeichnis für jede Person angezeigt, außerdem werden Sie für die E-Mail-Adressbildung der Mitarbeiter benötigt. Des Weiteren dient der Bereich der Administration des Microsoft Active Directorys als Indikator für die organisatorische Verortung der Person.

Nr. 42: Status Account

Die Datenfelder für den Status im IDM dienen der Abbildung von Bearbeitungszuständen in Abhängigkeit von den jeweiligen Arbeitsabläufen.

Nr. 43-47: Kostenstellenverantwortlichkeit, Kostenstellen: Daten zur Erstellung eines Organigramms

Da zur Etablierung des Berechtigungssystems ein Organigramm notwendig ist, wird auch die Kostenstellenhierarchie der TUBAF mittels des Controlling Moduls COB des HIS-GX Systems als Quellsystem verwendet. Dabei werden die entsprechenden Attribute ausgelesen, eine Übermittlung ergibt sich nur bei Änderungen in der Kostenstellenstruktur. Die Attribute werden verwendet, um eine konkrete Zuordnung zu Organisationseinheiten zur Ableitung von Rechten und Ressourcen in den Zielsystemen zu ermöglichen.

Die Information zum jeweils zugeordneten Kostenstellenverantwortlichen ist notwendig, um feststellen zu können, wer für die Erteilung von besonderen IT-Rechten für die betreffende Person Genehmigungsbefugnisse besitzt. Außerdem wird die Information für den internen Gebrauch (Information der Mitarbeiter) genutzt – dazu lässt sich aus dem IDM-System ein PDF-Dokument generieren, welches die Kostenstellen nebst den Verantwortlichen darstellt.

Nr. 48: Benutzergruppe nach DFN AAI

Die Datenfelder für die Benutzergruppe spezifizieren die Beziehung einer Person zur Universität auf generischer Ebene. Diese Datenfelder drücken eine nach Funktion und Stellung innerhalb der Universität typisierte Zugehörigkeit aus. Eine Einteilung findet in die Kategorien Angehöriger der Universität, Mitarbeiter, Student und Bibliotheks-Walk-In statt. Eine Person kann dabei auch in mehrere Kategorien fallen.

Nr. 49: Login Disabled /Sperrvermerk /Loginstatus

Gibt Information darüber ob ein Benutzerkonto außerordentlich gesperrt wurde. Da dies im Regelfall im Zeitraum des eigentlichen Vertragsverhältnisses mit der TUBAF geschieht, ist eine gesonderte Pflege notwendig.

Nr. 50: Berechtigungen

Dienen der Vergabe von Gruppen- und Einzelrechten an Personen/Personengruppen.

3 IDMS-Standardprozesse

3.1 Administrationskonzept - Differenzierte Vergabe von Zugriffsrechten (Benutzerprofile)

Die technische und inhaltliche Pflege und Administration des IDMS obliegt im Wesentlichen dem Universitätsrechenzentrum. Die Neueinrichtung und die direkte Personenbetreuung erfolgt durch den inhaltlichen Administrator (Frau Gläser), welcher auch die direkte Betreuung von Personen am Service-Desk übernimmt. Der technische Administrator (Herr Frost) wird ebenfalls als Betreuer im Bereich Service-Desk agieren, sowie ggf. auftretende technische Probleme am IDMS beheben und an der Weiterentwicklung des Systems beteiligt sein. Beide Mitarbeiter erhalten gesonderte Berechtigungen im System. Momentan erfüllen sowohl Frau Gläser als auch Herr Frost ähnliche Aufgaben im Bereich der Personenverwaltung am URZ.

Verwaltungsrelevante Daten können nur von autorisierten Mitarbeitern (Sub-Administratoren) modifiziert werden.

Abläufe des IDMS werden über die webbasierte grafische Oberfläche, die sogenannte User Application realisiert. Inmitten der User Application wird ein feingranulares Berechtigungssystem implementiert, welches sicherstellt, dass nur die jeweils mit der Aufgabe betreuten Mitarbeiter Zugriff auf die erforderlichen erhalten.

Für alle Mitarbeiter, die im Rahmen ihrer Tätigkeiten mit dem IDMS in Kontakt kommen werden umfangreiche, an den jeweiligen Aufgaben der Mitarbeiter orientierte, Schulungen durch das URZ mit Unterstützung durch die Maintainet AG durchgeführt.

3.2 Dokumentation zulässiger Auswertungen

Vom IDMS werden alle Neuzugänge, Datenänderungen und Abgänge protokolliert – ein Reporting über diese ist mittels des Reporting-Modules möglich, regelmäßig aber nicht vorgesehen.
Darüber hinaus beinhaltet das IDMS ein Tool – den Event Auditing Service - welches Modifikationen der Daten der Identität und Nutzerinteraktionen am Benutzerprofil (Passwortänderungen, Änderungen im Rückkanal) protokolliert. Eine Log-Auswertung von Nutzerinteraktionen über den IDMS-Kern hinaus ist nicht möglich.

3.3 Anlage neuer Identität im IDMS

Das Anlegen einer neuen Identität wird durch das Hinzufügen eines neuen Vertrages in das IDMS durch eines der Quellsysteme angestoßen. Sind noch keine Daten für diese Person vorhanden, so werden diese neu angelegt. Das mit der Anlage einer Identität erzeugte Benutzerkonto für die Nutzung von IT-Diensten ist vorerst funktionell eingeschränkt, solange die Person ihr Benutzerkonto nicht aktiviert hat. Personen werden bei der erstmaligen Anmeldung an der User Application dazu aufgefordert, ihr Einmalkennwort durch ein persönliches Kennwort zu ersetzen. Anschließend werden sie zur Benutzerkontenaktivierung geleitet. Dieser Aktivierungsprozess muss für jedes Benutzerkonto einmalig bei Neuanlage durchlaufen werden, bevor die Daten in die entsprechenden Zielsysteme provisioniert werden. Ebenfalls muss im Aktivierungsprozess die Zustimmung zur IUK und der UB-Benutzerordnung der TUBAF erfolgen. Das weitere Vorgehen zur Kontenaktivierung unterscheidet sich für Studenten, Mitarbeiter, Externe der Bibliothek und Gäste.

Solange die Person das Benutzerkonto noch nicht erfolgreich aktiviert hat, erhält sie keinen Zugang zu den Universitätssystemen (ausgeschlossen hiervon ist das Mailsystem).

3.4 Identity Lifecycle - Regelfristen für die Löschung von Verträgen eines Nutzers

Endet der letzte Vertrag einer Person, so wird dieser Vertrag gelöscht. Damit beginnt die Ablaufphase. Mit Beginn dieser Phase erfolgen die folgenden Aktionen:

- Anlegen von IDMS-spezifischen Richtlinien zum Verschieben in einen gesonderten Bereich für inaktive Identitäten innerhalb des IDMS
- Anlegen von IDMS-spezifischen Richtlinien zum Löschen der Identität und des damit verbundenen Benutzerkontos

Während der Ablaufphase ist das Benutzerkonto noch aktiv. Sie dient im Wesentlichen einer Karenz. Sollte innerhalb dieser Zeit ein neuer Vertrag für diese Person geliefert werden, so kann der alte aktive Zustand wieder hergestellt werden. Diese Phase dauert max.30 Tage (einstellbar).
Nach Ablauf der Ablaufphase werden alle Rollen von der Identität entfernt, alle verbliebenen Vertragsinformationen gelöscht und das Benutzerkonto wird deaktiviert. Anschließend wird die Identität in den inaktiven Bereich verschoben. Als Informationen verbleiben an der Identität:

- Stammdaten (Login der Person)
- Informationen zur E-Mail-Adresse
- Unix ID (wenn vorhanden)

Die Inaktivitätsphase dauert 180 Tage.

Nach Ablauf der Inaktivitätsphase wird das Benutzerkonto inklusive der personenbezogenen Daten vollständig im IDMS gelöscht. Die E-Mail Adresse und der Login-Name wird zur Blockierung im Bereich Sperre gespeichert, um eine Wiederverwendung zu auszuschließen.

3.4.1 **Löschen von Benutzerkonten innerhalb Vertragslaufzeit**

Eine Löschung von Benutzerkonten während der Vertragslaufzeit ist nicht vorgesehen. Für eine Sperrung des Benutzerkontos kann es verschiedene Gründe geben, auf eine Auflistung soll hier verzichtet werden.

4 Sicherheitskonzept

Es wurden zusätzliche Risikofaktoren betrachtet, diese sind in Tabelle 3 dargestellt. Diesen Risikofaktoren kann mit Maßnahmen des Rechenzentrums der TU-BAF begegnet werden. Darauffolgende Tabelle 4 stellt die Maßnahmen übersichtweise dar.

Risikofaktor	**Maßnahmen**
Diebstahl (Hardware)	1, 9, 13, 16, 17
Festplattenausfall	2, 3 ,4
Netzwerkausfall	5, 6
Ausfall der Stromversorgung	7
Zerstörung durch höhere Gewalt	3, 4, 8
Zerstörung durch Menschen	1, 2, 3, 4
Unberechtigter Zugriff	1, 5, 9, 10, 12, 13, 14, 15, 16
Missbräuchlicher Zugriff durch Administratoren	9, 10, 11, 12, 13, 14, 15, 16, 17
Missbräuchlicher Zugriff durch Betriebsfremde Personen	1, 5, 9, 12, 13, 14, 15, 16, 17

Tabelle 2: Risikofaktoren Betrieb IDM-System

Nr	**Maßnahme**
1	Standort in den nur für berechtigte Mitarbeiter zugänglichen Serverräumen der TU Bergakademie Freiberg.
2	Redundanter Betrieb der Server.
3	Betrieb der Komponenten in einem Cluster unter einer virtualisierten Umgebung (VMware)
4	Backupkonzept
5	Datenaustausch nur innerhalb des Netzes der TU Bergakademie Freiberg
6	Redundant ausgelegte Netzwerkkomponenten (z.B. Router, Switches)
7	Unterbrechungsfreie Stromversorgung der Server
8	Standort in den Serverräumen der TU Bergakademie Freiberg
9	Die administrativen Zugänge auf Ebene der Betriebssysteme von iManager, Verzeichnisdienst, Identity Manager und Workflow System sind, nach der Passwortrichtlinie der TU Bergakademie Freiberg, jeweils passwortgeschützt und können - durch Firewall-Regeln eingeschränkt - nur von dedizierten Konsolenserver aus, von berechtigten Administratoren erfolgen.
10	Benennung von nur 2 langjährigen, sensibilisierten Mitarbeitern des Rechenzentrums als Administratoren des Systems
11	Verpflichtung auf Wahrung des Datengeheimnisses
12	Protokollierung von Zugriffen
13	Ausdifferenziertes Zugriffsberechtigungs-Konzept, dass Zugriffe auf bestimmte Anwendungen von Administratoren und Anwendern rollenbasiert unterscheidet.
14	Schriftliches Antragsverfahren für Einrichtung und Änderung von Zugriffsberechtigungen.

15	Definiertes Abstimmungsverfahren von allen verantwortlichen Entscheidern der betroffenen Organisationen bei Anbindung neuer Zielsysteme.
16	Verschlüsselungsverfahren bei sämtlichen Datenübermittlungen (SSH, SSL).
17	reversible Verschlüsselung von Passwörtern mit einer Schlüssellänge von 4096 Bit innerhalb eines verschlüsselten Attributes (Schlüssellänge 2048 Bit) (siehe Abschnitt 4.4)

Tabelle 3: Maßnahmen Risikoreduzierung TU Bergakademie Freiberg

Abkürzungsverzeichnis

HIS	Hochschulinformationssystem
HIS-COB	HIS-Modul für Kosten- / Leistungsrechnung
HIS -POS	HIS-Modul für Prüfungsorganisation
HIS -SOS	HIS-Modul für Studentenverwaltung
HIS -SVA	HIS-Modul für Mitarbeiterverwaltung
IdM	Identitätsmanagement
IDMS	Identitätsmanagementsystem
IuK	Informations- und Kommunikationstechnik
KMS	Kartenmanagementsystem
SCHAC	Schema for Academia
UB	Universitätsbibliothek
VM	Virtuelle Maschine
VOIP	Voive over IP Telefonie
ZNDB	Zentrale Nutzerdatenbank

Technische Universität Bergakademie Freiberg
Fakultät für Wirtschaftswissenschaft
Universitätsrechenzentrum

Anlage 2 zur Dienstvereinbarung Identitätsmanagement Zielsysteme

TU Bergakademie Freiberg
Akademiestraße 6
D–09599 Freiberg

Inhalt

1 Zielsysteme IDMS – Übersicht

1.1 Aktuelle Zielsysteme

Gemäß Abschnitt 2.2 in der Anlage 1 unterscheidet ein IDMS nach Quell- und Zielsystemen, wobei ein System auch gleichzeitig Quell- und Zielsystem sein kann. Folgende Zielsysteme werden an das IDMS der TUBAF angebunden:

Zielsysteme

- Microsoft Active Directory / Microsoft Exchange (Anschnitt 2)
- E-Mail (Abschnitt 3)
- Zentrale Nutzerdatenbank (u.a. zur Realisierung Shibboleth) (Abschnitt 4)
- Libero – Bibliothek (Ausleihe) (Abschnitt 5)
- HIS-POS (Prüfungsverwaltung) (Abschnitt 6)
- Siport – Zutrittskontrollsystem (Abschnitt 7)
- Zeiterfassung CTI Leancom (Abschnitt 8)

Sowohl Quell- als auch Zielsysteme

- HIS-SOS – Studentenverwaltung (Abschnitt 9)
- HIS-SVA – Personalverwaltung (Abschnitt 10)
- User Application (UA) (Abschnitt 11)
- Telefonie (indirekt) (Abschnitt 12)

2 Zielsystem: Microsoft Active Directory/Microsoft Exchange

2.1 Systembeschreibung

Der Verzeichnisdienst des Rechenzentrums wird zur Authentifizierung und Autorisierung an den angeschlossenen Rechnern, zur Bereitstellung von Netzwerkspeicherplatz, Netzwerkdruckern und zur Verteilung von Software genutzt. Dazu wird jeder im IDMS verwalteten Person das notwendige Benutzerkonto zur Verfügung gestellt. Außerdem ist von außerhalb des Universitäts-Campus E-Mail-Zugriff, sowie Zugriff auf eigene auf dem Netzwerkspeicher gespeicherte Daten möglich. Ebenfalls ist der Verzeichnisdienst Basis für den Zugang zum Universitätsnetz über VPN. Darüber hinaus wird durch das Active Directory der Zugriff auf den Exchange-Mailserver realisiert (dies allerdings ausschließlich für Mitarbeiter).

2.2 Ziele

Ziel des Verzeichnisdienstes ist die Bereitstellung von EDV-Ressourcen für Beschäftigte und Studierende.

2.3 Benötigte Daten

Folgende Datenfelder von Beschäftigten werden aus dem Identity Management System im Verzeichnisdienst des Rechenzentrums benötigt:

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	Dient der Identifikation
2	Vorname	Siehe 1.
3	Titel	Titel der Person, wird für die Anzeige in der VOIP-Telefonie verwendet
4	Login-Name/Benutzername	Eindeutige Kennung TUBAF
5	Passwort	Kann durch die reversible Speicherung im IDMS verschlüsselt an das Active Directory übergeben werden. Die meisten Authentifizierungsvorgänge an der TUBAF werden am das Active Directory vorgenommen
6	Telefonnummer (TUBAF)	Die Dienstliche Telefonnummer wird im Adressbuch des Exchange-Servers angezeigt

7	E-Mail-Adresse(n) TU-BAF	Für den Exchange Server
8	Full Name	Bestehend aus Nach- und Vornamen – wird bei Anrufen der Person angezeigt.
9	Bereich/Mail-Subdo-main	Dient der organisatorischen Verortung der Person im Verzeichnisdienst

2.4 Administration

Das passwortgeschützte Microsoft Active Directory wird von einer Mitarbeiterin des Rechenzentrums und klar definierten Teil-Administratoren in den Zentralen Einheiten und den Fakultäten administriert.

2.5 Datenschutz

Die Aufrechterhaltung des Datenschutzes im Verzeichnisdienst des Rechenzentrums ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (die Administratoren) und durch Abschirmung von unberechtigtem Zugriff nach außen (sowohl gegen das campusinterne Netz als auch gegen das Internet) gewährleistet.

2.6 Art der Datenweitergabe und –verwendung

Der Datenfluss ist unidirektional aus dem Identity Management System in den Verzeichnisdienst des Rechenzentrums festgelegt. Änderungen im Verzeichnisdienst des Rechenzentrums werden nicht in das Identity Management System übernommen.

Grundsätzlich handelt es sich bei Neuanlage und Ablauf der Benutzerkonten von Beschäftigten und Studierenden um automatisch ablaufende Prozesse. Nur im Ausnahmefall soll ein manueller Eingriff durch die Administratoren erfolgen. Die Ableitung der Berechtigungen des Benutzerkontos erfolgt anhand der Zugehörigkeit zu Organisationseinheiten.

3 E-Mail Server

3.1 Systembeschreibung

Der Hauptmailserver der TUBAF und wird von allen Einrichtungen als Host genutzt. Er dient der Sicherstellung der E-Mail-Kommunikation über alle Personengruppen.

3.2 Ziele

Für die Belieferung des Mailservers durch das IDMS sind alle E-Mail-Adressen einer Person im IDMS einzutragen. Zudem ist die Aliasdatei[1] zu beliefern, die alle gültigen, zusätzlichen Mailadressen enthält.

3.3 Benötigte Daten

Folgende Datenfelder von Beschäftigten werden aus dem Identity Management System im Mailserver des Rechenzentrums benötigt

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	In der Emailadresse enthalten
2	Vorname(n)	In der Emailadresse enthalten
3	Login-Name	Dient der Identifikation
4	E-Mail-Adresse(n)	Zur Sicherstellung der Kommunikation

3.4 Administration

Der zentrale Mailserver wird von einem Mitarbeiter des Rechenzentrums administriert. Nur dieser kann sich am Server authentifizieren und autorisieren. Weitere Administratoren sind nicht benannt, es gibt allerdings einen benannten Vertreter für Abwesenheitszeiten des eigentlichen Administrators.

3.5 Datenschutz

Die Aufrechterhaltung des Datenschutzes wird durch den klar benannten Administrator sichergestellt. Nur dieser hat die Berechtigung, Daten auf dem Server einzusehen. Der E-Mail Verkehr selbst ist für jede Person passwortgeschützt realisiert.

[1] Ein E-Mail Alias ist eine alternative E-Mail-Adresse für ein bereits bestehendes Postfach

3.6 Art der Datenweitergabe und –verwendung

Die Übertragung der Daten erfolgt über Dateien. Geplant ist, die Daten um 23:50 Uhr des jeweiligen Tages bereit zu stellen. Die Bereitstellung erfolgt durch das IDMS in einem definierten Verzeichnis. Die Daten sind durch Zugriffsbeschränkungen nur für das IDMS und den Mailserver abrufbar

4 Zentrale Nutzerdatenbank (ZNDB)

4.1 Systembeschreibung / Ziele

Die Zentrale Nutzerdatenbank wird an der TUBAF neben direkt vom IDMS beeinflussten Prozessen für weitere, dem IDMS nachgelagerte Prozesse verwendet. Folgende Funktionalitäten werden umgesetzt.

- Shibboleth-Authentifizierung (Abschnitt 4.2.1)
- Nutzerservice: Generieren von zusätzlichen Mailaliasen über Mailpool-Funktionalität (Abschnitt 4.2.2)
- Nutzerdatenlieferung an weitere, außerhalb des URZ administrierte Active Directorys (Studierende) (Abschnitt 4.2.3)
- Service: Bereitstellung des webbasierten E-Mail- und Telefonverzeichnisses (Abschnitt 4.2.4)
- Service: Versand des Uni-Info-Letters (Abschnitt 4.2.5)
- Export Vorlesungsverzeichnis (Abschnitt 4.2.6)
- Service: Buchung von VM-Ressourcen (Abschnitt 4.2.7)

In Abschnitt 4.2 ist nur der Teilausschnitt mit den an die ZNDB übermittelten Attributen dargestellt, die nachfolgenden Unterabschnitte stellen die Funktionalitäten detailliert dar.

4.2 Benötigte Daten - Übersicht

Folgende Datenfelder werden aus dem Identity Management System in der ZNDB benötigt. Die Tabelle stellt für jede der in 4.1 Beschriebenen Vorgänge die benötigten Daten detailliert dar.

	Shibboleth	Mailpool	AD BWL	AD Maschinenbau	AD Informatik	E-Mail / Telefonverzeich-	Versand Uni-Info-Letter	Vorlesungsverzeichnis	VM-Ressourcen
Nachname	x		x	x	x	x	x	x	
Vorname(n)	x		x	x	x	x	x	x	
Titel							x	x	
Personalnummer	x							x	
Matrikelnummer	x								
Vertragsbeginn									
Vertragsende			x						
Studiengang	x								
Vertiefung	x								
Fachsemester	x								
Abschluss (angestrebt)	x								
Login-Name - Benutzername	x		x	x	x			x	x
Emailadresse(n) (TUBAF)	x		x		x	x	x		
Bereich/Mail-Subdomain	x	x	x	x	x	x	x	x	
Status Account			x	x	x				
Kostenstelle (Nummer)		x							
Kostenstelle (Bezeichnung)		x							
Kostenstelle Bezeichnung - Langform		x							
Benutzergruppe	x								
Login Disabled /Sperrvermerk /Loginstatus							x		
Berechtigungen	x								

4.2.1 **Shibboleth-Authentifizierung**

Das etablierte Shibboleth-Verfahren wird an der TUBAF mittels der ZNDB realisiert. Der Hauptanwendungsbereich ist das Themengebiet des eLearning, damit verbunden die Authentifizierung und Autorisierung am OPAL-System der Bildungsportal Sachsen GmbH. Die Attributübersicht zeigt die maximale Ausprägung der von den verschiedenen Diensteanbieter abgefragten Attribute.

An verschiedene Diensteanbieter wird ein unterschiedlicher Umfang an Daten weitergegeben. An die meisten nur die Benutzergruppe (eingeteilt in Mitarbeiter, Studenten, Externe Bibliothek und sonstige Angehörige). In jedem Fall werden

der Person beim Anmeldevorgang die zur Übertragung vorgesehenen Daten explizit angezeigt. Erfolgt keine Zustimmung, werden keine Daten weitergegeben.

Nr.	Datenfeld	Anmerkung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Personalnummer	Eindeutige Kennung Mitarbeiter
4	Matrikelnummer	Eindeutige Kennung Studierende
5	Studiengang	Autorisierung Studierende, vor allem für Lehrmaterialen
6	Vertiefung	Siehe 5.
7	Fachsemester	Siehe 5.
8	Abschluss (angestrebt)	Siehe 5.
9	Login-Name - Benutzername	Authentifizierung
10	Emailadresse(n) (TUBAF)	Werden bei manchen Diensteanbietern als Kontaktadresse hinterlegt
11	Bereich/Mail-Subdomain	Siehe 5.
12	Benutzergruppe	Bestimmt die Rolle – Mitarbeiter können z.B. Lehrmaterialen einstellen, Studierende nicht
13	Berechtigungen	Gesonderte Berechtigungen, betrifft nur einzelne Personen

4.2.2 Nutzerservice: Generieren von zusätzlichen Mailaliasen (Mailpool)

Wurden über das Webinterface „E-Mail-Adressverwaltung“ zusätzliche Mailaliase für definierte Subdomains von tu-freiberg.de gebucht, so werden diese in der ZNDB-Datenbanktabelle „mailpool“ hinterlegt. Diese zusätzlichen Mailaliase werden nicht an das IDMS übertragen.

Nr.	Datenfeld	Anmerkung
1	Bereich/Mail-Subdomain	Zuordnung Bereich – Kostenstelle - Subdomain
2	Kostenstelle (Nummer)	Siehe 1.
3	Kostenstelle (Bezeichnung)	Bezeichnung der Kostenstelle
4	Kostenstelle Bezeichnung - Langform	Bezeichnung der Kostenstelle ohne Abkürzungen

4.2.3 **Nutzerdatenlieferung (Studenten) an weitere, URZ-externe ADs**

Neben dem am URZ betriebenen AD werden noch drei weitere ADs innerhalb der TU Freiberg betrieben:

- BWL
- Informatik
- Maschinenbau

Diese ADs dienen der Verwaltung von PC-Pools, in denen den sich die berechtigten Studierenden authentifizieren können sollen. Die ADs werden durch Skripte über neu hinzugekommene und zu löschende Nutzer aus den zugangsberechtigten Studiengängen informiert. Die Übergabe der Daten an die ADs erfolgt weiterhin über die bisher eingesetzten Skripte.

Je AD ist in den Fakultäten ein Mitarbeiter als Administrator definiert. Nur dieser erhält Vollzugriff auf die Daten.

AD BWL

Nr.	**Datenfeld**	**Anmerkung**
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Vertragsende	Gültigkeitsfrist
4	Login-Name - Benutzername	Wird übertragen, damit Studierende sich am spezifischen PC-Pool der Fakultät mit ihrem vom URZ vergebenen Login-Namen authentifizieren können. Es ist allerdings zu beachten, dass im Regelfall ein separates Passwort vergeben werden muss
5	Emailadresse(n) (TUBAF)	Kontaktadresse für den Administrator
6	Bereich/Mail-Subdomain	Gegenprüfung, ob Studierende Berechtigt ist
7	Status Account	Aktiv/Inaktiv – Inaktive Accounts werden gesperrt

AD Maschinenbau

Nr.	Datenfeld	Anmerkung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Login-Name - Benutzer-name	Wird übertragen, damit Studierende sich am spezifischen PC-Pool der Fakultät mit ihrem vom URZ vergebenen Login-Na-men authentifizieren können. Es ist aller-dings zu beachten, dass im Regelfall ein separates Passwort vergeben werden muss
4	Bereich/Mail-Subdomain	Gegenprüfung, ob Studierende Berechtigt ist
5	Status Account	Aktiv/Inaktiv – Inaktive Accounts werden gesperrt

AD Informatik

Nr.	Datenfeld	Anmerkung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Login-Name - Benutzer-name	Wird übertragen, damit Studierende sich am spezifischen PC-Pool der Fakultät mit ihrem vom URZ vergebenen Login-Na-men authentifizieren können. Es ist aller-dings zu beachten, dass im Regelfall ein separates Passwort vergeben werden muss
4	Emailadresse(n) (TUBAF)	Kontaktadresse für den Administrator
5	Bereich/Mail-Subdomain	Gegenprüfung, ob Studierende berechtigt ist
6	Status Account	Aktiv/Inaktiv – Inaktive Accounts werden gesperrt

4.2.4 Service: Bereitstellung des webbasierten E-Mail- und Telefonverzeichnisses

Es existiert ein Webservice für die Suche von Telefonnummern und E-Mail-Adressen von Mitarbeitern. Die Suche erfolgt hierbei über den Nach- und/oder Vornamen des Mitarbeiters. Das Verzeichnis wird von dem Administrator der Telefonanlage der TUBAF betreut. Nur dieser erhält Vollzugriff auf die Daten.

Nr.	Datenfeld	Anmerkung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.

3	E-Mail-Adresse(n) (TU-BAF)	Werden im Verzeichnis nach Suche angezeigt
4	Bereich/Mail-Subdomain	Siehe 3.

4.2.5 **Service: Versand des Info-Letters**

Es existiert ein Service für den Versand von Rundmails „Info-Letter“ an alle dafür registrierten Mitglieder der TUBAF. Hierbei sind folgende Rundmails zu unterscheiden:

- „**Uni-Info-Letter**“ – enthält allgemeine und studienrelevante Informationen, welche von allen TU-Angehörigen geschrieben werden können. Studenten erhalten diese Rundmail immer (Pflicht), Mitarbeiter können sich für den Empfang bei der Anmeldung am URZ freiwillig registrieren.
- „**Info-Letter**“ – Rundmail nur für Mitarbeiter der TU Freiberg, wird an alle Mitarbeiter versendet (Pflicht)
- „**Prof-Letter**“ - Rundmail nur für Professoren der TU Freiberg, wird an alle Professoren versendet (Pflicht)

Der Versand aller Rundmails erfolgt täglich 2:00 über einen Listserver. Die hierfür benötigten Listen werden über die ZNDB generiert. Es ist keine gesonderte Administration notwendig.

Nr.	**Datenfeld**	**Anmerkung**
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Titel	Zur Unterscheidung, welcher Info-Letter versendet werden soll
4	E-Mail-Adresse(n) (TU-BAF)	Kontaktadressen
5	Bereich/Mail-Subdomain	Zur Unterscheidung Mitarbeiter und Studenten
6	Login Disabled /Sperrvermerk /Loginstatus	Ist dieses Attribut auf „true“ gesetzt, erfolgt kein Versand des Info-Letters

4.2.6 **Export Vorlesungsverzeichnis**

Es erfolgt ein Export von Mitarbeiter-Daten an das elektronische Vorlesungsverzeichnis, welches ebenfalls vom Rechenzentrum der TUBAF administriert wird. Die Mitarbeiter haben hier die Aufgabe, Beschreibungen zu Vorlesungen und anderen Lehrveranstaltungen einzupflegen.

Das Vorlesungsverzeichnis wird von einem Mitarbeiter im Rechenzentrum betreut. Nur dieser erhält Vollzugriff auf die Daten.

Nr.	Datenfeld	Anmerkung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Titel	Titel des Mitarbeiters, nur intern genutzt
4	Personalnummer	Eindeutige Kennung Mitarbeiter
5	Login-Name - Benutzer-name	Wird übertragen, damit dem Mitarbeiter auch für diese Funktionalität eine Authen-tifizierung mittels dem vom URZ vergebe-nen Login-Namen möglich ist.
6	Bereich/Mail-Subdomain	Benötigt der Administrator zur organisato-rischen Verortung des Mitarbeiters

4.2.7 **Service: Buchung von VM-Ressourcen**

Am Rechenzentrum können über ein automatisiertes Web-Formular virtuelle Maschinen beantragt werden. Dieses Formular sowie alle damit verbundenen Abläufe bleiben erhalten, durch das IDMS muss der ZNDB lediglich der Login-Name bereitgestellt werden.

Die Buchung von VM-Ressourcen wird von einem Mitarbeiter im Rechenzentrum betreut.

Nr.	Datenfeld	Anmerkung
1	Login-Name	Eindeutige Nutzerkennung, wird übergeben, um die Authentifizierung am VM-Server zu ermöglichen

4.3 Administration

Die ZNDB wird von zwei definierten Mitarbeitern des Rechenzentrums (und einem benannten Vertreter) betreut. Diese Administratoren sind gleichzeitig die Administratoren des IDMS. Nur der technische Administrator hat einen Vollzugriff auf die passwortgeschützte Datenbank.

4.4 Datenschutz

Die Aufrechterhaltung des Datenschutzes in der Zentralen Nutzerdatenbank ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (die Administratoren) und durch Abschirmung von unberechtigtem Zugriff nach außen (sowohl gegen das campusinterne Netz als auch gegen das Internet) gewährleistet.

4.5 Art der Datenweitergabe und –verwendung

Der Datenfluss ist unidirektional aus dem Identity Management System in die Zentrale Nutzerbank festgelegt. Vom IDMS unabhängige Datenänderungen in der ZNDB sind nicht vorgesehen, daher ist ein Rückfluss von Daten in das Identity Management System nicht erforderlich. Grundsätzlich handelt es sich bei den beschriebenen Prozessen um automatische, aus dem Identity Management System heraus angestoßene Prozesse. Nur im Ausnahmefall soll ein manueller Eingriff durch die Administratoren erfolgen.

5 Libero – Universitätsbibliothek

5.1 Systembeschreibung

Das Libero-System der Universitätsbibliothek dient der Verwaltung der Bibliothekskonten aller Personen. Dabei werden in der Bibliothek Studierende, Mitarbeiter und Externe unterschieden. Im Libero-System werden die Daten inklusive aller Ausleihvorgänge gespeichert, außerdem ist der Katalog der Bibliothek zur Recherche beinhaltet. In der Universitätsbibliothek gibt es darüber hinaus eine Reihe von Recherche PC-Arbeitsplätzen, die hardwareseitig perspektivisch in einer separaten Active Directorys verwaltet werden/ bzw. werden sollen.

5.2 Ziele

Ziel ist ein automatisiertes Management der Kontenanlage im Bibliothekssystem, außerdem wird mittels des IDMS die Authentifizierung am Bibliothekssystem über das Active Directory realisiert.

5.3 Benötigte Daten

Für die verschiedenen Nutzergruppen werden verschiedene Datenfelder benötigt. Die Aufnahme der Datenfelder orientiert sich an den Bibliotheks-Prozessen und der Anzahl der Mahnvorgänge. Externe der Bibliothek erhalten gesonderte Basis-Berechtigungen, welche lediglich die Anmeldung an den Recherche-PC-Arbeitsstationen ermöglichen.

Nr.	Datenfeld	Anmerkung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Geburtsdatum	Siehe 1.
4	Geschlecht	Zur Generierung einer Anrede für Anschreiben
5	Personalnummer	Eindeutige Identifizierung Mitarbeiter
6	Matrikelnummer	Eindeutige Identifizierung Studierende
7	Vertragsbeginn	Zur Setzung von Gültigkeitsfristen
8	Vertragsende	Zur Setzung von Gültigkeitsfristen
9	Personalkategorie	Beeinflusst Ausleihfristen Mitarbeiter
10	Bibliotheksnummer	Eindeutige Identifikation Libero-System
11	Private Anschrift	Nur bei Studierenden und Externen – Für Mahnungsschreiben
12	Login-Name / Benutzername	Zur Authentifizierung am Libero-System gegen den Verzeichnisdienst der TUBAF

13	Kartennummer	Wird für das Spind System der Bibliothek benötigt
14	E-Mail-Adresse (TUBAF)	Für Mahnvorgänge, nicht bei Externen der Bibliothek
15	E-Mail-Adresse (privat)	Für Mahnvorgänge, nur bei Externen der Bibliothek

5.4 Administration

Das Libero-System wird von Administratoren in der Bibliotheks-EDV-Abteilung betreut. Nur diese namentlich benannten Administratoren haben einen Vollzugriff auf das System.

5.5 Datenschutz

Der Datenschutz wird durch die Benennung fester Administratoren in der EDV-Abteilung der Universitätsbibliothek sichergestellt. Der Zugriff auf das Libero-System und den administrativen Bereich erfolgt ausschließlich passwortgeschützt. Darüber hinaus werden für Datenübergaben ausschließlich verschlüsselte Verbindungen genutzt.

5.6 Art der Datenweitergabe und –verwendung

Die Datenweitergabe erfolgt, die Zustimmung zu den Nutzungsbedingungen der Bibliothek vorausgesetzt, automatisch. Es erfolgt eine Transformation der Daten nach streng definierten Regeln. Der Datenfluss ist unidirektional aus dem Identity Management System in das Libero-System festgelegt. Unabhängige Datenänderungen im Libero-System sind für die übergebenen Attribute nicht vorgesehen, daher ist ein Rückfluss von Daten in das IDMS nicht erforderlich.

6 HIS-POS (Prüfungsverwaltung)

6.1 Systembeschreibung

Das POS-Modul des HIS-Systems der TUBAF dient der Prüfungs- und Notenverwaltung der Studierenden durch die dazu berechtigen Mitarbeiter in der Verwaltung und den Fakultäten.

6.2 Ziele

Ziel der Anbindung des POS-Modules an das IDMS ist die Übermittlung von Lehrenden- und Prüferdaten, um die Erstellung und Benotung von Prüfungsleistungen zu ermöglichen. Dabei muss noch zwischen Mitarbeitern, die neben ihrer Beschäftigung auch an der TUBAF studieren und klassischen Mitarbeitern unterschieden werden.

6.3 Benötigte Daten

Folgende Datenfelder von Beschäftigten werden aus dem IDMS im POS-Modul benötigt:

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Namenszusätze	Siehe 1.
4	Titel	Titel des Prüfenden/Lehrenden
5	Geschlecht	-
6	Personalnummer	Eindeutige Kennung Mitarbeiter
7	Abteilung / Organisationseinheit	Organisatorische Zuordnung Prüfender / Lehrender (zur Berechtigungsvergabe im Modul selbst)
8	Login-Name	Genutzt für Authentifizierung und Autorisierung
9	Telefonnummer (TUBAF)	Rückkanal für Dezernat 2

6.4 Administration

Das POS-System wird durch einen speziellen Administrationszugang verwaltet. Die verantwortliche Administratorin ist im Rechenzentrum klar benannt. Darüber hinaus gibt es noch eine inhaltliche Administratorin im Dezernat 2. Die Mitarbeiter, die mit der (detaillierten) inhaltlichen Pflege des Systems betraut worden sind, erhalten spezielle, nur ihre Prüfungsleistungen betreffende Berechtigungen.

6.5 Datenschutz

Die Aufrechterhaltung des Datenschutzes ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (die Administratoren) und durch Abschirmung von unberechtigtem Zugriff nach außen (sowohl gegen das campusinterne Netz als auch gegen das Internet) gewährleistet. Im Falle der Prüfungsergebnisse ist eine Veröffentlichung der Daten im Selbstbedienungsportal und in den Universitätsaushängen Teil des Soll-Prozesses. Für das System wurde 2006 ein Verfahrensverzeichnis eingereicht, welches 2011 erneuert wurde.

6.6 Art der Datenweitergabe und –verwendung

Der HIS-POS Treiber liefert Prüferdaten aus dem IDMS in das POS System. Es werden keine Informationen aus POS nach IDMS übertragen.

7 Zutrittskontrollsystem Siemens Siport

7.1 Systembeschreibung

Das Zutrittskontrollsystem der TUBAF wird mittels Siemens Siport realisiert. Der Zutritt selbst erfolgt mittels Chipkarte, welche von der Leitzentrale / Siemens eine eigene Applikation für diesen Zweck implementiert bekommt.

7.2 Ziele

Mit der Anbindung des Zutrittskontrollsystems an das IMDS werden bestehende Prozesse beschleunigt und die Datenqualität im Siport-System erhöht. Der Datenqualität, vor allem die der Vertragslaufzeiten der Mitarbeiter ist bei einem Zutrittskontrollsystem besondere Beachtung zu schenken, da nicht übermittelte Informationen im Zweifelsfall dazu führen, dass nicht (mehr) Zutrittsberechtigte Gebäude der TUBAF betreten können.

7.3 Benötigte Daten

Folgende Daten werden aus dem Identity Management System im Zutrittskontrollsystem benötigt. Die übergebenen Daten entsprechen den Festlegungen der zum System gehörenden Dienstvereinbarung über die Nutzung des Elektronischen Schließ- und Zugangskontrollsystems (SIPORT).

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	Dient der Identifikation
2	Vorname	Siehe 1.
3	Namenszusätze	Siehe 1.
4	Personalnummer	Eindeutige Kennung Mitarbeiter
5	Matrikelnummer	Eindeutige Kennung Studenten
6	Vertragsbeginn	Zur Festlegung von Zutrittsfristen
7	Vertragsende	Siehe 6.
8	Kartennummer	Enthält die Seriennummer der Chipkarte (Mitarbeiter- und Studierendenausweis), welche für die Kommunikation zwischen Siport und den On- und Offlinezylindern des Schließsystems benötigt werden

7.4 Administration

Das System wird von fest definierten Mitarbeitern der Leitzentrale der TUBAF betreut. Nur diese haben Zugriffsberechtigungen auf das passwortgeschützte System.

7.5 Datenschutz

Die Aufrechterhaltung des Datenschutzes im Zutrittskontrollsystem ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (die Administratoren) und durch Abschirmung von unberechtigtem Zugriff nach außen (sowohl gegen das campusinterne Netz als auch gegen das Internet) gewährleistet. Keinesfalls erfolgt eine Veröffentlichung der Daten.

7.6 Art der Datenweitergabe und –verwendung

Der Datenfluss ist unidirektional vom IDMS zum Siport-System. Es werden über verschlüsselte Kanäle CSV-Dateien übergeben, welche im Siport-System (teil-) automatisiert weiterverarbeitet werden. Es besteht keine direkte Anbindung der Siport-Datenbank an das IDMS.

8 Zeiterfassung – CTI Leancom Time

8.1 Systembeschreibung

Das Zeiterfassungssystem der TUBAF wird mittels dem Softwareprodukt CTI Leancom Time realisiert. Es dient der Anwesenheitskontrolle einer definierten Gruppe von Mitarbeitern.

8.2 Ziele

Mit der Anbindung des Zeiterfassungssystems an das IMDS werden bestehende Prozesse beschleunigt und die Datenqualität im CTI-Leancom-System erhöht.

8.3 Benötigte Daten

Folgende Daten werden aus dem Identity Management System im Zutrittskontrollsystem benötigt. Die Daten orientieren sich an der bestehenden Dienstvereinbarung über die gleitende Arbeitszeit und wurden um die Vertragslaufzeiten und die Abteilung ergänzt. Die Vertragslaufzeiten sollen die Bereinigung der Datenbank bekräftigen. Die Abteilung wird übergeben, um die Zuordnung zum richtigen Mandanten (Teilbereiche in der Datenbank) zu ermöglichen.

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Namenszusätze	Siehe 1.
4	Personalnummer	Eindeutige Kennung Mitarbeiter
5	Vertragsbeginn	Zur Festlegung von Fristen, Bereinigung Datenbank
6	Vertragsende	Siehe 5.
7	Abteilung / Organisationszugehörigkeit	Zuordnung zum richtigen Mandaten, Sicherstellung, dass Zeiterfassung für Mitarbeiter geltend
8	Kartennummer	Enthält die Seriennummer der Chipkarte (Mitarbeiterausweis), welche für die Kommunikation zwischen dem Server und den (4) Terminals des Zeiterfassungssystems benötigt wird.

8.4 Administration

Das Zeiterfassungssystem wird von einer Mitarbeiterin des Rechenzentrums administriert. Die inhaltliche Pflege wird von je einer Mitarbeiterin des Personaldezernates und der Universitätsbibliothek vorgenommen. Für Abwesenheit einer

der Mitarbeiter wurden Vertreter im Personaldezernat und der Bibliothek definiert. Nur diese Personen haben Zugriffsrechte auf das passwortgeschützte System.

8.5 Datenschutz

Die Aufrechterhaltung des Datenschutzes im Zeiterfassungssystem ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (die Administratoren) und durch Abschirmung von unberechtigtem Zugriff nach außen (sowohl gegen das campusinterne Netz als auch gegen das Internet) gewährleistet. Für das Zeiterfassungssystem wurde 2006 ein Verfahrensverzeichnis erstellt.

8.6 Art der Datenweitergabe und –verwendung

Der Datenfluss ist unidirektional vom IDMS zum Zeiterfassungssystem. Es werden über verschlüsselte Kanäle CSV-Dateien übergeben, welche im Zeiterfassungssystem manuell weiterverarbeitet werden. Es besteht mangels Schnittstellen auf Seiten CTI Leancom Time keine direkte Anbindung zwischen IDMS und der Datenbank des Zeiterfassungssystems.

9 HIS-SOS – Studierendenverwaltung

9.1 Systembeschreibung

Das HIS-SOS-Modul dient der Studierendenverwaltung an der TUBAF. Mittels des Modules werden die Stammdaten der Studierenden gehalten und aktualisiert. Darüber hinaus wird der Rückmeldungsprozess abgebildet.

9.2 Ziele / Benötigte Daten

Die Anbindung des SOS-Modules an das IDMS erfolgt bidirektional. Hin zum IDMS werden die Stammdaten jedes Studierenden übermittelt, die entsprechenden Attribute sind in der Anlage 1 der Dienstvereinbarung zu finden. Das IDMS beliefert das SOS Modul lediglich mit den E-Mail-Adressen und dem Login-Namen aller Studierenden. Die Emailadresse wird übermittelt, um den Verwaltungsmitarbeitern die TUBAF-Kontaktadresse zur Verfügung zu stellen. Der Login-Name wird übergeben, um den Studierenden eine Authentifizierung und Autorisierung am Selbstbedienungsportal mit dem Universitäts-Passwort zu ermöglichen. In dem Selbstbedienungsportal kann die Rückmeldung und die Prüfungsverwaltung durch die Studierenden vorgenommen werden.

Nr.	Datenfeld	Kurzbeschreibung
1	E-Mail-Adresse(n) TU-BAF	Enthält die studentische Mailadresse des Studierenden
2	Login-Name	Benutzer-Name zur Authentifizierung/ Autorisierung

9.3 Administration

Das SOS-Modul wird von einer Mitarbeiterin des Rechenzentrums betreut. Nur diese Administratorin und deren Benannter Vertreter haben den Vollzugriff auf das System. Die inhaltliche Pflege des Systems wird von definierten Mitarbeitern des Dezernates 2 übernommen, die Berechtigungen werden feingranular entsprechend der Arbeitsaufgaben von der Administratorin vergeben.

9.4 Datenschutz

Die Aufrechterhaltung des Datenschutzes ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (die Administratoren) und durch Abschirmung von unberechtigtem Zugriff nach außen (sowohl gegen das campus-

interne Netz als auch gegen das Internet) gewährleistet. Es erfolgt keine Veröffentlichung der Daten. Für das System wurde 2006 ein Verfahrensverzeichnis eingereicht, welches 2011 erneuert wurde.

9.5 Art der Datenweitergabe und –verwendung

Wie in 9.2 beschrieben wird das SOS-System bidirektional angebunden. In beiden Richtungen wird zur automatisierten Datenübergabe ein Datenbank-Treiber über verschlüsselte Transportwege implementiert. Hierzu werden auf Seite HIS-SOS Transfertabellen (Intermediate-Tabellen) für die Datenübermittlung eingerichtet. Datenänderungen in HIS-SOS werden durch HIS-SOS bzw. das IDMS (nur für E-Mail-Adresse und Login-Name) in die Intermediate-Tabellen eingetragen. Über DB-Trigger wird der Datenbank-Treiber vom IDMS angesprochen, welches wiederum die Daten aus den Transfertabellen übernimmt und verarbeitet.

10 HIS-SVA – Personalverwaltung

10.1 Systembeschreibung

Das HIS-SVA-Modul dient der Mitarbeiterverwaltung an der TUBAF. Mittels des Modules werden die Stammdaten der Mitarbeiter gehalten und aktualisiert. Über das Modul erfolgen die Eingruppierung und die Steuerung der Vergütung der Mitarbeiter.

10.2 Ziele/Benötigte Daten

Die Anbindung des SVA-Modules an das IDMS erfolgt bidirektional. Hin zum IDMS werden die Stammdaten jedes Mitarbeiters übermittelt, die entsprechenden Attribute sind in der Anlage 1 der Dienstvereinbarung zu finden. Das IDMS beliefert das SVA-Modul lediglich mit den E-Mail-Adresse und den dienstlichen Telefonnummern aller Mitarbeiter. Diese werden übermittelt, um den Mitarbeitern des Personaldezernates die TUBAF-Kontaktadresse zur Verfügung zu stellen.

Nr.	Datenfeld	Kurzbeschreibung
1	E-Mail-Adresse(n)	Dienstliche E-Mail-Adresse(n)
2	Telefonnummer (dienstl.)	Dienstliche Telefonnummer

10.3 Administration

Das SVA-Modul wird von einer Mitarbeiterin des Rechenzentrums betreut. Nur diese Administratorin und deren benannter Vertreter haben den Vollzugriff auf das System. Die inhaltliche Pflege des Systems wird von definierten Mitarbeitern des Dezernates 3 übernommen, die Berechtigungen werden feingranular entsprechend der Arbeitsaufgaben von der Administratorin vergeben.

10.4 Datenschutz

Die Aufrechterhaltung des Datenschutzes ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (die Administratoren) und durch Abschirmung von unberechtigtem Zugriff nach außen (sowohl gegen das campusinterne Netz als auch gegen das Internet) gewährleistet. Es erfolgt keine Veröffentlichung der Daten.

10.5 Art der Datenweitergabe und –verwendung

Wie in 10.2 beschrieben wird das SVA-System bidirektional angebunden. In beiden Richtungen wird zur automatisierten Datenübergabe ein Datenbank-Treiber über verschlüsselte Transportwege implementiert.

11 User Application (UA)

11.1 Systembeschreibung

Die am Corporate Design der TUBAF ausgerichtete Nutzeroberfläche soll den im IDMS verwalteten Personen die Möglichkeit der Selbstverwaltung von (einigen wenigen) eigenen Nutzerdaten bieten. Weiterhin werden den explizit als Administrator ausgewiesenen Mitarbeitern administrative Funktionalitäten bereitgestellt. Dies umfasst:

- **Datenselbstauskunft und -verwaltung (alle Personen)**
- Benutzerkonto aktivieren (alle Personen)
- Informationen für die Hotline bereitstellen (administrativ)
- Einrichten und Verwalten von Gastkonten (alle Mitarbeiter)
- Einrichten eines externen Bibliotheksnutzers (Bibliotheksmitarbeiter)
- **Telefonbuchfunktion (alle Personen)**
- Verwaltung und Pflege von Telefonnummern (administrativ)
- **Verwaltung von Kostenstellen** (administrativ)
- **Kartenmanagement** (administrativ)

Abläufe, bei denen die User Application „zielsystemartig“ genutzt wird, sind **fett** gedruckt. Die Verwaltung und Pflege von Telefonnummern ist in Abschnitt 12 noch einmal detaillierter beschrieben. Nicht fett gedruckte Abläufe sind „quellsystemartig“ und werden hier nicht näher betrachtet. Es ist zu vermerken, dass in der User Application keine weitere Datenbasis aufgebaut wird, sondern lediglich streng definierter Einblick in Teile der Datenbank des IDMS gegeben wird.

11.2 Ziele

Die User Application ist ein integrierter Teil des IDMS und dient der Abbildung der unter 11.1 beschriebenen Abläufe. Dafür werden teilweise Daten bezogen, die originär aus einem der Quellsysteme kommen, allerdings ohne diese noch einmal zu speichern. Diese sind im Abschnitt 11.3 dargestellt

11.3 Benötigte Daten

11.3.1 Selbstauskunft

Hier erhalten die Benutzer Auskunft über die im System gespeicherten Daten ihrer Person.

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	-
2	Vorname(n)	-
3	Namenszusätze	-
4	Geburtsdatum	-
5	Geburtsname	Optional
6	Geburtsort	Optional
7	Private Anschrift	Nur Studierende und Externe Bibliothek
8	Matrikelnummer	-
9	Personalnummer	-
10	Status	Immatrikuliert, beurlaubt, usw.
11	Fakultät	Nur Studierende
12	Abteilung/Organisationszugehörigkeit	Nur Mitarbeiter
13	E-Mail-Adresse(n) (TU-BAF)	-
14	Aktivierungsdatum	Datum, an welchen der Account freigeschalten wurde
15	Vertragsende	Datum Ende des letzten dem IDM bekannten Vertrages
16	Datum der letzte Aktualisierung der vorgenannten Daten	-
17	Titel	-
18	Geschlecht	-
19	Studiengang	-
20	Studiengang – Bezeichnung	-
21	Hörerstatus	Nur Studierende
22	Studienart	Nur Studierende
23	Fachsemester	Nur Studierende
24	Abschluss	Nur Studierende
25	Login-Name	-
26	Bibliotheksnummer	-
27	Vertiefung	Nur Studierende
28	Kostenstelle	Nur Mitarbeiter
29	Kostenstelle - Bezeichnung	Nur Mitarbeiter
30	Aktuelles Semester	Nur Studierende
31	Nächstes Semester	Nur Studierende

32	Vertragsnummer	Nur Mitarbeiter

11.3.2 **Telefonbuchfunktion**

Diese Funktion ermöglicht es Mitarbeitern und Studierenden innerhalb des IDMS-Verzeichnisdienstes nach Mitarbeitern zu suchen. Als Suchkriterien stehen dabei zur folgende Attribute zur Auswahl, ebendiese Attribute werden auch als Ergebnis der Suche angezeigt:

Nr.	**Datenfeld**	**Kurzbeschreibung**
1	Nachname	Suchfunktion im Verzeichnis
2	Vorname(n)	Siehe 1.
3	Telefonnummer	Siehe 1.
4	Bereich (Vorauswahl)	Siehe 1.

11.3.3 **Verwaltung von Kostenstellen**

Dieser Ablauf wird durch den HIS-COB Treiber (Quellsystemtreiber) angestoßen, sobald eine neue Kostenstelle im COB-System angelegt wird. Die Mitarbeiterin, welche für die Verwaltung der Kostenstellen verantwortlich ist, erhält die Möglichkeit, die Eingaben im COB-System mit organisatorischen Daten anzureichern. Dies sind im Wesentlichen die Festlegung der Kostenstellenverantwortlichen, die Hinterlegung von Gültigkeitszeiträumen und die Zuordnung des Bereiches der Kostenstelle. Die angereicherten Daten stehen dann berechtigten Mitarbeitern zur Information und Kommunikation zur Verfügung. Für die Funktion werden folgende Daten aus dem Identity Management System bezogen:

Nr.	Datenfeld	Kurzbeschreibung
1	Kostenstelle	Nummer (Originär HIS-COB)
2	Kostenstelle - Bezeichnung	Text (Originär HIS-COB)
3	Übergeordnete Kostenstelle	Nummer (Originär HIS-COB)
4	Kostenstelle Bezeichung Langform	Ausführlicher Text ohne Abkürzungen (Originär HIS-COB)
5	Name	Suche über alle Mitarbeiter möglich (nur für die Administratoren)
6	Vorname	Siehe 5.
7	Login-Name	Siehe 5.
8	Bereich / Mail-Subdomain	Suche über alle Bereiche möglich – Die Bereiche fassen mehrere Kostenstellen zusammen. Es ist möglich, dass eine neue Kostenstelle die Erstanlage eines neuen Bereiches zur Folge hat.

11.3.4 **Kartenmanagement**

Dieser Funktion ermöglicht das Initiieren der Prozesse Kartenverlust und –defekt. Beide Prozesse werden in einem definierten Ablauf initiiert. Dafür steht ein Auswahlmenü zur Verfügung, welche die Auswahl von Verlust oder Defekt ermöglicht.

Zusätzlich muss die betroffene Person anhand des Vornamens und/oder des Nachnamens ausgewählt werden.

Entsprechend werden dann das Zeiterfassungssystem, das Zutrittskontrollsystem und die Bibliothek über den Verlust bzw. den Defekt informiert und mit der aus dem Kartenmanagementsystem erhaltenen neuen Seriennummer am Nutzerobjekt aktualisiert. Dies hat zur Voraussetzung, dass eine neue Chipkarte produziert wurde.

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	Suchfunktion in der Funktion
2	Vorname	Siehe 1.
3	Kartennummer	Seriennummer der Chipkarte

11.4 Administration

Die User Application wird durch die Administratoren des IDMS betreut. Die inhaltliche Pflege der Funktionen bezieht in einigen Fällen Mitarbeiter anderer zentraler

Einheiten mit ein, welche als Teiladministratoren definiert werden und von den Administratoren klar definierte Zugriffsberechtigungen erhalten.

11.5 Datenschutz

Der User Application liegt ein Berechtigungssystem zugrunde, welches sicherstellt, dass nur berechtigte Personen zugreifen können. Der Zugriff auf die Applikation ist passwortgeschützt. Da die User Application ein Teil des IDMS ist, unterliegt sie derzeit einer gesonderten Prüfung durch den sächs. Datenschutzbeauftragten.

11.6 Art der Datenweitergabe und –verwendung

Wie oben erwähnt wird keine weitere Datenbasis aufgebaut. Die Datenweitergabe für die Funktionen erfolgt ausschließlich über verschlüsselte LDAP-Verbindungen.

12 Telefonie (indirekt)

12.1 Systembeschreibung

An der TUBAF gibt es derzeit mehrere Telefonanlagen, eine analoge Anlage (Siemens) außerdem eine VOIP-Anlage (Siemens) und eine VOIP-Anlage (Cisco). Die Heterogenität der Telefonanlage ist historisch und/oder mit Vorgaben des SMWK zu begründen. Die Anlagen stellen die Telekommunikation der TUBAF sicher.

12.2 Ziele

Ziel in Bezug auf das IDMS ist eine einheitliche Darstellung der Telefonnummern der Mitarbeiter in einem Telefonverzeichnis innerhalb der User Application. Dafür wird der für die Telefonie zuständige Mitarbeiter in einen halb-automatischen Ablauf einbezogen, um an definierter Stelle in der User Application die Telefondaten am Benutzerobjekt nachzupflegen. Der Mitarbeiter wird dafür gesondert periodisch per Mail über Neuzugänge, Bereichswechsel und Abgänge von Mitarbeitern informiert.

12.3 Benötigte Daten

Folgende Datenfelder werden aus dem IDMS benötigt:

Nr.	Datenfeld	Kurzbeschreibung
1	Nachname	Dient der Identifikation
2	Vorname(n)	Siehe 1.
3	Titel	Wird bei Anrufen gemeinsam mit dem Vor- und Nachnamen angezeigt
4	Telefonnummer	Falls in einem anderen Vertrag (Beschäftigungsverhältnis) bereits eine Telefonnummer vergeben wurde, wird diese geliefert
5	Bereichsbezeichnung	Es wird der Bereich angezeigt, für den die Telefonnummer noch fehlt
6	Bereichsbezeichnung (alt)	Bereichsbezeichnung für Bereich mit bereits vergebenen Telefonnummer

12.4 Administration

Sämtliche Telefonanlagen der TUBAF werden von einem definierten Administrator betreut. Nur dieser hat Zugriff auf die passwortgeschützten Systeme. Für krankheitsfälle gibt es einen definierten Vertreter.

12.5 Datenschutz

Die Aufrechterhaltung des Datenschutzes ist durch eine Beschränkung der Sichtbarkeit der Daten auf berechtigte Personen (im Wesentlichen der Administrator). Es erfolgt eine Veröffentlichung der Daten für das Telefonverzeichnis in der User Application und der TUBAF-Website.

12.6 Art der Datenweitergabe und –verwendung

Es gibt keine direkte Verbindung zwischen den Telefonanlagen und dem IDMS. Die Telefonanlagen sind über einen automatisierten Ablauf „angebunden“, der nach Übergabe der Daten in jedem Fall manuelle arbeiten des Administrators beinhaltet. Die für die Bearbeitung notwendigen Daten werden dem Administrator per Mail geschickt.