Anlage

zur

Rahmendienstvereinbarung zu Einführung und Betrieb des Meta Directory mit den daran angeschlossenen Quell- und Zielsystemen

Systembeschreibung und Datenfelder des Meta Directory

Vorbemerkungen

Überblicksweise wird das Meta Directory als Gesamtsystem vorgestellt und die im Meta Directory an den Thüringer Hochschulen benötigten Datenfelder werden beschrieben. Die Einführung und der Betrieb des Meta Directory erfolgt im Rahmen des Projekts „Integrierende Benutzer- und Ressourcenverwaltung an den Thüringer Hochschulen (Codex – Meta Directory)“. Es handelt sich um ein komplexes, thüringenweit koordiniertes Projekt. Diese Anlage reflektiert den aktuellen Arbeitsstand im Projekt „Codex – Meta Directory“ unter Berücksichtigung der Spezifika an den Thüringer Hochschulen und konzentriert sich auf die für den Abschluss der Rahmendienstvereinbarung wesentlichen Aspekte. Für eine tiefer gehende Betrachtung des Projekts „Codex – Meta Directory“ wird auf die Feinspezifikation „Spezifikation Meta Directory Stufe 1 der Hochschulen in Thüringen“ verwiesen.

Inhaltsverzeichnis

1. Systembeschreibung des Meta Directory 2
2. Personenbezogene Datenfelder des Meta Directory und ihre Anwendungen 4
   2.1 Personenbezogene Daten im Überblick 4
   2.2 Daten zur Identifizierung von Personen 7
   2.3 Anwendungsorientierte personenbezogene Daten 8
   2.4 Technisch orientierte Daten 11
3. Grundsätze zum Sicherheitskonzept des Meta Directory 11

1. Systembeschreibung des Meta Directory

Ein Meta Directory ist ein Rahmenwerk, das die Integration unterschiedlicher Verzeichnisse und anderer Informationsressourcen, wie zum Beispiel Datenbanken, gestattet und unterstützt. Die Hauptanwendung für ein Meta Directory liegt heute im Bereich der Verwaltung von digitalen Identitäten und Rollen, dem so genannten *Identitäts- und Rollen-Management*. Eine eindeutige Identifizierung von Personen und die Zuordnung gültiger Rollen sind die notwendigen Voraussetzungen für die sichere Funktion von IT-Diensten, beispielsweise für die autorisierte Benutzung von Portalfunktionalitäten zur rechnergestützten Forschung, Lehre und Verwaltung an den Thüringer Hochschulen. Das Integrationspotential des Meta-Directory-Paradigmas basiert auf folgenden technologischen Aspekten:

- Ein LDAP-konformer Verzeichnisdienst wird für die Abspeicherung der zu integrierenden Daten verwendet. Das internetfähige *Lightweight Directory Access Protocol* (LDAP) hat sich zu einem Standard für die Verwaltung von Benutzern und Ressourcen in den Netzwerkumgebungen entwickelt. Verzeichnisdienste bieten außerdem ein flexibles und leicht erweiterbares Datenmodell.
- Synchronisationsmechanismen auf der Basis sogenannter Konnektoren und Join Engines ermöglichen den Datenimport und –export. Mit Hilfe von Script-Sprachen und programmiertechnischen Erweiterungen in Form von *Application Program Interfaces* (APIs) sind komplexere Regeln und Arbeitsabläufe modellierbar.

Die Abbildung 1 zeigt das Integrationsszenario für die Einführung und Anwendung des Meta Directory an den Thüringer Hochschulen.

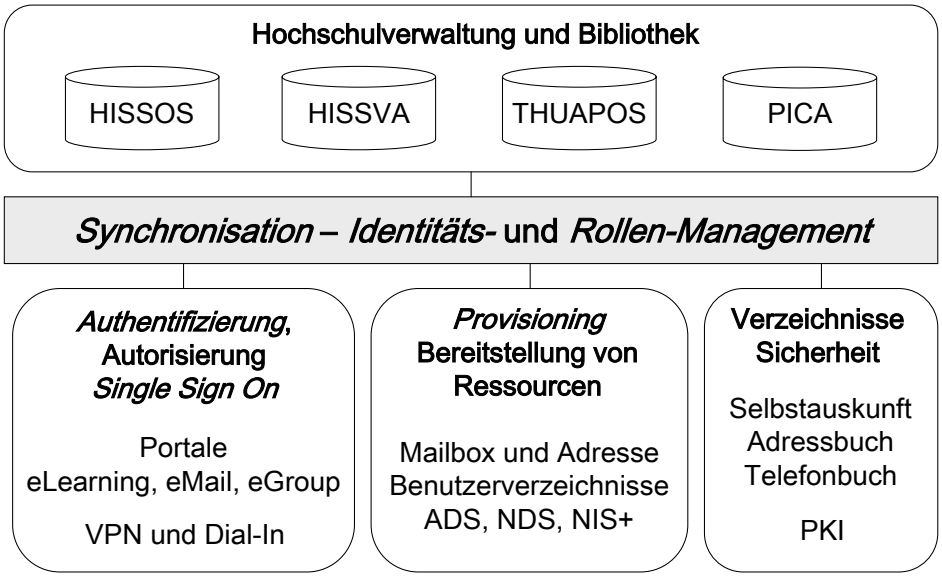

Abbildung 1: Meta-Directory-Szenario an den Thüringer Hochschulen

Die operationellen Datenbanken der Hochschulverwaltung und der Bibliothek sind Datenquellen für das Meta Directory. Über die entsprechenden Synchronisations-mechanismen werden lediglich die für das Identitäts- und Rollenmanagement und die Anwendungen des Meta Directory benötigten Daten übernommen. Dabei steht

HISSVA für die notwendigen Beschäftigtendaten, HISSOS für die notwendigen Studierendendaten und PICA für die notwendigen Daten der Bibliotheksbenutzer. Die zusätzliche Datenbank THUAPOS als Organisationssystem für andere Personen dient der Aufnahme von notwendigen Personendaten, die nicht aus den operationellen Datenbanken gewonnen werden können, wie zum Beispiel für Gäste der Thüringer Hochschulen.

Eine wichtige Anwendung des Meta Directory ist der Bereich der *Authentifizierung* und *Autorisierung*. LDAP-fähige Internetportale ermöglichen eine Anmeldung von Benutzern und die Zuteilung von Rechten mit Hilfe von Verzeichnisdiensten, die ein so genanntes Authentifizierungs- und Autorisierungssystem bilden. Auch die entfernte Einwahl *(Dial-In)* und die Anmeldung im *Virtual Private Network (VPN)* an der jeweiligen Hochschule erfolgt über den Authentifizierungsservice. Das Authentifizierungs- und Autorisierungssystem erhält die notwendigen Benutzerdaten über einen Konnektor vom Meta Directory. Auf der Grundlage dieses integrierten Verfahrens ist eine einheitliche Anmeldung, das sogenannte *Single Sign On*, für Dial-In, VPN und Portalfunktionalitäten realisierbar.

Provisioning an den Thüringer Hochschulen bedeutet, allen Beschäftigten, Studierenden und Bibliotheksbenutzern die für ihre rechnergestützte Arbeit notwendigen Ressourcen zur Verfügung zu stellen. Bisher erfordert das aufwendige Routinetätigkeiten der Benutzeradministration. Die Benutzeradministration umfasst beispielsweise das Einrichten der Mailbox, verbunden mit der Vergabe einer E-Mail-Adresse sowie die Eintragung als Benutzer in den betriebssystemorientierten Verzeichnissen der Rechnerpools, sowohl zentral im Rechenzentrum als auch dezentral in den Fakultäten und Fachgebieten. Die Arbeit der Administratoren erfährt durch Standardkonnektoren des Meta Directory zu den betriebssystemorientierten Verzeichnissen, wie z.B. Microsoft Active Directory Services (ADS) für Windows, Novell Directory Services (NDS) für verschiedene Betriebssysteme oder das Network Information System (NIS+) für Unix, eine wesentliche Unterstützung. Diese betriebssystemorientierten Verzeichnisse übernehmen die Daten aus dem Meta Directory, wobei die Autonomie der dem Meta Directory im Sinne eines Zielsystems nachgeordneten administrativen Bereiche erhalten bleibt. Ein Abgleich der Daten mit dem Meta Directory findet nur bei Bedarf statt.

Das System zur Selbstauskunft gibt allen im Meta Directory verzeichneten Personen die Gelegenheit, die über sie im Meta Directory gespeicherten Daten zu überprüfen. Der Zugriff erfolgt nur aus dem Rechnernetz der jeweiligen Hochschulen lesend ausschließlich auf die eigenen Daten. Die elektronische Selbstauskunft ist eine wichtige Voraussetzung für die informationelle Selbstbestimmung.

Zu den klassischen Aufgaben von Verzeichnisdiensten zählen elektronische *Adress-* und *Telefonbücher*. Im Zusammenhang mit dem E-Mail-System wird die hochschulinterne Abfrage von E-Mail-Adressen angeboten. Ein hochschulinternes elektronisches Telefonbuch setzt aktuelle Daten aus dem Bestand der Telekommunikationsanlage (TK-Anlage) voraus.

Verzeichnisdienste spielen auch eine wichtige Rolle beim Aufbau einer *Public Key Infrastructure (PKI)* für Anwendungen mit erhöhten Sicherheitsbedürfnissen, beispielsweise bei der elektronischen Prüfungsverwaltung. Eine PKI ist die Voraussetzung für den Übergang von der Authentifizierung durch Benutzername/Passwort zur zertifikatsbasierten Anmeldung, für das Signieren von Dokumenten und E-Mails sowie für die Verschlüsselung. Die jeweilige Hochschule benötigt für den Aufbau einer PKI eine vertrauenswürdige Zertifizierungsinstanz, welche die Identität der zu registrierenden Benutzer beglaubigt. Die

organisatorischen Abläufe zur Erstellung und Verwaltung von Zertifikaten können durch das Meta Directory optimiert werden.

Die zahlreichen durch das Meta Directory unterstützten Anwendungen erfordern auch die Abspeicherung personenbezogener Daten im Meta Directory. Die benötigten Datenfelder werden im Folgenden näher erläutert

2. Personenbezogene Datenfelder des Meta Directory und ihre Anwendungen

2.1 Personenbezogene Daten im Überblick

Die Spezifikation der Daten, die im Meta Directory abgespeichert werden müssen, erfolgt in Abhängigkeit von den bereits weiter oben beschriebenen, zu integrierenden Anwendungen. Der hier definierte Datensatz ist thüringenweit einheitlich und stellt einen Konsens dar, der sich aus den unterschiedlichen Prioritäten an den beteiligten Hochschulen ableitet. Die benötigten personenbezogenen Daten lassen sich prinzipiell in drei Kategorien einteilen:

- Daten zur Identifizierung von Personen und zum Aufbau eines hochschulweiten Identity Managements,
- anwendungsorientierte personenbezogene Daten sowie
- technisch orientierte Daten zum Aufbau der verzeichnisinternen Strukturen

Technisch betrachtet werden die Daten auf Verzeichniseinträge für Personen und Rollen abgebildet. Eine Person kann dabei mehrere Rollen besitzen, ein Beschäftigter kann beispielsweise gleichzeitig als Student eingeschrieben und Bibliotheksbenutzer sein. Rollen dienen der Abbildung komplexerer Zusammenhänge, wie zum Beispiel der Vergabe von Rechten entsprechend der organisatorischen Zugehörigkeit. Ein weiteres technisches Detail ist die Verwendung von Assoziationen. Eine Objekt-Assoziation stellt eine eindeutige Referenz zwischen einem Eintrag im Meta Directory und dem Objekt in der angeschlossenen Datenbank her. Die Assoziation ist ein verzeichnisinternes Attribut, das nicht ausgelesen wird.

Die Tabelle 1 gibt zunächst einen Überblick über die zur Zeit im Meta Directory der Thüringer Hochschulen vorhandenen Daten.

Lfd. Nr.	Datenfeld	Kurzbeschreibung
1.	Familienname	Identifizierung von Personen und Generierung von Basisdaten, z.B. Mailadresse, Loginname
2.	Vornamen	Siehe 1.
3.	Namenszusätze	Siehe 1.
4.	Geburtsdatum	Eindeutige Identifizierung von Personen beim Auftreten von Namenskonflikten
5.	HISSVA-interne Personalnummer	Eindeutige Abbildung von Personeneinträgen zwischen Meta Directory und HISSVA
6.	Matrikelnummer	Eindeutige Abbildung von Personeneinträgen zwischen Meta Directory und HISSOS

7.	PICA-interner Bibliotheksbenutzerbarcode	Eindeutige Abbildung von Personeneinträgen zwischen Meta Directory und PICA; nur zur Assoziation verwendet
8.	Identifikator	Abstrakter, anwendungsunabhängiger Identifikator für Personen innerhalb des Meta Directory
9.	Benutzername	Login-Name einer Person für die Benutzung von IT-Diensten der Hochschule
10.	Passwort	Initiales Passwort zur Synchronisation mit anderen Verzeichnissen als Voraussetzung für Single Sign On
11.	E-Mail-Adresse	Generierung einer E-Mail-Adresse für die Benutzer der IT-Dienste der Hochschule
12.	Bibliotheksbenutzernummer	Bibliotheksbenutzerbarcodenummer für den Bibliotheksbenutzerausweis zur Abstimmung mit dem Projekt thoska
13.	Anrede	Repräsentation des Geschlechts einer Person für eine korrekte Kontaktaufnahme
14.	Akademischer Grad	Korrekter Titel für akademische Anwendungen
15.	Immatrikulationsdatum	Einordnung von Studierenden in matrikelbezogene Verzeichnishierarchien und Generierung von Basisdaten; Berechtigungsvergabe, beispielsweise für Anmeldevorgänge
16.	Straße	Straße zur amtlich gemeldeten Adresse einer Person
17.	Adresszusatz	Adresszusatz zur amtlich gemeldeten Adresse einer Person
18.	Postleitzahl	Postleitzahl zur amtlich gemeldeten Adresse einer Person
19.	Stadt	Stadt zur amtlich gemeldeten Adresse einer Person
20.	Land	Land zur amtlich gemeldeten Adresse einer Person
21.	Name der Organisation (Hochschule)	Festlegung der organisatorischen Zugehörigkeit zu einer Hochschule bei einem Meta Directory für mehrere Hochschulen
22.	Zugehörigkeit	Bildung von Benutzergruppen und Vergabe von Rechten in den IT-Systemen der Hochschule
23.	Primäre Zugehörigkeit	Siehe 22. und Spezifikation der dominierenden Beziehung einer Person zur Hochschule
24.	Personalkategorie	Charakter der Beschäftigung zur Ermittlung der primären Zugehörigkeit bzw. der primären Rolle einer Person an der Hochschule

25.	Strukturzugehörigkeit	Ableitung von Rechten und Vergabe von Ressourcen in den jeweiligen Bereichen; Unterstützung der dezentralen Administration
26.	Kostenstelle	Ableitung der Strukturzugehörigkeit und Unterstützung von abrechnungsbezogenen Anwendungen
27.	Funktion	Funktionen einer Person im Kontext der Hochschule zur Ableitung von Rollen, Rechten und benötigter Ressourcen in den IT-Systemen
28.	Studiengang	Einordnung von Studierenden zur Abbildung auf Verzeichnishierarchien, Benutzergruppen und Mailing-Listen; Berechtigungsvergabe, beispielsweise für Anmeldevorgänge
29.	Fachsemester	Siehe 28.
30.	Angestrebter Abschluss	Siehe 28.
31.	Hörerstatus	Siehe 28.
32.	Telefonnummer	Dienstliche Telefonnummer für ein hochschulinternes elektronisches Telefonbuch und für das Facility Management
33.	Telefaxnummer	Dienstliche Telefaxnummer für ein hochschulinternes elektronisches Telefonbuch und für das Facility Management
34.	Gebäude	Identifizierung des Arbeitsplatzes eines Beschäftigten zur Koordinierung der Ressourcenverwaltung, inklusive des Netzwerkmanagements
35.	Raum	Siehe 34.
36.	Gültigkeitsdatum/Beginn	Beginn der Gültigkeit einer hochschulspezifischen Rolle, wie zum Beispiel „Student“, „Mitarbeiter“ oder „Gast“
37.	Gültigkeitsdatum/Ende	Ablauf der Gültigkeit einer hochschulspezifischen Rolle, wie zum Beispiel „Student“, „Mitarbeiter“ oder „Gast“
38.	Status eines Personeneintrages	Status eines Personeneintrages im Meta Directory für die Abbildung von Bearbeitungszuständen
39.	Referenzen auf die Rollen	Referenzen auf die Rollen einer Person im Meta Directory
40.	Referenz auf die primäre Rolle	Referenz auf die primäre Rolle einer Person im Meta Directory
41.	Rollenidentifikator	Abstrakter anwendungsunabhängiger Identifikator für Rollen innerhalb des Meta Directory
42.	Referenz auf den Rolleninhaber	Referenz auf den Inhaber (Person) einer Rolle im Meta Directory

43.	Rollentyp	Rollentyp, wie zum Beispiel „Mitarbeiter“ oder „Student“
44.	Status eines Rolleneintrages	Status eines Rolleneintrages im Meta Directory für die Abbildung von Bearbeitungszuständen
45.	HISSVA-interner Beschäftigungsidentifikator	Objektassoziation zu den mit HIS vereinbarten Datenstrukturen für Beschäftigte
46.	HISSVA-interner Identifikator für die organisatorische Zugehörigkeit	Objektassoziation zu den mit HIS vereinbarten Datenstrukturen für Beschäftigte
47.	HISSOS-interne Studiengangsnummer	Objektassoziation zu den mit HIS vereinbarten Datenstrukturen für Studierende

Tabelle 1: Überblick zu personenbezogenen Daten im Meta Directory

In den nächsten Abschnitten folgt eine detaillierte Aufstellung der einzelnen Datenfelder mit einer kurzen Beschreibung der Anwendung und des Zwecks sowie der Semantik.

2.2 Daten zur Identifizierung von Personen

Familienname, Vornamen, Namenszusätze

Familienname, Vornamen und Namenszusätze dienen der Identifizierung einer Person beim Eintragen in das Meta Directory, sowie der Generierung von Basisdaten wie E-Mail-Adresse und Login-Name. Die Datenfelder Familienname, Vornamen, Namenszusätze und Geburtsdatum besitzen für die eindeutige Identifizierung einer Person beim Eintragen ihrer Daten in das Meta Directory eine Schlüsselfunktion. Nach erfolgreicher Eintragung stehen die in den Datenbanken HISVA, HISSOS und PICA eindeutigen Schlüssel zur Identifizierung im Meta Directory zur Verfügung.

Geburtsdatum

Das Geburtsdatum dient der eindeutigen Identifizierung einer Person beim Auftreten von Namenskonflikten. So können zum Beispiel die im HISSVA verwalteten Beschäftigten gleichzeitig als Student im HISSOS eingeschrieben sein. In diesem Fall muss überprüft werden, ob es sich um ein und dieselbe Person handelt.

HISSVA-interne Personalnummer

Die Personalnummer identifiziert einen Beschäftigten an der jeweiligen Hochschule eindeutig. Die hier verwendete Personalnummer entspricht nicht der durch die zentrale Gehaltstelle vergebenen Personalnummer. Innerhalb der operationellen Datenbank HISSVA sind Beschäftigte über ihre interne Personalnummer lebenslang eindeutig identifizierbar. Damit können nach der Eintragung im Meta Directory die Einträge des Meta Directory und die Beschäftigtendaten des HISSVA durch eine Assoziation mit der internen Personalnummer eindeutig aufeinander abgebildet werden. Für einige hochschulinterne Arbeitsabläufe ist die interne Personalnummer unverzichtbar, wie zum Beispiel für das Projekt thoska zur Einführung einer multifunktionalen Chipkarte.

Matrikelnummer

Die Studierendennummer, auch als Matrikelnummer bezeichnet, identifiziert einen Studierenden an der Hochschule eindeutig und ist lebenslang gültig. Innerhalb der operationellen Datenbank HISSOS sind Studierende über ihre Matrikelnummer

eindeutig identifizierbar. Damit können nach der Eintragung im Meta Directory die Einträge des Meta Directory und die Studierendendaten des HISSOS eindeutig aufeinander abgebildet werden. Für viele hochschulinterne Arbeitsabläufe ist die Matrikelnummer unverzichtbar, wie zum Beispiel bei Einschreibevorgängen.

PICA-interner Bibliotheksbenutzerbarcode

Innerhalb der operationellen Datenbank PICA sind Benutzer der Universitätsbibliothek über ihren Bibliotheksbenutzerbarcode eindeutig identifizierbar. Der Bibliotheksbenutzerbarcode entspricht nicht der Barcodenummer auf den Leserausweisen. Diese können verloren gehen und die Nummer auf dem „neuen“ Leserausweis des Nutzers würde sich somit ändern. Nach der Übernahme werden die Einträge des Meta Directory und die Benutzerdaten des PICA mit Hilfe des Bibliotheksbenutzerbarcode eindeutig in Form einer Assoziation aufeinander abgebildet.

Identifikator

Der Identifikator dient der eindeutigen Identifizierung einer Person innerhalb des Meta Directory. Da ein Meta Directory viele Anwendungen unterstützen soll, existiert die Notwendigkeit eines abstrakten anwendungsunabhängigen Identifikators. Es wird ein 128 Bit großer Globally Unique Identifier (GUID) verwendet, der beim Eintrag einer Person in das Verzeichnis zu generieren ist.

2.3 Anwendungsorientierte personenbezogene Daten

Benutzername

Der Benutzername spezifiziert den Login-Namen einer Person für die Benutzung von IT-Diensten der Hochschule. Der Benutzername wird beim ersten Eintragen einer Person in das Meta Directory generiert. Bei der Initialisierung des Meta Directory müssen die existierenden Benutzer mit ihren bereits vorhandenen Login-Namen berücksichtigt werden. Der Benutzername wird vom Authentifizierungs- und Autorisierungssystem benötigt und kann auch mit den Benutzerverzeichnissen in den Fakultäten abgeglichen werden.

Passwort

Da sich kein Benutzer direkt am Meta Directory anmelden darf, wird das Passwort lediglich zur Passwortsynchronisation mit anderen Verzeichnissen herangezogen. So kann zum Beispiel ein initiales Passwort generiert und anschließend in die angeschlossenen Applikationen synchronisiert werden. Obwohl sich die Passwortsynchronisation zwischen unterschiedlichen Systemen sehr schwierig gestaltet, ist mit der Zulassung dieses Datenfeldes eine wichtige Voraussetzung für Bestrebungen in Richtung Single Sign On gegeben.

E-Mail-Adresse

Das Datenfeld E-Mail-Adresse enthält die an der Hochschule gültige E-Mail-Adresse eines Benutzers. Die E-Mail-Adresse wird beim ersten Eintragen einer Person generiert. Für bereits existierende E-Mail-Benutzer muss dieser Wert aus dem E-Mail-System der Hochschule übernommen werden. Eine an der Hochschule gültige E-Mail-Adresse ist die Voraussetzung für den Nachrichtenaustausch zur Organisation des Arbeits- und Studienalltags sowie zur Inanspruchnahme der portalgestützten Dienste, wie die elektronische Anmeldung und Prüfungsverwaltung.

Bibliotheksbenutzernummer

Die Bibliotheksbenutzernummer ist für den Barcode auf dem Bibliotheksbenutzerausweis bestimmt. Die Aufnahme in das Meta Directory erlaubt die Abstimmung mit der Ausgabe der Thüringer Hochschul- und Studentenwerkskarte thoska.

Anrede

Die Anrede gibt Auskunft über das Geschlecht einer Person. Es handelt sich dabei um die verzeichnisinterne Repräsentation des Geschlechts.

Akademischer Grad

Ein Datenfeld für akademische Titel bzw. akademische Grade einer Person ist von Seiten der akademischen Anwendungen notwendig. Es gehört zum Recht eines jeden Akademikers, mit dem korrekten Titel angesprochen zu werden.

Immatrikulationsdatum

Das Datenfeld enthält das Immatrikulationsdatum eines Studierenden. Es dient der Einordnung von Studierenden und wird in der Praxis zur Generierung von Basisdaten sowie zur Abbildung auf Verzeichnishierarchien herangezogen. Zum Beispiel werden aus Gründen der Lastverteilung die Studierenden entsprechend ihres Immatrikulationsdatums in Benutzerverzeichnissen verwaltet.

Straße, Adresszusatz, Postleitzahl, Stadt, Land

Die Adresse besteht aus den Feldern Straße, Adresszusatz, Postleitzahl, Stadt und Land. Sie dient der Abspeicherung der amtlich gemeldeten Postadresse einer Person. Die Aufnahme der Adressdaten wurde für den späteren Abgleich zwischen den operationellen Datenbanken gefordert.

Name der Organisation (Hochschule)

Die Festlegung der organisatorischen Zugehörigkeit zu einer Hochschule ist bei einem Meta Directory notwendig, das von mehreren Hochschulen benutzt wird. So besteht zum Beispiel die Notwendigkeit, beim Personalisieren der multifunktionalen Chipkarte thoska die beteiligten Einrichtungen voneinander zu unterscheiden.

Zugehörigkeit und primäre Zugehörigkeit

Die Datenfelder für die Zugehörigkeit bzw. die primäre Zugehörigkeit spezifizieren die Beziehung einer Person zur Hochschule auf oberer Ebene. Die Zugehörigkeit bzw. die primäre Zugehörigkeit ermöglichen eine Kategorisierung von Personen und sind damit die Basis für die Bildung von Benutzergruppen und die Vergabe von Rechten in den Zielsystemen. Mögliche Werte für diese Datenfelder sind zum Beispiel „Mitarbeiter“, „Student“, „Bibliotheksbenutzer“ und „Gast“. Der Wert des Datenfeldes für die primäre Zugehörigkeit sollte sich auch bei den Werten für die Zugehörigkeit wieder finden. Außerdem sind auch die Werte für die Rollentypen aus dem Wertevorrat der Zugehörigkeiten abgeleitet.

Personalkategorie

Die Personalkategorie gibt Auskunft über den Charakter der Beschäftigung zur Ermittlung der primären Zugehörigkeit bzw. der primären Rolle einer Person an der Hochschule. So ist zum Beispiel ein Studierender, der gleichzeitig als Beschäftigter der Personalkategorie wissenschaftliche Hilfskraft tätig ist, primär als „Student“ anzusehen.

Strukturzugehörigkeit

Das Datenfeld für die Strukturzugehörigkeit enthält den Namen einer Organisationseinheit der Hochschule. Aus der Strukturzugehörigkeit sind vor allem Rechte und notwendige Ressourcen in den jeweiligen Organisationseinheiten ableitbar. Es handelt sich dabei um eine wichtige Voraussetzung für die Unterstützung der dezentralen administrativen Bereiche durch das Meta Directory.

Kostenstelle

Das Datenfeld spezifiziert die Kostenstelle bzw. die Kostenstellen, denen ein Beschäftigter zugeordnet ist. Von der Kostenstelle leitet sich die Strukturzugehörigkeit ab und sie wird in einigen Zielsystemen, wie zum Beispiel der Verwaltungssoftware für die TK-Anlage, benötigt.

Funktion

Das Datenfeld enthält Werte für die Funktionen bzw. Positionen einer Person innerhalb des Kontexts der Hochschule. Beispielwerte sind Rektor, Kanzler, Dekan, stellvertretender RZ-Leiter, Administrator usw. Aus diesen Werten lassen sich Rollen, Rechte und benötigte Ressourcen ableiten. So besteht unter anderem die Möglichkeit, in Abhängigkeit von der Funktion Mailing-Listen zu generieren, um beispielsweise alle Administratoren der Hochschule über eine neue Sicherheitslücke und die entsprechenden Gegenmaßnahmen zu informieren.

Studiengang, Fachsemester, angestrebter Abschluss und Hörerstatus

Die Datenfelder für Studiengang, Fachsemester, angestrebter Abschluss und Hörerstatus dienen der Einordnung von Studierenden und ihrer Zuordnung zu den Lehrveranstaltungen. 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 Hörerstatus sind ebenfalls damit verknüpft. Der Hörerstatus erlaubt darüber hinaus auch die Einteilung in Mitglieder und Angehörige. Die Informationen werden mit jeder Einschreibung und Rückmeldung aktualisiert. Damit existiert die Möglichkeit, Studierende auf Verzeichnishierarchien, Benutzergruppen und Mailing-Listen abzubilden, die von Studiengang, Fachsemester, angestrebtem Abschluss und Hörerstatus abhängen.

Telefonnummer und Telefaxnummer

Die Datenfelder enthalten die dienstlichen Telefonnummern und Telefaxnummern, unter denen ein Beschäftigter zu erreichen ist. Für die Synchronisation dieses Attributs ist eine Verbindung zur Datenbank der TK-Anlage notwendig. Die Anwendungen für diese Daten reichen vom hochschulinternen elektronischen Telefonbuch auf wirklich aktuellem Stand bis hin zum Facility Management im Zusammenhang mit der Bereitstellung von Telekommunikationsressourcen.

Gebäude und Raum

Die Datenfelder identifizieren ein Gebäude und einen Raum der Hochschule, der dem Beschäftigten als Arbeitsplatz zugeordnet ist. Die Attribute unterstützen die Koordinierung der Verwaltung von Benutzern und technischen Ressourcen, inklusive dem Netzwerkmanagement.

Gültigkeitsdatum/Beginn, Gültigkeitsdatum/Ende

Die Datenfelder spezifizieren das Datum, an dem die Gültigkeit eines Eintrags für eine Person oder einer hochschulspezifischen Rolle beginnt bzw. abläuft. Gründe hierfür können zum Beispiel der Rückmeldestatus eines Studierenden oder die

Befristung eines Beschäftigten sein. Dieses Datum steuert Prozesse, wie die Änderung der Zugehörigkeit von „Student“ nach „Mitarbeiter“, andere Statusänderungen sowie die Freigabe der an eine Rolle gebundenen Ressourcen.

Status eines Personen- und eines Rolleneintrages

Die Datenfelder für den Status eines Personeneintrages und den Status eines Rolleneintrages im Meta Directory dienen der Abbildung von Bearbeitungszuständen in Abhängigkeit von den jeweiligen Arbeitsabläufen. So kann zum Beispiel das Löschen einer Rolle und der damit verbundenen Ressourcen die vorherige Information des jeweiligen Benutzers per E-Mail erfordern.

2.4 Technisch orientierte Daten

Referenzen auf die Rollen und Referenz auf die primäre Rolle

Die Referenzen stellen den verzeichnisinternen Bezug zwischen dem Eintrag einer Person und den jeweils zugeordneten Rolleneinträgen her. Rolleneinträge werden dabei eindeutig durch ihren Rollenidentifikator identifiziert.

Rollenidentifikator

Der Rollenidentifikator dient der eindeutigen Identifizierung einer Rolle innerhalb des Meta Directory. Es wird ein 128 Bit großer *Globally Unique Identifier* (GUID) verwendet, der beim Eintrag einer Rolle in das Verzeichnis zu generieren ist.

Referenz auf den Rolleninhaber

Jeder Rolleneintrag enthält eine Referenz, die den verzeichnisinternen Bezug zu dem jeweiligen Eintrag der zugeordneten Person, also des Rolleninhabers, herstellt.

Rollentyp

Der Rollentyp erlaubt eine Kategorisierung der personengebundenen Rollen. Die bisher definierten Werte, „Mitarbeiter“, „Student“, „Gast“ und „Bibliotheksbenutzer“ stellen eine Teilmenge des Wertebereiches für die weiter oben bereits definierte Zugehörigkeit dar.

HISSVA-interner Beschäftigungsidentifikator, HISSVA-interner Identifikator für die organisatorische Zugehörigkeit, HISSOS-interne Studiengangsnummer

HISSVA-interner Beschäftigungsidentifikator, HISSVA-interner Identifikator für die organisatorische Zugehörigkeit und HISSOS-interne Studiengangsnummer dienen der technischen Realisierung einer Objektassoziation zwischen dem Meta Directory und den mit der HIS GmbH vereinbarten Datenstrukturen in Form von Staging-Tabellen.

3. Grundsätze zum Sicherheitskonzept des Meta Directory

Das Meta Directory mit sämtlichen darin enthaltenen Daten ist entsprechend der jeweils aktuellen technischen und organisatorischen Möglichkeiten vor Missbrauch, Manipulation, und Ausspähung zu schützen. Dazu ist an den jeweiligen Hochschulen ein Sicherheitskonzept auf Basis der Feinspezifikation „Spezifikation Meta Directory Stufe 1 der Hochschulen in Thüringen“ zu erstellen. Es muss vor Inbetriebnahme des Meta Directory vorliegen und insbesondere folgende Punkte regeln:

- Die Aufgabe des Meta Directory besteht darin, konsolidierte Daten über Konnektoren zur Verfügung zu stellen bzw. zu generieren. Keine Applikation erhält ohne einen Konnektor Zugriff auf das Meta Directory.
- Benutzer haben keinen direkten Zugriff auf das Meta Directory. Benutzer, deren Identitäten im Meta Directory verwaltet werden, können sich nur über

ein Portal am Meta Directory anmelden, um Zugriff auf die der jeweiligen Identität zugeordneten Daten zu erlangen.

- Im Meta Directory werden so genannte funktionsbezogene Benutzer, zum Beispiel für den Zugriff der Konnektoren, verwaltet. Diese funktionsbezogenen Benutzer stellen keine zu verwaltenden Personen im herkömmlichen Sinne dar. Funktionsbezogene Benutzer, wie zum Beispiel admin, hissos, hissva, tka (TK-Anlage), pica, postmaster, hostmaster, greifen lesend und schreibend auf das Meta Directory zu.
- Die Art und Weise des Zugriffs dieser funktionsbezogenen Benutzer ist so zu gestalten, dass die Kommunikationsbeziehungen und der Datenaustausch mit dem Meta Directory auf das erforderliche Mindestmaß eingeschränkt werden. Für die einzelnen Funktionen wird festgelegt, welche Einträge und Attribute der funktionsbezogene Benutzer lesen bzw. schreiben darf. Diese Rechte sind im Sicherheitskonzept zu dokumentieren.
- Die Verbindung zwischen entfernten Konnektoren auf anderen Rechnern und dem Meta Directory wird ausschließlich verschlüsselt hergestellt.
- Der Meta Directory-Server befindet sich in einem dafür vorgesehenen Server-Netz. Dieses Server-Netz sollte durch geeignete Maßnahmen vor unerwünschtem Zugriff aus dem Internet geschützt sein.