Anlage 1

Systembeschreibung und Begriffe, Zugangsattribute, Ansprechpartner des Systembetreibers

1 Systembeschreibung und Begriffe

Systembeschreibung und Felder des Datenschemas sind Bestandteile der Anlage zur Rahmendienstvereinbarung zu Einführung und Betrieb des Meta Directory[1]. An der FH wird davon nicht abgewichen.

Durch ein **Identity Management System (IdM-System)** werden konsistente und aktuelle Personendaten gewährleistet. Besonders vorteilhaft für alle Nutzer ist unter anderem eine Anmeldung mit einheitlichen Zugangsdaten in allen angeschlossenen Systemen.

Das Kernstück des IdM-Systems ist ein zentrales Verzeichnis (**Meta Directory**). Das Meta Directory enthält **digitale Identitäten.** Eine digitale Identität besteht aus den zu einer Person elektronisch gespeicherten Personenmerkmalen (**Personenattribute**) wie zum Beispiel Name, Vorname, Geburtsdatum und Adresse. Personen haben **Rollen**, die das Verhältnis einer Person zur Hochschule darstellen. Hauptrollen sind „Mitarbeiter“ mit Attributen wie beispielsweise Personalnummer und Kostenstelle sowie „Studierende“ mit Attributen wie Studiengang, Matrikelnummer, Fachsemester. Die dazu gehörenden Attribute werden als **Rollenattribute** bezeichnet.

Die Mitarbeiterdaten werden in einer Personal-Datenbank (HIS-SVA) erfasst und gepflegt. Die HIS-SVA-Datenbank bildet damit ein **Quellsystem** für das Meta Directory.

Die Studierenden-Daten werden in einem Studierendendatenverarbeitungssystem (HIS-SOS) erfasst und gepflegt. Die HIS-SOS-Datenbank ist das zweite wichtige Quellsystem für das Meta Directory.

HIS-SVA und HIS-SOS werden an das Meta Directory jeweils über eine Software-Schnittstelle (**Konnektor**) angeschlossen. Über den Konnektor fließen Attribute in das Meta Directory. Alle Änderungen in den Quellsystemen werden automatisch übermittelt, so dass die Daten im MetaDirectory immer aktuell und konsistent sind.

Durch den modularen Aufbau können weitere Quellsysteme für Personen, die über die beiden genannten Datenbanken nicht erfasst werden, angeschlossen werden - beispielsweise für Gäste oder Bibliotheksnutzer.

Innerhalb des Meta Directory werden bei der Anlage einer neuen digitalen Identität zusätzliche Attribute erzeugt: Hochschul-Mailadresse und Hochschul-Account (Benutzerkennung). Sie werden auf ihre Einmaligkeit und Eindeutigkeit geprüft; weiterhin wird ein Erstpasswort gebildet.

[1] Rahmendienstvereinbarung zu Einführung und Betrieb des Meta Directory mit den daran angeschlossenen Quell- und Zielsystemen vom 14.05.2006 in der Fassung der Vereinbarung zwischen dem Thüringer Kultusministerium und dem Hauptpersonalrat beim Thüringer Kultusministerium vom 26.08.2009. Amtsblatt des Thüringer Kultusministeriums Nr. 9/2009, S. 278 ff.

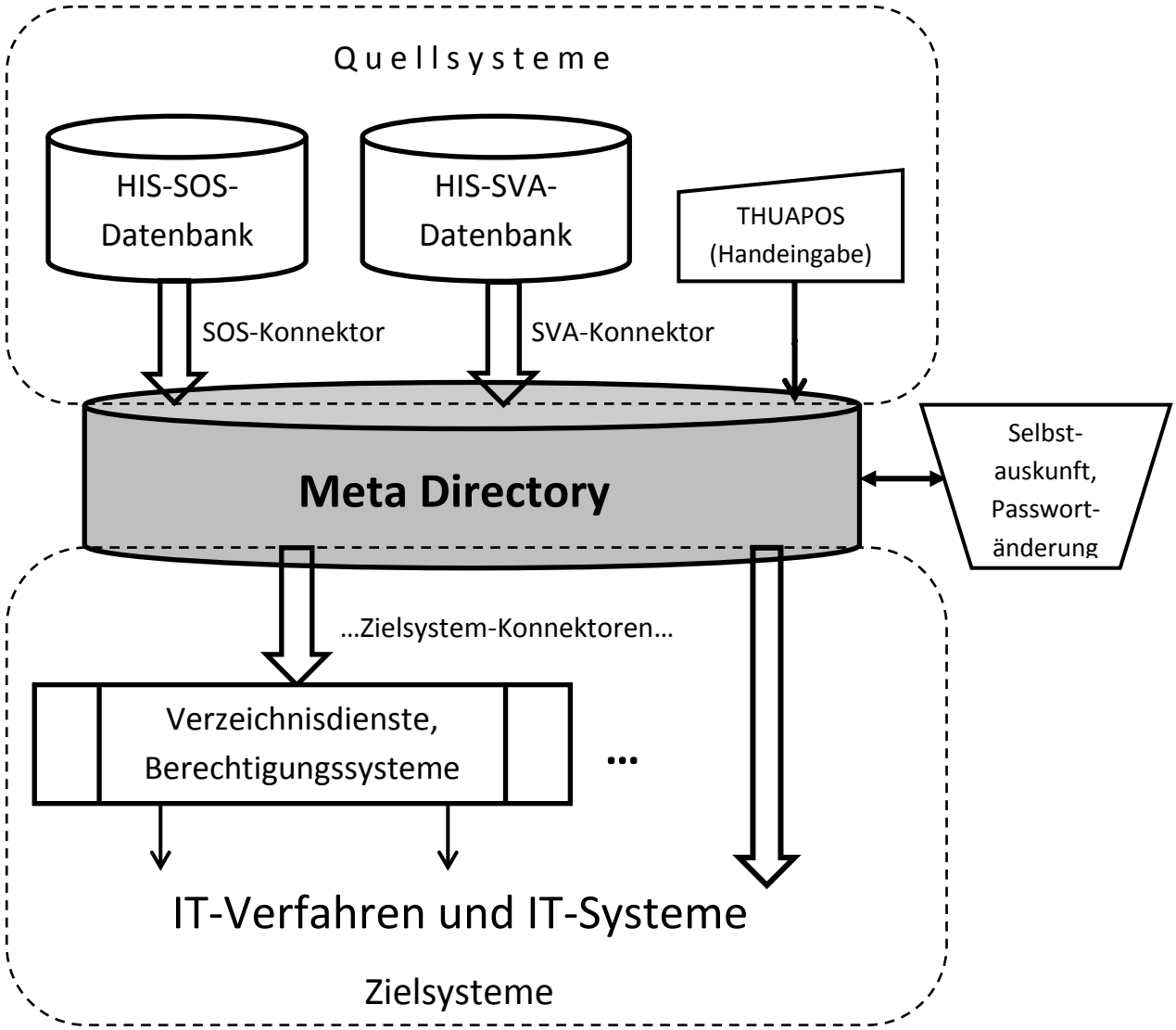
Aus den in das Meta Directory übertragenen Attributen werden Rollen- und Lebenszyklus-Informationen gebildet (Zugehörigkeit, primäre Zugehörigkeit, Rollenreferenzen sowie Status im Lebenszyklus und Status des Personeneintrags).

Auf diesen Bestand an Personen- und Rollenattributen greifen Systeme und Verfahren zu, die bislang eigene, interne Nutzerverzeichnisse besaßen (**Zielsysteme**). Sie werden jeweils über eigene Konnektoren angeschlossen, die sicherstellen, dass nur genau die Daten dorthin fließen, die im Zielsystem tatsächlich gebraucht werden.

Im Meta Directory sind alle digitalen Identitäten in der gleichen Ebene gespeichert. Angeschlossene **Verzeichnisdienste** ordnen die Nutzerinformationen den Organisationsstrukturen und Ressourcen (z.B. Novell eDirectory, Microsoft Active Directory) zu, **Berechtigungssysteme** erteilen die Nutzerberechtigungen.

Über diese Verzeichnisdienste und Berechtigungssysteme werden die vielen einzelnen Nutzerverzeichnisse in den IT-Systemen und IT-Verfahren abgelöst und durch zentrale Mechanismen der Nutzererkennung (**Authentifizierung**) und der Berechtigungsvergabe (**Provisioning**) ersetzt.

Abbildung 1: Grundschema des Identity Management Systems der FH Erfurt



Eine zentrale Kennung (**Hochschul-Account**) mit zugehörigem Passwort ermöglicht künftig den Zugriff auf alle Verfahren und Systeme, für die ein Nutzer berechtigt ist (einmalige Anmeldung: **Single Login**).

2 Zugangsattribute

Sobald eine neue Identität an das Meta Directory übergeben wird, startet dort ein so genannter Value Adder Konnektor, der als Eigenprozess mehrere Personenattribute generiert, die die Person für Zugangsberechtigungen an der Hochschule benötigt:

- **Hochschul-E-Mail-Adresse** mit der Bildungsvorschrift

  erstervorname[.namenszusatz].nachname[.zähler]@fh-erfurt.de

  erstervorname:
  Da Rufnamen nicht hervorgehoben werden, wird der erste in der HIS-Datenbank eingetragene Vorname verwendet.

  namenszusatz
  Wird aufgenommen, falls ein solcher bei der Person existiert.

  nachname:
  Verwendet wird der in der HIS-Datenbank eingetragene Nachname. Nachnamen aus mehreren mit Bindestrich getrennten Teilen werden so komplett übernommen. Mehrere Nachnamen (ohne Bindestrich dazwischen) werden durch Punkt jeweils getrennt.

  zähler:
  Bei Gleichheit der genannten Merkmale mit einer bereits vorhandenen Mailadresse wird zur Unterscheidung eine fortlaufende Zahl (1…99) angefügt.

- **Hochschul-Account** (Hochschul-Nutzerkennung, Login-Name) mit der Bildungsvorschrift

  vvzahlnn

  vv:
  Die ersten zwei Zeichen des ersten in der HIS-Datenbank eingetragenen Vornamens (Kleinbuchstaben).

  zahl:
  Vierstellige Zufallszahl

  nn:
  Die ersten zwei Zeichen des in der HIS-Datenbank eingetragenen Nachnamens (Kleinbuchstaben).

- **Erstpasswort**

  Achtstellige zufällig gebildete Zeichenkette aus Klein- und Großbuchstaben sowie den Ziffern 0…9.
  Berechtigt zum erst-/einmaligen Zugang zum IdM-System.

3 Ansprechpartner des Systembetreibers des Meta Directory

Das Hochschulrechenzentrum ist der Systembetreiber für das IdM-System. Ansprechpartner für alle technischen und organisatorischen Belange des Meta Directory sind der/die

- Leiter(in) des Hochschulrechenzentrums bzw.
- stellvertretende(r) Leiter(in) des Hochschulrechenzentrums.

Für den Fall, dass beide vorgenannten Ansprechpartner(innen) nicht erreichbar sind, auch der/die

- Systembetreuer(in) webbasierter Dienste,
- Systembetreuer(in) Dienste-Server,
- HIS-Administrator(in).

Anforderungen, Störungsmeldungen usw. können per E-Mail (hrz@fh-erfurt.de), auf Anrufbeantworter (0361 6700-123), per Fax (0361 6700-133) oder telefonisch direkt an die oben genannten Ansprechpartner aufgegeben werden.

Anlage 2

Sicherheitskonzept zum Betrieb des Meta Directory an der FH Erfurt

1 Allgemeines

Ziel des Identity Management Systems an der FH Erfurt ist die Etablierung eines hochschulweiten sowie hochschuleinheitlichen Systems zur Verwaltung digitaler Identitäten und Rollen von Personen (Identity Management, IdM) unter Verwendung eines integrierenden Verzeichnisdienstes (Meta Directory).

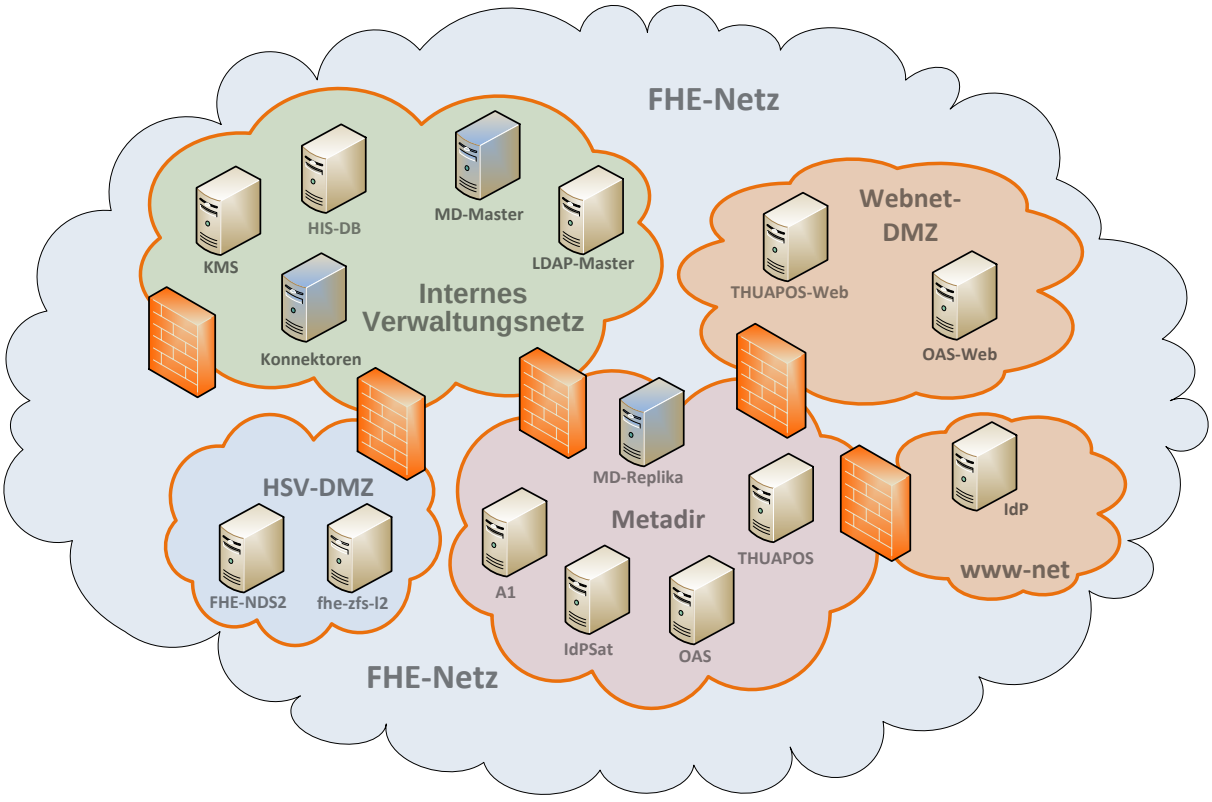
Die Aufgabe des Meta Directory besteht darin, konsolidierte Daten über Konnektoren aus Quellsystemen zu übernehmen und Zielsystemen zur Verfügung zu stellen.

2 Netzarchitektur

Das Hochschulnetz ist über eine Haupt-Firewall vom Wissenschaftsnetz und damit vom Internet abgeschottet. Innerhalb des Hochschulnetzes sind weitere Sicherheitssegmente eingerichtet, die jeweils über eine Firewall abgetrennt sind:

- Internes Verwaltungsnetz
- HSV-DMZ: Demilitarisierte Zone für Server im Umfeld der Hochschulverwaltung (HSV)
- Metadir-Netzsegment für die wesentlichen Meta-Directory-Server
- Webnet-DMZ, www-net: Demilitarisierte Zonen für Webservices

Abbildung 1: Serverzuordnung zu Netzsegmenten



Auf den Servern werden folgende Server-Dienste ausgeführt:

Server	**Server-Dienst**
HIS-DB	HIS-Datenbankserver (HIS-SVA und HIS-SOS)
MD-Master	Meta Directory Master-Server; zentraler Knoten für die Quellsysteme
Konnektoren	Remote-Konnektoren-Server (dort laufen die Konnektoren zu den angeschlossenen Systemen)
LDAP-Master	Mail-/LDAP-Masterserver (siehe Anlage 9)
MD-Replika	Meta Directory Replika-Server (darauf greifen die Konnektoren zu)
A1	A1-Server (siehe Anlage 7)
THUAPOS	THUAPOSlight-Server zur Handeingabe (siehe Anlage 5)
OAS	Daten-/Verzeichnisserver des FHE-Benutzerportals OAS (siehe Anlage 8)
FHE-NDS2	Master-Server des eDirectory-Verzeichnisdienstes (siehe Anlage 6)
fhe-zfs-l2	Server im zentralen Datenspeicherdienst (Fileservice) der Hochschule
OAS-Web	Webserver des FHE-Benutzerportals OAS (siehe Anlage 8)
THUAPOS-Web	Webserver für die THUAPOS-Handeingabe (siehe Anlage 5)
KMS	Datenbank- und Applikationsserver (siehe Anlage 10)
IdPSat	Satellitensystem IdPSat (siehe Anlage 11)
IdP	Identity Provider zur Teilnahme an der DFN-AAI (siehe Anlage 11)

Die HIS-Datenbanken (HIS-SVA, HIS-SOS) werden auf einem Server im internen Verwaltungsnetz betrieben. Dort befinden sich auch der Meta Directory Master Server sowie der Server für die HIS-Konnektoren.

Im separaten Metadir-Netzsegment sind die übrigen IdM-Server untergebracht mit Ausnahme der Webserver für das FHE-Benutzerportal OAS-Web, für die Handeingabe anderer Personen THUAPOS-Web und der IdP zur Authentifizierungsanforderung für Shibboleth, die sich in der Webnet-DMZ bzw. www-net befinden.

Durch diese Servereinordnung in Netz-Substrukturen ist ein hohes Maß an Sicherheit gewährleistet.

Für die Regelwerke der Firewalls gilt generell und grundsätzlich, dass alles verboten ist, was nicht dediziert erlaubt wurde. Somit wird gewährleistet, dass alle nicht-administrativen Zugriffe von außerhalb der geschützten Netzsegmente und DMZ abgewiesen werden.

3 Betriebssicherheit

Sämtliche Dienste innerhalb des IdM-Systems sind entweder auf physischen Servern oder virtuell auf Hostsystemen installiert. Virtuelle Server sind in die Sicherheitsumgebung des VMWare-Hostsystems eingebunden.

Alle Server und Hostsysteme werden im Hochschulrechenzentrum in abgesicherter Umgebung betrieben. Der HRZ-Bereich ist einbruchsgesichert. Der Serverraum verfügt zusätzlich über Fensterkontakte zur Einbruchmeldeanlage. Brand- und Rauchmelder überwachen den gesamten Bereich.

Die Stromversorgung für den HRZ-Bereich ist zweistufig gegen Ausfälle abgesichert (Unterbrechungsfreie Stromversorgung – USV). Kurzzeitausfälle und Schwankungen werden über eine zentrale online-USV ausgeglichen; längere Ausfälle führen zum Zuschalten einer Netzersatzanlage (Diesel-Aggregat).

Die Klimatisierung des Serverraums erfolgt über eine zentrale Kälteanlage mit Umluftkühlern vor Ort. Die Klimatechnik ist in die Unterbrechungsfreie Stromversorgung eingebunden.

4 Zugriffsschutz

Benutzer haben keinen direkten Zugriff auf das Meta Directory. Um ihre eigenen Daten einsehen zu können, müssen sie sich am FHE-Benutzerportal OAS anmelden und authentifizieren.

Konnektoren benötigen lesenden und schreibenden Zugriff auf das Meta Directory. Damit dieser gewährleistet werden kann, werden funktionsbezogene Benutzer (keine Personen im herkömmlichen Sinne) mit administrativen Rechten eingerichtet. Sie werden getrennt von den Personen- und Rollenattributen im Container „service.uni“ verwaltet. Ihre Berechtigungen werden über Trustee-Beziehungen zu den jeweiligen Verzeichnisobjekten beschrieben (siehe Anlagen).

Administrativen Zugriff auf das Meta Directory haben nur namentlich festgelegte Systemadministratoren des HRZ.

Der Zugriff beschränkt sich auf folgende Arbeitsfelder:

- Betriebsüberwachung des Gesamtsystems,
- Entwicklungsarbeiten für weiterführende Teilaufgaben,
- Datenkonsolidierung beim Anschluss weiterer Zielsysteme,
- Bereinigung von Fehlerzuständen,
- Problembehebung bei Unstimmigkeiten zur Gewährleistung eindeutiger digitaler Identitäten.

Zugriffe von Anwendungen auf Daten im Meta Directory erfolgen niemals direkt, sondern ausschließlich über einen Konnektor.

Der Meta-Directory-Server (MD-Master) wird kontinuierlich zu einem weiteren im Metadir-Netzsegment stationierten Server repliziert (MD-Replika). Zielsysteme beziehen ihre Attribute ausschließlich über den MD-Replika-Server.

5 Sicherheit und Schutz der Daten

Vertraulichkeit:

Sämtliche Datenaustauschverbindungen zwischen dem Meta Directory und den angeschlossenen Quell- und Zielsystemen funktionieren grundsätzlich über SSL (Secure Socket Layer) – Verschlüsselung. Damit sind die Transportwege abhörsicher.

Zum administrativen Zugriff auf Systeme des Meta Directory und somit auch auf die Datenbestände sind nur wenige Personen berechtigt (entsprechend Anlage 1). Zugriffe werden nur über Authentifizierung mit Datenverschlüsselung zugelassen.

Integrität:

Die Datenaustauschbeziehungen sind eindeutig dokumentiert (Anlagen 3 ff.). Identitäts- und Rollendaten sind im Meta Directory hochschulweit einheitlich, stets aktuell und konsistent. Veränderungen an Daten werden auf nachvollziehbare Weise vorgenommen.

Verfügbarkeit:

Die Sicherung der Daten vor Verlust erfolgt durch technische Maßnahmen wie Replikation von Servern, RAID-Organisation von Festplatten-Speichersystemen, zweistufige Datensicherung (Backup) zunächst auf ein Festplattensystem, später dann in eine Bandbibliothek. Die Sicherungsbänder werden, sofern sie der Bandbibliothek entnommen wurden, in einem anderen Brandabschnitt zutritts- und zugriffgesichert aufbewahrt.
Die Daten sind somit hochverfügbar.

Authentizität:

Die Datenquellen sind eindeutig festgelegt: HIS-SVA-Datenbank, HIS-SOS-Datenbank, THUAPOSlight zur Handeingabe einzelner Personen.

Revisionsfähigkeit:

Jeder Konnektor erzeugt Trace-Dateien auf dem jeweiligen Server, in denen alle Änderungen von Attributen innerhalb des Konnektors zur Analyse im Fehlerfall aufgezeichnet werden. Ist eine Trace-Datei mit Ereignissen gefüllt, wird eine weitere angelegt. Nach der zehnten gefüllten Trace-Datei wird die erste gelöscht und neu angelegt. Damit ist ein zyklisches Löschen gewährleistet. Die Größe der Trace-Dateien ist so festgelegt, dass eine Aufbewahrungsfrist der Daten von etwa zwei Wochen zu erwarten ist. Zugriff auf die Trace-Dateien haben nur die Systemadministratoren des Meta Directory im HRZ.

Transparenz:

Die Datenaustauschbeziehungen und Filtermechanismen in den Konnektoren sind dokumentiert. Damit ist die Transparenz der Verfahren jederzeit gesichert.

6 Regel-Löschfristen

Jede Person besitzt eine Identität und mindestens eine Rolle.

Rolle	Eine Rolle einer Person hat einen Beginn und ein Ende (Lebenszyklus). Die Rolle wird zwei Jahre nach ihrem Ablauf gelöscht.
Identität	Unmittelbar nach dem Löschen der letzten Rolle wird die Identität gelöscht.

Innerhalb des Meta Directory werden spezielle Personenattribute für den Zugang zu Diensten erzeugt (Zugangsattribute):

- E-Mail-Adresse
- Hochschul-Account

Hochschul-Account und E-Mail-Adresse bleiben 90 Tage nach Ablauf der letzten Rolle der Person aktiv.

7 Organisation

Die Bestimmungen der aktuellen Benutzungsordnung des HRZ gelten.

Zutritt zu den HRZ-Räumlichkeiten besteht nur für autorisierte Personen über Schlüssel der HRZ-Schließgruppe bzw. über Transponder für ein elektronisches Schließsystem. Innerhalb des HRZ-Bereiches ist der Serverraum noch einmal separat zutrittsgesichert, so dass dort auch HRZ-Gäste bzw. Besucher im HRZ keinen Zutritt haben.

Alle am Meta Directory beteiligten Mitarbeiter des HRZ sowie die Administratoren der Fakultäten werden regelmäßig über den Stand, die Mechanismen und die Sicherheitsvorkehrungen im IdM-System unterrichtet.

Anlage 3

Datenaustauschbeziehungen des Meta Directory mit dem Quellsystem HIS-SVA zur Personal- und Stellenverwaltung

1 Einordnung des Systems zur Personal- und Stellenverwaltung HIS-SVA in Bezug auf das Meta Directory

HIS-SVA ist eine Datenbankanwendung für die Personal- und Stellenverwaltung, programmiert durch die Hochschul-Informationssysteme-GmbH Hannover (HIS GmbH).

HIS-SVA enthält alle Informationen über die Beschäftigten der Fachhochschule Erfurt und wird als Quellsystem zur Belieferung des Meta Directory mit Identitäts- und Rollendaten verwendet.

2 Datenaustauschbeziehungen zwischen Meta Directory und HIS-SVA

Die Beschreibungen der Datenaustauschbeziehungen in diesem Abschnitt erfolgen aus der Sicht des Meta Directory.

2.1 Datenimport in das Meta Directory – HIS-SVA als Quellsystem

Der Datenaustausch wird technisch über den SVA-Konnektor vollzogen. Über Filtermechanismen ist eingestellt, welche Attribute aus HIS-SVA in das Meta Directory übernommen werden. Der Konnektor bezieht dabei die Daten aus einer programmierbaren Datenbank-Sicht (View), die im Umfeld der HIS-SVA-Datenbank installiert ist. Der Konnektor erzeugt beim Transport einen Rollenidentifikator (CN Common Name).

In Tabelle 1 ist dargestellt, welche SVA-Daten zur Erzeugung einer digitalen Identität als Personenattribute in das Meta Directory übernommen werden. In Klammern sind die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie evtl. abweichende Attributbezeichnungen im örtlichen Meta Directory aufgeführt.

Tabelle 1: Attribute für Personeneinträge im Meta Directory

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenimports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – wie Mailadresse, Benutzerkennung
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – wie Mailadresse, Benutzerkennung
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – z.B. Mailadresse

4. (4)	Geburtsdatum (thuEduDateOfBirth)	- Identifizierung einer Person beim Auftreten von Namenskonflikten
5. (5)	SVA-interne Personalnummer (workforceID)	- Eindeutige Abbildung (Assoziation) von Personeneinträgen zwischen Meta Directory und HISSVA - Benötigtes Attribut für das Rückschreiben von Mailadresse und Benutzerkennung ins HISSVA
6. (13)	Anrede (thuEduSalutation)	- Basis für die Generierung der Anrede zum Zweck einer konkreten Kontaktaufnahme
7. (14)	Akademischer Grad (thuEduAcademicTitle)	- Benötigt für die Benachrichtigung über Mailadresse und Benutzerkennung zur Namensvervollständigung
8. (16)	Straße (thuEduPostalAddress)	- Straße und Hausnummer zur amtlich gemeldeten Adresse
9. (18)	Postleitzahl (thuEduPostalCode)	- Postleitzahl zur amtlich gemeldeten Adresse
10. (19)	Stadt/Ort (thuEduPostalCity)	- Stadt/Wohnort zur amtlich gemeldeten Adresse
11. (20)	Land (thuEduPostalCountry)	- Land zur amtlich gemeldeten Adresse
12. (50)	Titel (thuEduTitle)	- Benötigt für die Benachrichtigung über Mailadresse und Benutzerkennung zur Namensvervollständigung

Tabelle 2 stellt dar, welche Attribute aus dem HIS-SVA zur Kennzeichnung von Rollen in das Meta Directory fließen.

Tabelle 2: Attribute für Rolleneinträge im Meta Directory

Lfd.-Nr.	**Attribut**	**Zweckbestimmung des Datenimports**
1. (24)	Personalkategorie/ Beschäftigungsverhältnis (thuEduJobType)	- Ermittlung der primären Rolle - Zuordnung von Privilegien aus dem Charakter der Beschäftigung
2. (25)	Strukturzugehörigkeit (OU – OrganizationalUnitName)	- Ableitung von Rechten - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
3. (26)	Kostenstelle (thuEduCostAllocation)	- Ableitung der Strukturzugehörigkeit - Ableitung von Rechten - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
4. (36)	Gültigkeitsdatum/Beginn (thuEduStartDate)	- Beginn der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen
5. (37)	Gültigkeitsdatum /Ende (thuEduExpiryDate)	- Ablauf der Gültigkeit der Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen

2.2 Datenexport vom Meta Directory in das HIS-SVA

Die SVA-Datenbankstruktur bietet ein Feld für die E-Mailadresse, nicht jedoch für weitere Zugangs-Attribute. Deshalb wird nur die im Meta Directory erzeugte Hochschul-Mailadresse nach der Erzeugung an das HIS-SVA zurückgeschrieben. Technisch wird dieser Vorgang ebenfalls über den SVA-Konnektor vollzogen (Tabelle 3).

Tabelle 3: Attribut des Exports in HIS-SVA

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (11)	E-Mail-Adresse (Internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. „admin“ besitzt die in Tabelle 4 dargestellten Trustee-Rechte.

Tabelle 4: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Der Zugriff auf den HIS-SVA-Datenbankserver erfolgt über eine SSL-verschlüsselte Verbindung mit einem 2048 Bit großen RSA-Schlüssel. Der Konnektor läuft auf dem Server für Remote-Konnektoren innerhalb des internen Verwaltungsnetzes, in dem sich auch der HIS-Datenbankserver befindet. Der Meta Directory Master Server befindet sich im gleichen Netzsegment.

Anlage 4

Datenaustauschbeziehungen des Meta Directory mit dem Quellsystem HIS-SOS zur Studierendenverwaltung

1 Einordnung des Systems zur Studierendenverwaltung HIS-SOS in Bezug auf das Meta Directory

HIS-SOS ist eine Datenbankanwendung für die Studierendenverwaltung an Hochschulen innerhalb des Campusmanagements, programmiert von der Hochschul-Informations-systeme GmbH Hannover (HIS GmbH).

HIS-SOS enthält alle Informationen über Studierende. Somit stellt es ein Quellsystem zur Belieferung des Meta Directory mit Identitäts- und Rollenattributen dieser Personengruppe dar.

2 Datenaustauschbeziehungen zwischen Meta Directory und HIS-SOS

Die Beschreibungen der Datenaustauschbeziehungen in diesem Abschnitt erfolgen aus der Sicht des Meta Directory.

2.1 Datenimport in das Meta Directory – HIS-SOS als Quellsystem

Der Datenaustausch wird technisch über den SOS-Konnektor durchgeführt. Über Filtermechanismen ist eingestellt, welche Daten aus den HIS-SOS-Tabellen in das Metadirectory als Attribute übernommen werden. Der Konnektor bezieht dabei die Daten über eine programmierbare Datenbank-Sicht (View), die im Umfeld der HIS-SOS-Datenbank installiert ist. Der Konnektor erzeugt beim Transport einen Rollenidentifikator (CN Common Name).

In Tabelle 1 ist dargestellt, welche SOS-Daten zur Erzeugung einer digitalen Identität in das Meta Directory übernommen werden. In Klammern sind die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie abweichende Attributbezeichnungen im lokalen Meta Directory aufgeführt.

Tabelle 1: Attribute für Personeneinträge im Meta Directory

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenimports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – wie Mailadresse, Benutzerkennung
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – wie Mailadresse, Benutzerkennung
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme

		- Generierung von Basisdaten – z.B. Mailadresse
4. (4)	Geburtsdatum (thuEduDateOfBirth)	- Identifizierung einer Person beim Auftreten von Namenskonflikten
5. (6)	Matrikelnummer (thuEduStudentNumber)	- Eindeutige Abbildung (Assoziation) von Personeneinträgen zwischen Meta Directory und HISSOS - Benötigtes Attribut für das Rückschreiben von Mailadresse und Benutzerkennung ins HISSOS
6. (13)	Anrede (thuEduSalutation)	- Basis für die Generierung der Anrede zum Zweck einer konkreten Kontaktaufnahme
7. (14)	Akademischer Grad (thuEduAcademicTitle)	- Benötigt für die Benachrichtigung über Mailadresse und Benutzerkennung zur Namensvervollständigung
8. (15)	Immatrikulationsdatum (thuEduDateOfMatriculation)	- Beginn der Berechtigung zur Ressourcennutzung (eDirectory, E-Mail usw.)
9. (16)	Straße (thuEduPostalAddress)	- Straße und Hausnummer zur amtlich gemeldeten Adresse
10. (17)	Adresszusatz (thuEduPostalAddress-Extension)	- Adresszusatz zur amtlich gemeldeten Adresse
11. (18)	Postleitzahl (thuEduPostalCode)	- Postleitzahl zur amtlich gemeldeten Adresse
12. (19)	Stadt/Ort (thuEduPostalCity)	- Stadt/Wohnort zur amtlich gemeldeten Adresse
13. (20)	Land (thuEduPostalCountry)	- Land zur amtlich gemeldeten Adresse

Tabelle 2 stellt dar, welche Daten aus HIS-SOS zur Kennzeichnung von Rollen in das Meta Directory fließen.

Tabelle 2: Attribute für Rolleneinträge im Meta Directory

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenimports
1. (25)	Strukturzugehörigkeit (OU – OrganisationalUnitName)	- Ableitung von Rechten - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
2. (28)	Studiengang (thuEduCourseOfStudy)	- Einordnung in Listen, Verzeichnisse, Gruppenberechtigungen, Maillisten
3. (29)	Fachsemester (thuEduSemesterOfCourse-Study)	- Einordnung in Listen, Verzeichnisse, Gruppenberechtigungen, Maillisten
4. (30)	Angestrebter Abschluss (thuEduQualification)	- Einordnung in Listen, Verzeichnisse, Gruppenberechtigungen, Maillisten
5. (31)	Hörerstatus (thuEduStudentType)	- Einordnung in Listen, Verzeichnisse, Gruppenberechtigungen; Maillisten
6. (36)	Gültigkeitsdatum/Beginn (thuEduStartDate)	- Beginn der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen

7. (37)	Gültigkeitsdatum /Ende (thuEduExpiryDate)	- Ablauf der Gültigkeit der Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen

2.2 Datenexport vom Meta Directory in das HIS-SOS

Im Meta Directory werden Zugangsattribute (Hochschule-E-Mail-Adresse, Hochschul-Account, Erstpasswort) erzeugt und in die HIS-SOS-Datenbank zurückgeschrieben. Technisch wird dieser Vorgang ebenfalls über den SOS-Konnektor durchgeführt (Tabelle 3).

Tabelle 3: Attribute des Exports in HIS-SOS

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (9)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste (Hochschul-Account) - Zur Benachrichtigung der Person
2. (10)	Passwort (thuEduSimplePassword)	- Generiertes Erstpasswort zur einmaligen Anmeldung. - Zur Benachrichtigung der Person.
3. (11)	E-Mail-Adresse (Internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. „admin“ besitzt die in Tabelle 4 dargestellten Trustee-Rechte.

Tabelle 4: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Der Zugriff auf den HIS-SOS-Datenbankserver erfolgt über eine SSL-verschlüsselte Verbindung mit einem 2048 Bit großen RSA-Schlüssel. Der Konnektor läuft auf dem Server für Remote-Konnektoren innerhalb des internen Verwaltungsnetzes, in dem sich auch der HIS-SOS-Datenbankserver befindet. Der Meta Directory Master Server befindet sich im gleichen Netzsegment.

Anlage 5

Datenaustauschbeziehungen des Meta Directory mit dem Quellsystem THUAPOSlight zur Handeingabe einzelner Personen

1 Einordnung des Handeingabesystems für einzelne Personen THUAPOSlight in Bezug auf das Meta Directory

Das Thüringer Organisationssystem für andere Personen (THUAPOSlight) ist ein Eingabesystem für die Daten einzelner Personen, die nicht über die Quellsysteme HIS-SOS bzw. HIS-SVA in das Meta Directory fließen, aber zeitlich begrenzt Hochschulressourcen nutzen sollen. Diese Personen werden im Folgenden kurz als „einzelne Personen“ bezeichnet.

2 Datenaustauschbeziehungen zwischen Meta Directory und THUAPOSlight

Die Beschreibungen der Datenaustauschbeziehungen in diesem Abschnitt erfolgen aus der Sicht des Meta Directory.

2.1 Datenimport in das Meta Directory – THUAPOSlight als Quellsystem

Die Anwendung THUAPOSligth basiert auf einer PHP-Webapplikation auf einem eigenen Server mit einer internen Datenbank (basierend auf PostGreSQL), in die zunächst die erfassten Identitäts- und Rollenattribute eingetragen werden. Mit Hilfe des THUAPOSL-Konnektors werden die Attribute dann in das Meta Directory übertragen. THUAPOSlight ist ein Quellsystem. Der THUAPOSL-Konnektor erzeugt beim Transport einen Rollenidentifikator (CN CommonName).

In Tabelle 1 ist dargestellt, welche Daten zur Erzeugung einer digitalen Identität aus dem THUAPOSlight in das Meta Directory übertragen werden. In Klammern stehen die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie abweichende Attributbezeichnungen im lokalen Meta Directory.

Tabelle 1: Attribute für Personeneinträge im Meta Directory

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenimports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – z.B.

		Mailadresse
4. (4)	Geburtsdatum (thuEduDateOfBirth)	- Identifizierung einer Person beim Auftreten von Namenskonflikten
5. (13)	Anrede (thuEduSalutation)	- Zur Benachrichtigung der Person
6. (14)	Akademischer Grad (thuEduAcademicTitle)	- Zur Benachrichtigung der Person
7. (16)	Straße (thuEduPostalAddress)	- Straße und Hausnummer zur amtlich gemeldeten Adresse
8. (17)	Adresszusatz (thuEduPostalAddress Extension)	- Zusatz zur amtlich gemeldeten Adresse
9. (18)	Postleitzahl (thuEduPostalCode)	- Postleitzahl zur amtlich gemeldeten Adresse
10. (19)	Stadt/Ort (thuEduPostalCity)	- Stadt/Wohnort zur amtlich gemeldeten Adresse
11. (20)	Land (thuEduPostalCountry)	- Land zur amtlich gemeldeten Adresse
12. (21)	Name der Organisation/Hochschule (O, OrganizationalName)	- Ableitung der organisatorischen Zugehörigkeit zu einer Hochschule
13. (50)	Titel (thuEduTitle)	- Zur Benachrichtigung der Person

Zur Rollendefinition werden weitere Daten aus dem THUAPOSlight in das Meta Directory übergeben (Tabelle 2).

Tabelle 2: Attribute für Rolleneinträge im Meta Directory

Lfd.-Nr.	**Attribut**	**Zweckbestimmung des Datenimports**
1. (24)	Personalkategorie/ Beschäftigungsverhältnis (thuEduJobType)	- Zur Ermittlung der primären Rolle - Zuordnung von Privilegien aus dem Charakter der Tätigkeit
2. (25)	Strukturzugehörigkeit (OU, OrganizationalUnitName)	- Ableitung von Rechten - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
3. (36)	Gültigkeitsdatum/Beginn (thuEduStartDate)	- Beginn der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen
4. (37)	Gültigkeitsdatum/Ende (thuEduExpiryDate)	- Ablauf der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen
5. (42)	Referenz auf den Rolleninhaber (RoleOccupant)	- Referenz innerhalb des Meta Directory
6. (43)	Rollentyp (thuEduRoleType)	- Basis für die Vergabe von Rechten und zur Bildung von Benutzergruppen

2.2 Datenexport vom Meta Directory in das THUAPOSlight

Um den einzelnen Personen, die über THUAPOSlight in das Meta Directory eingegeben wurden, unmittelbar ihre Zugangsdaten zur Verfügung stellen zu können, werden diese nach Erzeugung innerhalb des Meta Directory sofort in das THUAPOSlight zurückgeschrieben.

Gleichzeitig wird dadurch bestätigt, dass die einzelne Person als digitale Identität im Meta Directory eingetragen wurde.

Technisch geschieht das ebenfalls mit Hilfe des THUAPOSL-Konnektors (Tabelle 3).

Tabelle 3: Attribute des Exports in THUAPOSlight

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (9)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste (Hochschul-Account) - Zur Benachrichtigung der Person
2. (10)	Passwort (thuEduSimplePassword)	- Generiertes Erstpasswort zur einmaligen Anmeldung - Zur Benachrichtigung der Person
3. (11)	E-Mail-Adresse (Internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. „admin“ besitzt die in Tabelle 4 dargestellten Trustee-Rechte.

Tabelle 4: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Auf dem THUAPOS-Server wird eine eigene Datenbank (PostGreSQL-Datenbank) zum Zwischenspeichern der eingegebenen Daten bis zur Transaktion in das Meta Directory betrieben. Die Attribute werden nicht direkt zum Meta-Directory-Masterserver übertragen, sondern zu dessen Replik innerhalb des Metadir-Netzsegmentes (MD-Replika). Durch Zeitstempel-Verfahren wird gesichert, dass die Daten innerhalb des Replika-Verbundes konsistent sind. Die Verbindung ist SSL-verschlüsselt mit einem 2048 Bit großen RSA-Schlüssel.

Der THUAPOS-Web-Server (Webschnittstelle) befindet sich in der Webnet-DMZ. Zum Zugriff auf den THUAPOS-Server innerhalb des Metadir-Netzsegmentes erfolgt eine gesicherte Kommunikation über Firewall-Ports. Die gesicherte Kommunikation zwischen THUAPOS-Server und Meta Directory Replika-Server findet innerhalb des Metadir-Netzsegmentes statt.

4 Anwendung

Die Eingabe einer einzelnen Person im Sinne von Abschnitt 1 dieser Anlage muss formgebunden beantragt werden. Diese Person erklärt auf dem Antrag durch Unterschrift ihr Einverständnis zur Speicherung ihrer personenbezogenen Daten (Tabellen 1 und 2).

Die Genehmigung erteilt der zuständige Dekan oder ein Mitglied des Präsidiums.

Die Dateneingabe über THUAPOSlight erfolgt durch das HRZ. Das HRZ kann weitere Beschäftigte der Hochschule für die Dateneingabe autorisieren und berechtigen.

Anlage 6

Datenaustauschbeziehungen des Meta Directory mit dem Verzeichnisdienst eDirectory als Zielsystem

1 Einordnung des Verzeichnisdienstes eDirectory in Bezug auf das Meta Directory

Der hochschulweite Verzeichnisdienst eDirecory dient der Verknüpfung von Benutzern mit Zugriffen auf bzw. Berechtigungen für Ressourcen und Dienste im Hochschulnetz. eDirectory (früher: NDS) ist ein Produkt der Firma Novell und wird über einen NDS-Masterserver sowie mehrere im Hochschulnetz an verschiedenen Standorten verteilte NDS-Replikaserver zur Verfügung gestellt und stets konsistent und aktuell gehalten.

2 Datenaustauschbeziehungen zwischen Meta Directory und eDirectory

Der Datenaustausch wird über den so genannten Habnet-Konnektor vollzogen.

Bezogen auf das Meta Directory stellt der Verzeichnisdienst eDirectory ein Zielsystem dar. Die Beschreibungen der Datenaustauschbeziehungen in diesem Abschnitt erfolgen aus der Sicht des Meta Directory.

In Tabelle 1 ist dargestellt, welche Daten einer digitalen Identität aus dem Meta Directory in das eDirectory übernommen werden. In Klammern stehen die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie abweichende Attributbezeichnungen im lokalen Meta Directory.

Tabelle 1: Personen-Attribute, die an das eDirectory übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – z.B. Mailadresse
4. (6)	Matrikelnummer (thuEduStudentNumber)	- Eindeutige Abbildung (Assoziation) von Rolleneinträgen zwischen Meta Directory und HISSOS
5. (9)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste (Hochschul-Account) - Zur Benachrichtigung der Person

6. (10)	Passwort	- Passwort für mehrere Dienste
7. (11)	E-Mail-Adresse (Internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person
8. (23)	Primäre Zugehörigkeit (eduPersonPrimaryAffiliation)	- Dominierende Benutzergruppe, zu der die Person gehört - Im Meta Directory selbst gebildetes Attribut
9. (38)	Status eines Personeneintrags (thuEduStatus)	- Abbildung von Bearbeitungszuständen - Im Meta Directory selbst gebildetes Attribut
10. (40)	Referenz auf die primäre Rolle (thuEduPrimaryRoleDN)	- Primäre Rolle einer Person - Im Meta Directory selbst gebildetes Attribut

Zur weiteren Qualifikation der Einträge im eDirectory werden auch Rollendaten aus dem Meta Directory übergeben (Tabelle 2).

Tabelle 2: Rollen-Attribute, die an das eDirectory übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (24)	Personalkategorie (thuEduJobType)	- Charakter der Beschäftigung
2. (25)	Strukturzugehörigkeit (OU, OrganizationalUnitName)	- Ableitung von Rechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
3. (26)	Kostenstelle (thuEduCostAllocation)	- Ableitung von Gruppenrechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
4. (37)	Gültigkeitsdatum/Ende (thuEduExpiryDate)	- Ablauf der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen
5. (43)	Rollentyp (thuEduRoleType)	- Basis für die Vergabe von Rechten und zur Bildung von Benutzergruppen

3 Umsetzung des Sicherheitskonzepts (Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. “admin“ besitzt die in Tabelle 3 dargestellten Trustee-Rechte.

Tabelle 3: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Die Attribute werden nicht direkt vom Meta-Directory-Masterserver übernommen, sondern von dessen Replik innerhalb des Metadir-Netzsegmentes (MD-Replika). Die Verbindung zum NDS-Masterserver erfolgt über SSL-Verschlüsselung mit einem 2048 Bit großen RSA-Schlüssel.

Da sich der NDS-Masterserver in der HSV-DMZ befindet, der MD-Replika-Server jedoch im Metadir-Netzsegment, erfolgt Kommunikation über Firewall-Ports.

Anlage 7

Datenaustauschbeziehungen des Meta Directory mit dem Berechtigungssystem A1 als Zielsystem zur Authentifizierung

1 Einordnung des Authentifizierungssystems A1 in Bezug auf das Meta Directory

Das A1-Authentifizierungssystem hat die Aufgabe, als Berechtigungssystem Nutzer gegenüber verschiedenen weiteren Zielsystemen im Sinne eines Single-Login (einmalige Anmeldung) zu authentifizieren. Dazu stellt der A1-Konnektor die erforderlichen Attribute bereit. Die A1-Authentifizierung soll innerhalb des IdM-Systems bereits in Ansätzen eingeführt werden und später bei Hinzunahme weiterer Zielsysteme entsprechend ausgeweitet werden. Im IdM-System findet eine A1-Authentifizierung bisher für den Administratorzugang zum Handeingabesystem THUAPOSlight statt.

2 Datenaustauschbeziehungen zwischen Meta Directory und Authentifizierungssystem A1

Die Beschreibungen der Datenaustauschbeziehungen in diesem Abschnitt erfolgen aus der Sicht des Meta Directory. Das A1-System stellt ein Zielsystem dar.

In Tabelle 1 ist dargestellt, welche Daten einer digitalen Identität (Personen-Attribute) aus dem Meta Directory zum Authentifizierungssystem A1 übergeben werden. In Klammern stehen die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienst-vereinbarung sowie evtl. abweichende Attributbezeichnungen im lokalen Meta Directory.

Tabelle 1: Personen-Attribute, die an das Authentifizierungssystem A1 übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – z.B. Mailadresse
4. (4)	Geburtsdatum (thuEduDateOfBirth)	- Identifizierung einer Person beim Auftreten von Namenskonflikten
5. (9)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste (Hochschul-Account) - Zur Benachrichtigung der Person
6. (10)	Passwort	- Passwort für mehrere Dienste

7. (11)	E-Mail-Adresse (Internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person
8. (13)	Anrede (thuEduSalutation)	- Basis für die Generierung der Anrede zum Zweck einer konkreten Kontaktaufnahme
9. (14)	Akademischer Grad (thuEduAcademicTitle)	- Benötigt für die Benachrichtigung über Mailadresse und Benutzerkennung zur Namensvervollständigung
10. (21)	Name der Organisation/Hochschule (O, OrganizationalName)	- Ableitung der organisatorischen Zugehörigkeit zu einer Hochschule
11. (22)	Zugehörigkeit (eduPersonAffiliation)	- Zugehörigkeit zu einer Benutzergruppe im Sinne von Gruppenberechtigungen - Im Meta Directory selbst gebildetes Attribut
12. (23)	Primäre Zugehörigkeit (eduPersonPrimaryAffiliation)	- Dominierende Benutzergruppe, zu der die Person gehört - Im Meta Directory selbst gebildetes Attribut
13. (38)	Status eines Personeneintrags (thuEduStatus)	- Abbildung von Bearbeitungszuständen - Im Meta Directory selbst gebildetes Attribut
14. (50)	Titel (thuEduTitle)	- Benötigt für die Benachrichtigung über Mailadresse und Benutzerkennung zur Namensvervollständigung

Neben den Personen-Attributen wird auch ein Rollen-Attribut an das A1 übergeben (Tabelle 2).

Tabelle 2: Rollen-Attribute, die an das A1 übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (41)	Rollenidentifikator (CN, CommonName)	- Rollenbezeichnung innerhalb des Meta Directory (vom Quellsystem-Konnektor erzeugt)

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ fesetgelegt „admin“ besitzt die in Tabelle 3 dargestellten Trustee-Rechte.

Tabelle 3: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Die Verbindung zwischen A1-Server und dem MD-Replikaserver erfolgt über eine SSL-verschlüsselte Verbindung mit einem 2048 Bit großen RSA-Schlüssel. Der Konnektor

läuft auf dem A1-Server innerhalb des Metadir-Netzsegmentes. Da dort auch der MD-Replika-Server untergebracht ist, erfolgt die Kommunikation innerhalb eines Netzsegments.

Anlage 8

Datenaustauschbeziehungen des Meta Directory mit dem FHE-Benutzerportal OAS für Selbstauskunft und Passwortänderung

1 Einordnung des OAS-Systems in Bezug auf das Meta Directory

Das FHE-Benutzerportal OAS (Operatives Auskunft-System) funktioniert über eine Webschnittstelle (OAS-Web) und wird für die Selbstauskunft und Passwortänderungen verwendet. Ausschließlich im Zusammenhang mit der Neueinstellung von Personal wird es zur Auskunft über erforderliche Daten durch ausgewählte weitere Beschäftigte verwendet.

2 Datenaustauschbeziehungen zwischen Meta Directory und OAS

Der Datenaustausch wird über den OAS-Konnektor vollzogen. Bezogen auf das Meta Directory stellt das Operative Auskunftssystem mit seinem Hauptzweck der Selbstauskunft ein Zielsystem dar. Die Beschreibungen der Datenaustauschbeziehungen in diesem Abschnitt erfolgen aus der Sicht des Meta Directory.

In Tabelle 1 ist dargestellt, welche Daten einer digitalen Identität aus dem Meta Directory in das OAS übernommen werden. In Klammern stehen die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie evtl. abweichende Attributbezeichnungen im lokalen Meta Directory.

Tabelle 1: Personen-Attribute, die an das OAS übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – z.B. Mailadresse
4. (4)	Geburtsdatum (thuEduDateOfBirth)	- Identifizierung einer Person beim Auftreten von Namenskonflikten
5. (5)	SVA-interne Personalnummer (workforceID)	- Eindeutige Abbildung (Assoziation) von Rolleneinträgen zwischen Meta Directory und HISSVA
6. (6)	Matrikelnummer (thuEduStudentNumber)	- Eindeutige Abbildung (Assoziation) von Rolleneinträgen zwischen Meta Directory und HIS-SOS

7. (8)	Personenidentifikator (thuEduIdentifier)	- Meta-Directory-interne Identifikation
8. (9)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste (Hochschul-Account) - Zur Benachrichtigung der Person
9. (10)	Passwort (thuEduSimplePassword)	- Generiertes Erstpasswort zur einmaligen Anmeldung - Zur Benachrichtigung der Person
10. (11)	E-Mail-Adresse (internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person
11. (13)	Anrede (thuEduSalutation)	- Basis für die Generierung der Anrede zum Zweck einer konkreten Kontaktaufnahme
12. (14)	Akademischer Grad (thuEduAcademicTitle)	- Benötigt für die Benachrichtigung über Mailadresse und Benutzerkennung zur Namensvervollständigung
13. (15)	Immatrikulationsdatum (thuEduDateOf Matriculation)	- Beginn der Berechtigung zur Ressourcennutzung (eDirectory, E-Mail usw.)
14. (16)	Straße (thuEduPostalAddress)	- Straße und Hausnummer zur amtlich gemeldeten Adresse
15. (17)	Adresszusatz (thuEduPostalAddress Extension)	- Zusatz zur amtlich gemeldeten Adresse
16. (18)	Postleitzahl (thuEduPostalCode)	- Postleitzahl zur amtlich gemeldeten Adresse
17. (19)	Stadt/Ort (thuEduPostalCity)	- Stadt/Wohnort zur amtlich gemeldeten Adresse
18. (20)	Land (thuEduPostalCountry)	- Land zur amtlich gemeldeten Adresse
19. (21)	Name der Organisation/Hochschule (O, OrganizationalName)	- Ableitung der organisatorischen Zugehörigkeit zu einer Hochschule
20. (22)	Zugehörigkeit (eduPersonAffiliation)	- Zugehörigkeit zu einer Benutzergruppe im Sinne von Gruppenberechtigungen - Im Meta Directory selbst gebildetes Attribut
21. (23)	Primäre Zugehörigkeit (eduPersonPrimaryAffiliation)	- Dominierende Benutzergruppe, zu der die Person gehört - Im Meta Directory selbst gebildetes Attribut
22. (38)	Status eines Personeneintrags (thuEduStatus)	- Abbildung von Bearbeitungszuständen - Im Meta Directory selbst gebildetes Attribut
23. (39)	Referenz auf die Rollen (thuEduRoleDN)	- Rollen einer Person im Meta Directory - Im Meta Directory selbst gebildetes Attribut
24. (40)	Referenz auf die primäre Rolle (thuEduPrimaryRoleDN)	- Primäre Rolle einer Person im Meta Directory - Im Meta Directory selbst gebildetes Attribut
25. (41)	Rollenidentifikator (CN, CommonName)	- Rollenbezeichnung innerhalb des Meta Directory (vom Quellsystem-Konnektor erzeugt)
26. (50)	Titel (thuEduTitle)	- Benötigt für die Benachrichtigung über Mailadresse und Benutzerkennung zur Namensvervollständigung

Neben den Personen-Attributen werden auch Rollen-Attribute an das OAS übergeben (Tabelle 2).

Tabelle 2: Rollen-Attribute, die an das OAS übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (24)	Personalkategorie (thuEduJobType)	- Charakter der Beschäftigung
2. (25)	Strukturzugehörigkeit (OU, OrganizationalUnitName)	- Ableitung von Rechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
3. (26)	Kostenstelle (thuEduCostAllocation)	- Ableitung von Gruppenrechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
4. (28)	Studiengang (thuEduCourseOfStudy)	- Ableitung von Gruppenrechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
5. (29)	Fachsemester (thuEduSemesterOfCourse Study)	- Ableitung von Gruppenrechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
6. (30)	Angestrebter Abschluss (thuEduQualification)	- Ableitung von Gruppenrechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
7. (31)	Hörerstatus (thuEduStudentType)	- Ableitung von Gruppenrechten auf lokale Ressourcen im eDirectory - Unterstützung der dezentralen Administration - Aufbau verteilter Verzeichnisstrukturen
8. (36)	Gültigkeitsdatum/Beginn (thuEduStartDate)	- Beginn der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen
9. (37)	Gültigkeitsdatum/Ende (thuEduExpiryDate)	- Ablauf der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen
10. (42)	Rolleninhaber (Role Occupant)	- Referenz auf eine Person im Meta Directory
11. (43)	Rollentyp (thuEduRoleType)	- Basis für die Vergabe von Rechten und zur Bildung von Benutzergruppen
12. (44)	Status eines Rolleneintrags (thuEduStatus)	- Abbildung von Bearbeitungszuständen im Meta Directory - Im Meta Directory selbst gebildetes Attribut

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. „admin“ besitzt die in Tabelle 3 dargestellten Trustee-Rechte.

Zur Administration sowie zur Lösung von Problem- bzw. Konfliktfällen ist ein Administratorzugang mit umfassender Berechtigung unerlässlich. Dieser Zugang wird ausschließlich innerhalb des Hochschulrechenzentrums an ausgewählte Beschäftigte vergeben (siehe Anlage 1).

Tabelle 3: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Die Attribute werden nicht direkt vom Meta-Directory-Masterserver übernommen, sondern von dessen Replik innerhalb des Metadir-Netsegmentes (MD-Replika). Die Verbindung zum OAS-Server erfolgt über SSL-Verschlüsselung mit einem 2048 Bit großen RSA-Schlüssel.

Der OAS-Web-Server (Webschnittstelle) befindet sich in der Webnet-DMZ. Zum Zugriff auf den OAS-Server innerhalb des Metadir-Netzsegmentes erfolgt eine gesicherte Kommunikation über Firewall-Ports. Die gesicherte Kommunikation zwischen OAS-Server und Meta Directory Replika-Server findet innerhalb des Metadir-Netzsegmentes statt.

Der Zugriff auf die OAS-Webschnittstelle erfolgt ausschließlich über HTTPS.

4 Anwendung

4.1 Selbstauskunft

Für die individuelle Selbstauskunft erhält der Benutzer ausschließlich Zugriff auf seine eigenen, im Meta Directory gespeicherten Personen- und Rollenattribute. Dazu meldet er sich am FHE-Benutzerportal OAS an und authentifiziert sich.

4.2 Passwortänderung

Das innerhalb des Meta Directory erzeugte Erstpasswort dient zur erst-/einmaligen Anmeldung am FHE-Benutzerportal (OAS). Dort muss es nach dem ersten Anmelden durch ein selbst gewähltes (Betriebs-)Passwort entsprechend der vorgegebenen Passwortrichtlinie ersetzt werden. Mit dem Ereignis der Passwortänderung ist eine Freischaltung in den Zielsystemen gekoppelt (Mailsystem – Mailbox, eDirectory - Berechtigungen auf Ressourcen, Fileservice – Homedirectory, u.a.)

Eine Änderung des Passworts ist jederzeit über das FHE-Benutzerportal OAS möglich.

Das Passwort wird nicht im Meta Directory gespeichert. Es wird verschlüsselt direkt an die als Zielsysteme angeschlossenen Verzeichnisdienste und Berechtigungssysteme übertragen.

4.3. Auskunftssystem

Der Einsatz als Auskunftssystem erfolgt nur im zuständigen Dezernat für Personalangelegenheiten. Da HIS-SVA nur das Rückschreiben der E-Mail-Adresse erlaubt, die anderen Zugangsattribute aber auch zeitnah zur Verfügung stehen müssen, ist für ausgewählte Mitarbeiter ein erweiterter persönlicher Zugriff als DPR-OAS-Benutzer über das FHE-Benutzerportal OAS notwendig.

Dieser Zugriff beschränkt sich auf Identitäten mit der Rolle der Mitarbeiter im Meta Directory und enthält folgende Attribute, die für eine verlässliche Identifikation der Person benötigt werden:

- Anrede
- Familienname
- Vorname
- Namenszusätze
- akademischer Grad
- Titel
- Geburtsdatum
- SVA-interne Personalnummer
- E-Mail-Adresse,
- Benutzername (Hochschul-Account),
- Erstpasswort.

Arbeitnehmer und Beamte erhalten im Rahmen ihrer Einstellung ihre persönlichen Zugangsattribute ausgehändigt (E-Mail-Adresse, Hochschul-Account, Erstpasswort).

Anlage 9

Datenaustauschbeziehungen des Meta Directory mit dem E-Mail-Berechtigungssystem LDAP als Zielsystem

1 Einordnung des E-Mail-LDAP-Systems in Bezug auf das Meta Directory

LDAP (Lightweight Directory Access Protocol) wird als Zugriffsprotokoll speziell für Mailserver und Mailboxen verwendet. Der LDAP-Dienst ist mit einer Master-Slave-Serveranordnung realisiert. Im LDAP werden sämtliche Mailadressen und Mailnutzerdaten sowie Hinweise auf den jeweils genutzten Maildienst geführt.

2 Datenaustauschbeziehungen zwischen Meta Directory und E-Mail/LDAP-System

Der Datenaustausch wird über den Mail-Konnektor vollzogen. Der Mail-Konnektor übergibt die innerhalb des Meta Directory generierte E-Mail-Adresse mit weiteren Attributen an den E-Mail-LDAP.

Bezogen auf das Meta Directory stellt das E-Mail/LDAP-System somit ein Zielsystem dar. Die Beschreibungen der Datenaustauschbeziehungen in diesem Abschnitt erfolgen aus der Sicht des Meta Directory.

In Tabelle 1 ist dargestellt, welche Daten einer digitalen Identität aus dem Meta Directory in das E-Mail/LDAP-System übernommen werden. In Klammern stehen die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie evtl. abweichende Attributbezeichnungen im lokalen Meta Directory.

Tabelle 1: Personen-Attribute, die an das E-Mail/LDAP-System übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten – z.B. Mailadresse
4. (9)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste (Hochschul-Account) - Zur Benachrichtigung der Person
5. (10)	Passwort	- Passwort für mehrere Dienste

6. (11)	E-Mail-Adresse (Internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person
7. (22)	Zugehörigkeit (eduPersonAffiliation)	- Zugehörigkeit zu einer Benutzergruppe im Sinne von Gruppenberechtigungen - Im Meta Directory selbst gebildetes Attribut
8. (23)	Primäre Zugehörigkeit (eduPersonPrimaryAffiliation)	- Dominierende Benutzergruppe, zu der die Person gehört - Im Meta Directory selbst gebildetes Attribut
9. (38)	Status eines Personeneintrags (thuEduStatus)	- Abbildung von Bearbeitungszuständen - Im Meta Directory selbst gebildetes Attribut
10. (39)	Referenz auf die Rollen (thuEduRoleDN)	- Rollen einer Person im Meta Directory - Im Meta Directory selbst gebildetes Attribut
11. (40)	Referenz auf die primäre Rolle (thuEduPrimaryRoleDN)	- Primäre Rolle einer Person im Meta Directory - Im Meta Directory selbst gebildetes Attribut
12. (41)	Rollenidentifikator (CN, CommonName)	- Rollenbezeichnung innerhalb des Meta Directory (vom Quellsystem-Konnektor erzeugt)

Neben den Personen-Attributen werden auch Rollen-Attribute an das E-Mail/LDAP-System übergeben (Tabelle 2).

Tabelle 2: Rollen-Attribut, das an das E-Mail/LDAP-System übergeben wird

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (37)	Gültigkeitsdatum/Ende (thuEduExpiryDate)	- Ablauf der Gültigkeit einer Rolle - Festlegung des Lebenszyklus und Generierung daraus abzuleitender Verpflichtungen

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. „admin“ besitzt die in Tabelle 3 dargestellten Trustee-Rechte.

Tabelle 3: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Der LDAP-Masterserver ist innerhalb des internen Verwaltungsnetzes angeordnet. Der MD-Replika-Server befindet sich im Metadir-Netzsegment. Die Verbindung erfolgt gesichert über Firewallports über SSL-Verschlüsselung mit einem 2048 Bit großen RSA-Schlüssel.

Anlage 10

Datenaustauschbeziehungen des Meta Directory mit dem Kartenmanagementsystem (thosKMS) als Zielsystem

1 Einordnung des thosKMS in Bezug auf das Meta Directory

Das Kartenmanagementsystem (thosKMS) befindet sich auf dem KMS-Server und dient der Bereitstellung der für die Chipkartenproduktion und -validierung benötigten Daten, der Übertragung der während der Chipkartenproduktion erzeugten Daten (wie z.B. Bibliotheksnummer) in das Meta Directory und der Übersicht produzierter Chipkarten zur Fehler- und Problembehebung. Es beinhaltet einen Applikationsserver und einen PostgreSQL-Datenbankserver. Über einen Konnektor werden die benötigten Daten aus dem Meta Directory in den Applikationsserver übertragen, der diese in einer Zwischenstruktur, der PostgreSQL-Datenbank, speichert. Von dort holt sich das Chipkartenproduktionssystem die Daten für die Chipkartenproduktion (siehe DV Einführung und Betrieb eines Chipkarteninformationssystems). Weiterhin schreibt das Chipkartenproduktionssystem die Bibliotheksnummer zusammen mit weiteren Daten zur produzierten Chipkarte in die Zwischenstruktur des thosKMS zurück. Applikationsserver und Konnektor übertragen die Bibliotheksnummer anschließend in das Meta-Directory.

2 Datenaustauschbeziehungen zwischen Meta Directory und thosKMS

Der Datenaustausch wird über den Konnektor vollzogen. Der Konnektor überträgt die Daten in den Applikationsserver, der für die Speicherung dieser in einer PostgreSQL-Datenbank und das Rückschreiben in das Meta Directory sorgt.

2.1 Datenexport aus dem Meta Directory in das thosKMS

Welche Daten aus den Metadirectory in das thosKMS und damit in die Zwischenstruktur übernommen werden, wird über Filtermechanismen im Konnektor eingestellt.

Die Attribute sind in Tabelle 1 dargestellt. In Klammern stehen die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie evtl. abweichende Attributbezeichnungen im lokalen Meta Directory.

Tabelle 1: Personen-Attribute, die an das thosKMS übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Aufdruck auf Chipkarte
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Aufdruck auf Chipkarte
3. (3)	Namenszusätze (thuEduNameExtension)	- Identifizierung einer Person - Aufdruck auf Chipkarte
4. (4)	Geburtsdatum (thuEduDateOfBirth)	- Identifizierung einer Person beim Auftreten von Namenskonflikten
5. (9)	Anrede (thuEduSalutation)	- Anrede
6. (6)	Akademischer Grad (thuEduAcademicTitle)	- Aufdruck auf Chipkarte

7. (5)	Titel (thuEduTitle)	- Aufdruck auf Chipkarte
8. (13)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste
9. (64)	Identifikator (CN, CommonName)	- Bezeichnung innerhalb des Meta Directory
10. (23)	Status eines Personeneintrags (thuEduStatus)	- Abbildung von Lifecyclezuständen im Meta Directory

Neben den Personen-Attributen werden auch Rollen-Attribute an das thosKMS übergeben (Tabelle 2).

Tabelle 2: Rollen-Attribute, die an das thosKMS übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (75)	Rolleninhaber (Role Occupant)	- Referenz auf eine Person im Meta Directory
2. (29)	Rollentyp (thuEduRoleType)	- Basis für die Vergabe von Rechten und zur Bildung von Benutzergruppen
3. (23)	Status eines Rolleneintrags (thuEduStatus)	- Abbildung von Lifecyclezuständen im Meta Directory
4. (63)	Gültigkeitsdatum/Ende (thuEduExpiryDate)	- Ablauf der Gültigkeit einer Rolle (Lifecycle)
5. (33)	Strukturzugehörigkeit (OU, OrganizationalUnitName)	- Ableitung von Rechten
6. (34)	Kostenstelle (thuEduCostAllocation)	- Ableitung von Rechten
7. (42)	Angestrebter Abschluss (thuEduQualification)	- Ableitung von Gruppenrechten
8. (62)	Gültigkeitsdatum/Beginn (thuEduStartDate)	- Beginn der Gültigkeit einer Rolle (Lifecycle)
9. (32)	Name der Organisation/Hochschule (O, OrganizationalName)	- Ableitung der organisatorischen Zugehörigkeit zu einer Hochschule
10. (64)	Identifikator (CN, CommonName)	- Bezeichnung innerhalb des Meta Directory (vom Quellsystem-Konnektor erzeugt)

2.2 Datenimport in das Meta Directory – thosKMS als Quellsystem

Im Chipkartenproduktionssystem wird die Bibliotheksnummer generiert und gemeinsam mit weiteren Daten der Chipkarte (siehe DV zur Einführung und Betrieb eines Chipkarteninformationssystems) in die Zwischenstruktur (PostgreSQL-Datenbank) eingetragen. Der Konnektor sorgt anschließend für das Übertragen der Bibliotheksnummer in das Meta Directory (Tabelle 3).

Tabelle 3: Attribute des Exports in das Meta Directory

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (39)	Bibliotheksbenutzernummer (thuEduLibraryCodeNumber)	- Aktuell gültige Bibliotheksbenutzernummer - Identifiziert Benutzer der jeweiligen Bibliothek

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. „admin“ besitzt die in Tabelle 4 dargestellten Trustee-Rechte.

Tabelle 4: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Der KMS-Server ist innerhalb des internen Verwaltungsnetzes angeordnet. Der Konnektor befindet sich auf dem MD-Master-Server, der sich im gleichen Netzsegment befindet.

Anlage 11

Datenaustauschbeziehungen des Meta Directory mit dem Identity Provider IdP (Shibboleth, DFN-AAI)

1 Einordnung des IdPSat-Systems in Bezug auf das Meta Directory

Der Identity Provider dient zur Teilnahme an der DFN-AAI, der Shibboleth-basierten Authentifizierungs- und Autorisierungsinfrastruktur des Deutschen Forschungsnetzes. Der Shibboleth-Identity-Provider erhält die aktuellen Benutzerdaten über ein Satellitensystem IdPSat, welches über einen Konnektor mit dem Meta Directory verbunden ist. Der Konnektor zwischen Meta Directory und IdPSat führt notwendige Abbildungen von Attributen und Attributwerten auf den DFN-AAI-Standard durch. Außerdem haben die Benutzereinträge im IdPSat-System einen auf die Bedürfnisse der DFN-AAI angepassten Lebenszyklus.

2 Datenaustauschbeziehungen zwischen Meta Directory und IdPSat-System

Die Datenaustauschbeziehungen beschreiben den Datenimport und den Datenexport aus der Sicht des Meta Directory.

2.1 Datenexport aus dem Meta Directory in das IdPSat-System

Der Datenaustausch erfolgt aus dem Meta Directory über Filtermechanismen eines Konnektors. Zur Authentifizierung und zur Autorisierung innerhalb der DFN-AAI werden die in Tabelle 1 aufgeführten Daten benötigt. Aus den Status- und Gültigkeitsdaten im Meta Directory leitet sich ab, ob ein Benutzereintrag im IdPSat-System angelegt oder gelöscht wird.

In Tabelle 1 ist dargestellt, welche Daten einer digitalen Identität aus dem Meta Directory in das IdPSat-System übernommen werden. In Klammern stehen die Nummer des Datenfeldes (Lfd.-Nr.) aus der Anlage zur Rahmendienstvereinbarung sowie evtl. abweichende Attributbezeichnungen im lokalen Meta Directory.

Tabelle 1: Personen-Attribute, die an das IdPSat-System übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (1)	Familienname (Surname)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
2. (2)	Vorname (Given Name)	- Identifizierung einer Person - Benötigtes Attribut für die meisten Zielsysteme - Generierung von Basisdaten - wie Mailadresse, Benutzername
3. (8)	Anzeigename (displayName)	- Anzeigename eines Benutzers
4. (13)	Benutzername (uniqueID)	- Die an der Hochschule gültige Benutzer-kennung für Dienste (Hochschul-Account) - Zur Benachrichtigung der Person

5. (15)	E-Mail-Adresse (internet Email Address)	- Die an der Hochschule gültige E-Mailadresse für die dienstliche Kommunikation - Zur Benachrichtigung der Person
6. (64)	Identifikator (CN, CommonName)	- Bezeichnung innerhalb des Meta Directory
7. (32)	Name der Organisation/Hochschule (O, OrganizationalName)	- Ableitung der organisatorischen Zugehörigkeit zu einer Hochschule

Die Tabelle 2 gibt einen Überblick, welche Daten beim Export aus dem Meta Directory für das IdPSat-System generiert werden.

Tabelle 2: Rollen-Attribute, die an das IdPSat-System übergeben werden

Lfd.-Nr.	Attribut	Zweckbestimmung des Datenexports
1. (19)	Zugehörigkeit (eduPersonAffiliation)	- Spezifikation der Beziehung einer Person zur Hochschule - Autorisierung innerhalb der DFN-AAI mit fest definierten Werten - derzeit für FHE gültig: student, employee, staff, faculty, member, affiliate,

2.2 Datenimport aus dem IdPSat-System in das Meta Directory

Das Meta Directory übernimmt keine Daten aus dem System IdPSat.

3 Umsetzung des Sicherheitskonzepts (nach Anlage 2)

Für den Zugriff des Konnektors auf das Meta Directory wurde der funktionsbezogene Benutzer „admin“ im Container „service.uni“ festgelegt. „admin“ besitzt die in Tabelle 3 dargestellten Trustee-Rechte.

Zur Administration sowie zur Lösung von Problem- bzw. Konfliktfällen ist ein Administratorzugang mit umfassender Berechtigung unerlässlich. Dieser Zugang wird ausschließlich innerhalb des Hochschulrechenzentrums an ausgewählte Beschäftigte vergeben (siehe Anlage 1).

Tabelle 3: Trustee-Rechte des funktionsbezogenen Benutzers „admin“

Objekt	Eigenschaft	Rechte
User	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren
Organisational Role	Rechte auf alle Attribute	Vergleichen, Lesen, Schreiben
	Rechte auf Einträge	Suchen, Kreieren

Das IdPSat-System ist über einen eDirectory-to-eDirectory-Konnektor an das Metadirectory angeschlossen, der eine SSL-verschlüsselte Verbindung mit einem 2048 bit großen RSA-Schlüssel unterstützt. Der Konnektor läuft auf der MD-Replika im Metadir-Netzsegment.