BENUTZERDOKUMENTATION

ZENTRALE IDM-LDAP SERVERFARM

BAND 1: EINFÜHRUNG & ÜBERSICHT

Version: 1.0

Status: Produktion

Datum: 30. September 2016

Autor(en): Martin Johannemann

E-Mail: idm@tu-dresden.de
Web: http://tu-dresden.de/die_tu_dresden/zentrale_einrichtungen/zih/dienste/identitaetsmanagement/
Post: Technische Universität Dresden
Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH)
IDM
01062 Dresden

Folgende weiteren Werke zur Reihe "Zentrale IDM-LDAP Serverfarm" sind bereits erschienen:
Band 1: Einführung & Übersicht

Erstausgabe im Oktober 2016 durch das ZIH, TU Dresden,
01062 Dresden

Autor: Martin Johannemann
Herausgeber: Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH)
Technische Universität Dresden

Inhaltsverzeichnis

1 EINFÜHRUNG

1.1 KONVENTIONEN DIESES DOKUMENTES

Kursivschrift	Bezeichnungen/ Wording die aus der Anwendung stammen
Hervorgehobene Schrift	Stellt Schlüsselwörter oder Überschriften dar
	Hervorgehobene Hinweise und Informationen. Boxen dieser Art sollten unbedingt beachtet werden
	Zusätzliche Hinweise die für den aktuellen Bereich gelten und nützlich sein könnten
	Marker auf ein bestimmtes Element in einer Grafik, der im Folgetext erläutert wird

1.2 ZENTRALE IDM-LDAP SERVERFARM

Die zentrale IDM-LDAP Serverfarm ist ein **hochverfügbarer Infrastrukturdienst** welcher vom ZIH der TU Dresden betrieben und zur Verfügung gestellt wird. Dieser Dienst ist kein Bestandteil des eigentlichen ZIH IDM-Systems sondern lediglich ein angebundenes Zielsystem, welches eine der technischen Möglichkeiten bietet IDM-Daten zu beziehen (siehe Abb. 001 – OpenLDAP).

Durch die Anbindung an die zentrale IDM-LDAP Serverfarm besteht die technische Möglichkeit sämtliche vorgehaltenen IDM-Daten per LDAP / LDAPS Protokoll zu beziehen. Der direkte Bezug dieser IDM-Daten wird nur als READ-ONLY angeboten. Die gesamte Datenverwaltung läuft dabei über das ZIH IDM-System.

Die zentrale IDM-LDAP Serverfarm selbst ist ein Verbund von OpenLDAP Servern die sich einen gemeinsamen Datenbestand, der vom ZIH IDM-System vorgegeben wird, teilen. Vorwiegend sind diese Daten für UNIX-artige Systeme konzipiert worden. Eine Anbindung alternativer Zielsysteme, darunter auch Shibboleth, wird dennoch gewährt und ist praktikabel im Einsatz. Die Serverfarm ist unter der URL-Adresse ldap://ldap-service.zih.tu-dresden.de auf TCP Port 389 oder unter ldaps://ldap-service.zih.tu-dresden.de auf TCP Port 636 erreichbar.

Neben der produktiven Serverfarm wird auch ein Testsystem für spezielle Testdaten und ohne aufwendige Sicherheitsdokumentation unter ldaps://ldap-test.zih.tu-dresden.de auf TCP Port 636 angeboten.

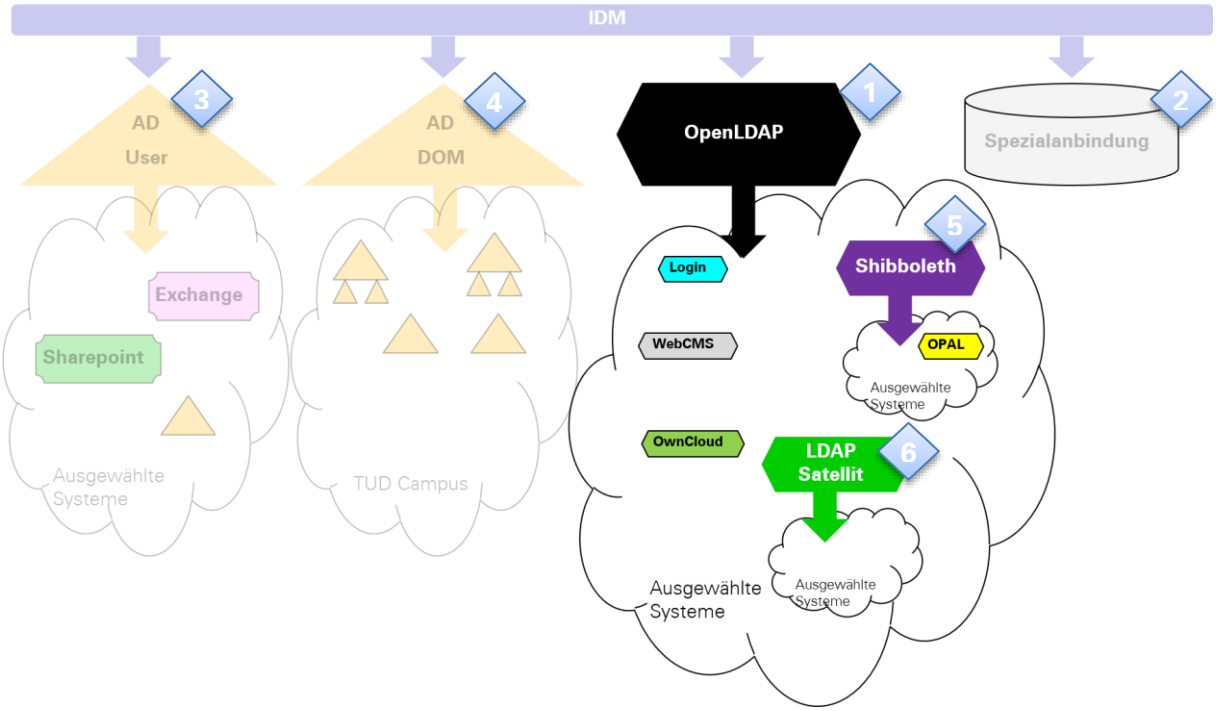

Abb. 001 – Verteilung der IDM Direktanbindungen in Bezug auf das OpenLDAP Zielsystem

1	*Zentrale IDM-LDAP Serverfarm* – Zielsystem für LDAP spezifische Abfragen und zur Verwaltung von ZIH-Accounts unter UNIX.
2	*Spezielle IDM-Anbindung* – Zielsysteme mit eigenen User-Life-Cycle oder speziellen Wünschen zur Verwaltung von IDM-Daten. Diese Anbindung erfolgt nur in seltenen Fällen.
3	*Active Directory User Domäne* – Zielsysteme / Domäne für alle zentralen Microsoft Dienste die vom ZIH angeboten werden.
4	*Active Directory Dom Domäne* – Zielsysteme / Domäne für die zentrale Nutzerauthentifizierung und Berechtigung unter Microsoft Windows.
5	*Shibboleth* – LDAP-Vorsatz zur sicheren Authentifizierung und Autorisierung von Webdiensten inklusive SingleSignOn.
6	*LDAP Satellit* – Erweiterter Ausbau der zentralen IDM-LDAP Serverfarm. Beinhaltet/ Bezieht einen Teil bzw. die gesamten IDM-LDAP Daten und stellt diese vor Ort zur Verfügung.

Die **Datenübertragung** zwischen der zentralen IDM-LDAP Serverfarm mit dem IDM-System ist **Just-In-Time**. Dabei werden sämtliche Daten ereignisgesteuert geliefert. Die Übertragung innerhalb der zentralen IDM-LDAP Serverfarm richtet sich nach dem Synchronisationsintervall der jeweiligen verwendeten Synchronisationsanbindung (siehe Abb. 002)

1.3 DIE ANBINDUNG AN DIE ZENTRALE IDM-LDAP SERVERFARM

Eine Anbindung an die zentrale IDM-LDAP Serverfarm ist über verschiedene Arten & Weisen realisierbar. Hierfür kann jede Anwendung / Programmiersprache genutzt werden die das LDAP / LDAPS Protokoll unterstützt. Die technische Umsetzung bleibt so variabel wie es der dahinter zugrunde liegende Datenschutz zulässt. Diese reicht vom einfachen Skript, was Daten aus der zentralen IDM-LDAP Serverfarm abfragt bis hin zur Synchronisation zum eigenen OpenLDAP bzw. LDAP-Konkurrenzprodukt Satellitenserver.

Die Art & Weise der technischen Umsetzung und der Bezug der jeweiligen Daten richtet sich stark nach dem erstellten Sicherheitskonzept welches vor Ort betrieben wird und bei der Stabsstelle für Informationssicherheit hinterlegt ist. Neben dem Datenschutz muss ebenfalls der Aufwand der Redundanz für die Hochverfügbarkeit betrachtet werden.

> ⓘ Ein eigener LDAP Satellitenserver kann performanter bei stark fragmentierten Abfragen sein und verfügbarer bei schwachen Netzwerkverbindungen. In Betracht muss hierbei die Menge der bezogenen Daten genommen werden, die der Datenschutz erlaubt (z.B. Ist ein eigener Serverraum zum Schutz vorhanden?) und spielt die Hochverfügbarkeit dieser LDAP Instanz eine große Rolle, sodass die Instanz redundant betrieben werden muss bzw. gibt es eine Ausfalllösung.

Für alle Anbindungen ob Test oder Produktion verwenden Sie bitte zu Beginn das IDM-Antragformular (siehe Anhang: IDM-Antragsformular). Ein vollständiger Antrag liegt nur bei der Produktionsanbindung vor.

2 TECHNISCHE ANBINDUNGSMÖGLICHKEITEN

Als Optionen für den Bezug von IDM-Daten über die zentrale IDM-LDAP Serverfarm werden folgende Anbindungsarten, die teilweise auf OpenLDAP Technologie aufbauen, zur Verfügung gestellt:

2.1 DIREKTE ANBINDUNG

Vorteile

- Kein eigener Datenbestand vor Ort nötig
- Hochverfügbare Infrastruktur seitens ZIH
- Kein weiterer Ressourcenaufwand nötig

Nachteile

- Hochverfügbare Infrastruktur auf Basis des darunter befindlichen Netzwerkes
- Verwaltung / Ergänzung der lokalen LDAP-Daten nicht möglich (ReadOnly)

Eine direkte Anbindung empfiehlt sich, wenn es sich bei dem anzubindenden Zielsystem um eine eigenständige Anwendung bzw. Einzelserver handelt. Hier sollen für diesen Einzelfall keine weiteren Ressourcen zum Einsatz kommen, sondern nur der hochverfügbare Bezug der IDM-Daten im Vordergrund stehen.

2.2 ANBINDUNG MITTELS LDAP-PROXY

Vorteile

- Kein eigener Datenbestand vor Ort nötig
- Performancesteigerung für LDAP-Abfragen, Netzwerk-Latenz mittels Caching

Nachteile

- Hochverfügbare Infrastruktur auf Basis des darunter befindlichen Netzwerkes
- Lokale Ressourcen müssen bereitgestellt werden (Räume, Technik, Personal) – kann durch ZIH Virtualisierung jedoch umgangen werden
- Hochverfügbarkeit muss nach Einsatzbereich selbst erstellt werden
- Verwaltung / Ergänzung der lokalen LDAP-Daten nicht möglich (ReadOnly)

Die Anbindung über einen LDAP-Proxy empfiehlt sich bei IT-Infrastrukturen die eine gewisse Menge an einzelnen LDAP Clientsystemen haben. Der größte Vorteil ergibt sich hier in der Bündelung der Abfragen mit zusätzlichen Caching der Daten. Hier kann bei stark fragmentierten Abfragen das Netzwerk mit entsprechenden Caching entlastet werden, ohne dass physikalische Daten vor Ort liegen. Des Weiteren ist es möglich den abgefragten IDM-Daten über den LDAP-Proxy weitere Eigenschaften mitzugeben die für die jeweiligen LDAP Clientsysteme notwendig sind.

2.3 ANBINDUNG PER SATELLITENSYSTEM

Vorteile

- Performancesteigerung für LDAP-Abfragen, Netzwerk-Latenz mittels eigenen Datenbestand
- Stabiler Betrieb bei Netzwerkausfall
- Verwaltung / Ergänzung lokaler LDAP-Daten möglich

Nachteile

- Lokale Ressourcen müssen bereitgestellt werden (Räume, Technik, Personal) – kann durch ZIH Virtualisierung jedoch umgangen werden
- Hochverfügbarkeit muss nach Einsatzbereich selbst erstellt werden

Die Anbindung per Satellitensystem empfiehlt sich bei IT-Infrastrukturen die eine zusätzliche lokale Datenverwaltung benötigen oder die Hochverfügbarkeit aufgrund von Netzwerkstörungen nicht gewährleitet kann.

Ein Satellitensystem besitzt einen ausgewählten lokalen Datenbestand von vorgegebenen IDM-Daten. Je nach Datenbestand müssen technische Voraussetzungen getroffen werden die den IT-Datenschutz erfüllen. Zusätzlich und je nach angebundener Variante aus Abb. 002 kann der lokale Datenbestand teilweise bis vollständig bearbeitet bzw. ergänzt werden.

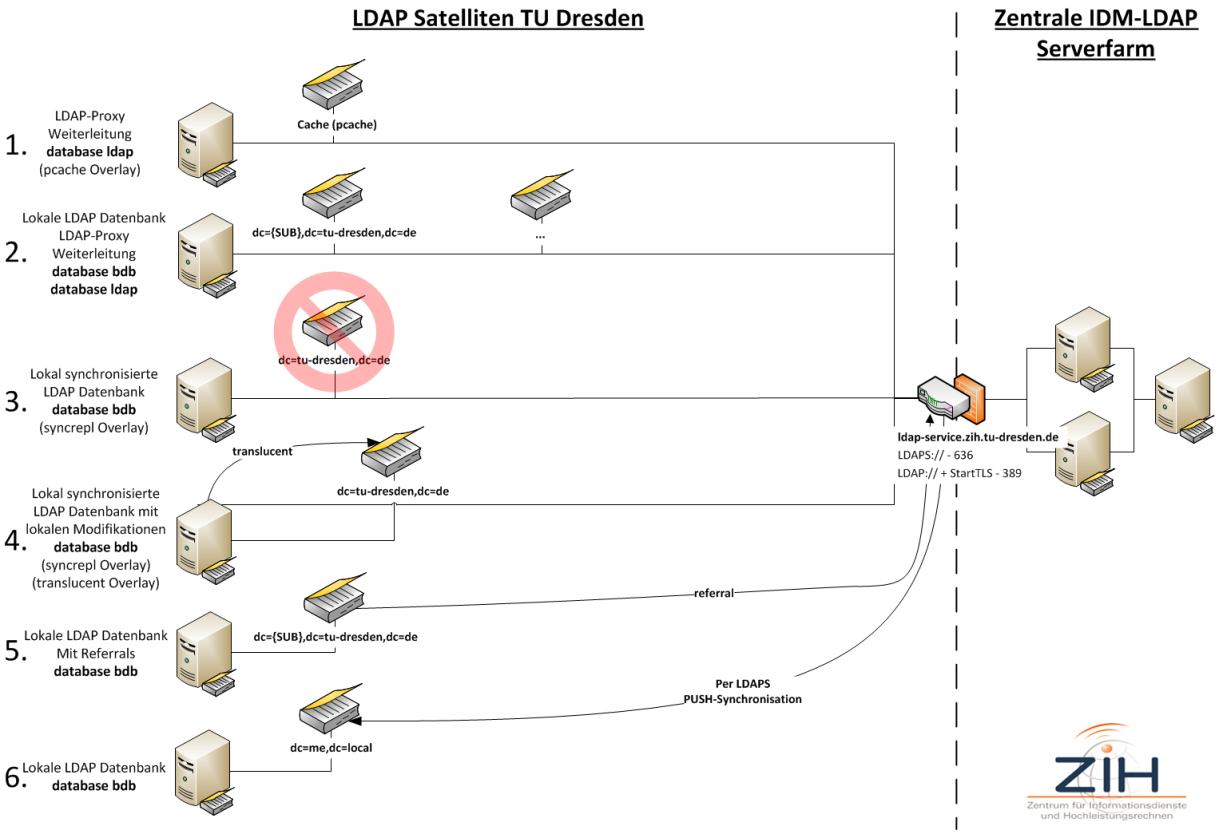

Abb. 002 – Beispielhafte Anbindung von OpenLDAP - Satelliten / -Proxy Systemen

Die gesamte LDAP Kommunikation verläuft verschlüsselt über die Ports **TCP 389** per **LDAP / StartTLS** oder **TCP 636** per **LDAPS**. Eine unverschlüsselte Kommunikation wird über die zentrale IDM-LDAP Serverfarm nicht gestattet.

Sämtliche lokalen LDAP Satellitensysteme sollten diesem Schema folgen. Die Verantwortung liegt hier beim zuständigen Administrator und unterliegt dem basierenden Sicherheitskonzept.

3 OPENLDAP AUFBAU & STRUKTUR

3.1 AUFBAU UND VERTEILUNG

Die zentrale IDM-LDAP Serverfarm besteht derzeit aus zwei getrennten Systemen. Dabei wird ein System, bestehend aus einem einzelnen Server, ausschließlich nur für Testanbindungen genutzt und ist unter der Domain ldap-test.zih.tu-dresden.de erreichbar. Das zweite System beinhaltet die produktiven IDM-Daten und umfasst eine komplexere Struktur. Diese Struktur teilt das System in Standorte ein, welche derzeit als Hauptstandort den TRE-Bau hat und als zweiten Standort das LZR. Am Hauptstandort, unter dem derzeit auch das IDMS beheimatet ist, ist die zentrale IDM-LDAP Serverfarm unter ldap-service.zih.tu-dresden.de erreichbar. Mittels vorgeschalteten LoadBalancer soll eine gleichmäßige Abfragelast auf allen LDAP-Servern verteilt sowie die Hochverfügbarkeit gewährleistet werden.

Neben der Standortverteilung gibt es vereinzelt am Campus der TU Dresden LDAP Satellitenserver die ebenfalls zur Ausfallsicherheit und Redundanz des Systems beitragen sollen.

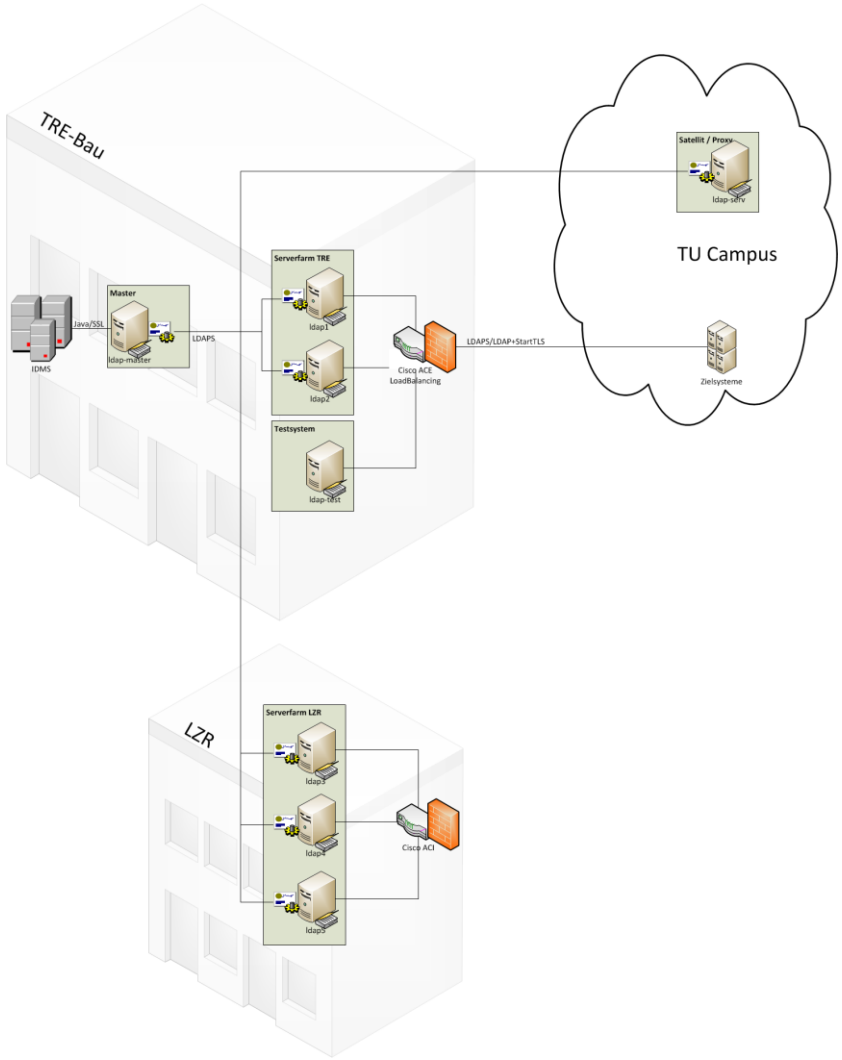

Abb. 003 – Aufbau und Verteilung der OpenLDAP Server am Campus der TU Dresden

3.2 STRUKTUR DER LDAP-DATEN

Die OpenLDAP Datenstruktur besteht aus einer einfachen und möglichst flachen Objektstruktur. Die Objekte sind dabei nach Objekttyp voneinander getrennt abrufbar. Folgende Objekte können aus der zentralen IDM-LDAP Serverfarm bezogen werden:

- Informationen über Organisationen
  - Beinhaltet alle internen und externen Organisationsobjekte
  - Die Organisationsobjekte werden hierarchisch als Baum zur Verfügung gestellt
- Informationen über Gruppen
  - Beinhaltet alle zentralen Gruppen und Gruppenmitgliedschaften
  - Wird als flache Struktur dargestellt
- Informationen über Nutzeraccounts
  - Beinhaltet alle aktiven ZIH-Accounts
  - Wird als flache Struktur dargestellt
- Informationen über inaktive / gelöschte Nutzeraccounts
  - Beinhaltet alle ehemaligen aktiven ZIH-Accounts mit minimaler Datenangabe
  - Wird als flache Struktur dargestellt
- Information über Gebäude und Räume
  - Beinhaltet alle Gebäudedaten der TU Dresden
  - Die Objekte werden hierarchisch als Baum zur Verfügung gestellt

Die daraus resultierende LDAP-Struktur ist wie folgt aufgebaut:

- **dc=**tu-dresden,**dc=**de
  - **ou=**users - *Container aller Accounts*
    - **uid=**ZIH-LOGIN
  - **ou=**groups - *Container aller Gruppen*
    - **cn=**Gruppenname
      - **memberUid=**ZIH-Login - *Gruppenmitglieder*
  - **ou=**structures - *Container für Organisationen*
    - **ou=**tu-dresden
      - **ou=**STRUKTUREINHEIT
    - **ou=**extern
      - **ou=**STRUKTUREINHEIT
  - **ou=**archive - *Container für archivierte Objekte*
    - **ou=**users - *Container archivierter Accounts*
      - **ou=**inactive - *Inaktive Accounts*
        - **uid=**ZIH-LOGIN
      - **ou=**blocked - *Gelöschte Accounts*
        - **uid=**ZIH-LOGIN
  - **ou=**facilities - Container aller Gebäude / Räume
    - **cn=**EINRICHTUNG

4 DATENSCHUTZ & DATENZUGRIFF

4.1 VORAUSSETZUNGEN

Für den Bezug von IDM-Daten über die zentrale IDM-LDAP Serverfarm ist in erster Instanz ein **IDM-Antrag** notwendig (siehe IDM-Antragsformular). Mit diesem Antrag wird eine Zusammenfassung der jeweiligen Anbindung definiert inklusive der gewünschten Daten.

Mit Eingang des Antrages kann zuvor eine LDAP Teststellung der Daten zur Verfügung gestellt werden. Soll der Antrag bis zum Ende bearbeitet werden, ist für das jeweilige System mittels **Verinice** ein Sicherheitskonzept anzufertigen und für die zu beziehenden Daten eine Verfahrensbeschreibung vorzulegen. Erst nach der Abnahme durch die Stabsstelle für Informationssicherheit kann eine Freischaltung des Zuganges zur produktiven IDM-LDAP Serverfarm erfolgen.

4.2 MINIMALPRINZIP

Anhand des IDM-Antrages werden die zu beziehenden Daten für das jeweilige Zielsystem minimiert. Dabei kann das Zielsystem lediglich die Daten beziehen die es im Antrag entsprechend definiert hat. Für jede Zielsystemanbindung wird ein Designdokument angefertigt in dem die Zugangsdaten sowie der Umfang der Bezugsdaten enthalten sind.

4.3 BESCHRÄNKUNGEN

Anhand des Minimalprinzips werden die Menge der Daten bereits auf den im IDM-Antrag angegebenen Umfang festgelegt. Dies betrifft die Objekte in LDAP selbst sowie deren Attribute sofern das Objekt gelesen werden kann.

Neben dieser Datenbeschränkung gibt es in der zentralen IDM-LDAP Farm noch eine Kapazitätsgrenze abzufragender Objekte und eine Zeitbeschränkung. Diese Beschränkungen liegen auf den OpenLDAP Standard von 500 Objekte und 3600 Sekunden pro Abfrage. Bei überziehen dieser Beschränkungen werden folgende Meldungen zurückgeowrfen: „Size limit exceeded (4)“ oder „Time limit exceeded (4)“. Sofern mehr als 500 Objekte pro Abfrage gewünscht werden sollte man in OpenLDAP „Paging“ verwenden.

5 ANHANG

A STICHWORTVERZEICHNIS

Authentifizierung	Nachweis/Identifizierung einer Eigenschaft (hier: Person)
Autorisierung	Zustimmung/Bestätigung bestimmter Rechte
Bidirektional	In beide Richtungen verlaufend
FAQ	Englisch: ***F****requently* ***A****sked* ***Q****uestions Deutsch: Häufig gestellte Fragen*
Screenshot	Bildschirmfoto
Tooltip	Kleines Pop-Up Fenster mit zusätzlichen Informationen
URL	Englisch: **U**niform **R**esource **L**ocator Deutsch: Ressourcenanzeiger

B GLOSSAR

Authentifizierungsdienst	Ein Authentifizierungsdienst stellt anderen IT-Systemen Benutzerdaten als Dienstleistung zur Verfügung. Die Nutzung eines zentralen Authentifizierungsdienstes erlaubt es den Benutzern, alle angebundenen IT-Systeme mit einer einheitlichen Benutzerkennung zu benutzen. Häufig verwendete Authentifizierungsdienste sind Active Directory (Verzeichnisdienst von Microsoft), OpenLDAP (Verzeichnisdienst von Linux und Unix) oder Shibboleth (Authentifizierungsdienst für Dienste und Anwendungen des Web)
Dienst	Als Dienst wird eine Anwendung bezeichnet die einen gewissen Dienst für Kunden anbietet z.B. E-Mail.
Dienstbetreiber	Als Dienstbetreiber bezeichnet man eine(n) Verantwortliche(n) für den Betrieb eines IT-Dienstes im Gesamten z.B. Exchange, Datennetz, Fileserver etc.
Identitätsmanagement (IDM)	Unter Identitätsmanagement wird die Summe aller Maßnahmen verstanden, die notwendig sind, um Benutzer in komplexen und heterogenen Systemlandschaften eindeutig zu erkennen sowie ihnen genau die Berechtigungen auf Dienste und Daten zur Verfügung zu stellen, die sie aktuell im Rahmen ihrer Tätigkeit benötigen. Dabei sind alle Maßnahmen im Rahmen von standardisierten und nachvollziehbaren Prozessen durchzuführen. Häufig wird ein IDM-System als technische Basis für das Identitätsmanagement benutzt.
IDM	siehe Identitätsmanagement
IDMS	Identitätsmanagement System; Siehe IDM-System

IDM-System	Ein IDM-System dient der zentralen Verwaltung von Benutzerdaten aller IT-Systeme innerhalb einer Organisation und stellt damit die technische Basis für das Identitätsmanagement dar. Der Betrieb eines IDM-Systems umfasst den Import von Daten aus den angebundenen Quellsystemen, die interne Verarbeitung von Daten und die Übermittlung von Daten an die angebundenen Zielsysteme. Häufig werden die Daten nicht direkt an die Zielsysteme übermittelt, sondern über zwischengeschaltete Authentifizierungsdienste bereitgestellt. An der TU Dresden wird ein IDM-System von Novell eingesetzt.
Just-In-Time	Anderer Ausdruck für bedarfsgerechte Lieferung. In diesem Dokument versteht man darunter den Datenaustausch nur bei Bedarf. Somit werden unnötige Datenübertragungen verhindert.
Konnektor	Anderes Wort für Verbindung. Im IDMS ist ein Konnektor eine Verbindungsschnittstelle die Daten vom IDM-Kern zum Zielsystem transportiert und transformiert.
Shibboleth	Siehe Authentifizierungsdienst
UA	Siehe UserApplication
UserApplication (UA)	Bei der Userapplication handelt es sich um eine zum IDM-System mitgelieferte Schnittstelle für die Endbenutzer. Es ist ein Java-basiertes Web-Frontend, das dem Benutzer die Möglichkeit gibt, abhängig von seinen Berechtigungen im IDM-System gespeicherte Daten von sich oder anderen zu betrachten, zu organisieren oder zu bearbeiten.
ZIH-Account	Als ZIH-Account wird ein Konto bezeichnet welches ein Nutzer gehört. Hier kann es möglich sein, dass ein Nutzer mehrere ZIH-Accounts besitzt.
ZIH-Login	Als ZIH-Login bezeichnet man die Einwahldaten die ein Nutzer benötigt um sich bei den entsprechenden Diensten einwählen zu können. Meistens wird das ZIH-Login auch als Bezeichnung für die Kombination ZIH-Account + ZIH-Passwort verwendet.

C DOKUMENTENVERSION

Version	Datum	Autor	Änderungen
1.0	30.10.2016	Martin Johannemann	Erstellung dieses Dokumentes

D IDM-ANTRAGSFORMULAR

TECHNISCHE UNIVERSITÄT DRESDEN

IDM - Antragsformular

1. Datenverarbeitende Stelle (gem. Pkt. 1 Anlage 1 zu MPrP 2/2015)

Bezeichnung:

Verantwortlicher Leiter / Verantwortliche Leiterin (Antragsteller / Antragstellerin)

Name: Vorname:

E-Mail: Telefon:

Zuständiger Administrator / Zuständige Administratorin

Name: Vorname:

E-Mail: Telefon:

Zuständiger Vertreter / Zuständige Vertreterin

Name: Vorname:

E-Mail: Telefon:

2. Anforderungen des Antragstellers / der Antragstellerin

Art der Anbindung

☐ (1) Anschluss eines zusätzlichen Zielsystems an das IDM-System
☐ (2) Änderung von existierenden Schnittstellen zum IDM-System
☐ (3) Verwaltung zusätzlicher Daten im IDM-System
☐ (4) Andere Anforderung an das IDM-System

Inhaltliche Beschreibung der Anforderung / Auflistung der zu liefernden Daten

(ggf. auf Zusatzblatt erweitern)

3. Entscheidung / Veranlassung des ZIH

Entscheidung des ZIH zur Umsetzung der Anforderung

◯ JA

◯ NEIN

Wenn NEIN, dann Begründung angeben:

Wenn JA, dann Art und Weise der Umsetzung durch das ZIH:

Art der Umsetzung:

Termin der Umsetzung:

Zuständiger Bearbeiter / Zuständige Bearbeiterin ZIH:

Name: Vorname:

E-Mail: Telefon:

Folgende Unterlagen liegen vor:

☐ Verfahrensverzeichnis gem. MPrP 2/2015
(http://www.verw.tu-dresden.de/VerwRicht/Sachwort/download.asp.file=mprp0215.pdf)

☐ IT-Sicherheitskonzept gem. BSI-Grundschutz

4. Signaturen / Unterschriften

Datum Antragsteller(in)

Datum IT-Referent(in)

Datum ZIH

Datum Stabsstelle für Informationssicherheit

Votum der Stabsstelle für Informationssicherheit: