Zwischen der Leitung der Universität Augsburg,
vertreten durch die Präsidentin und den Kanzler,

und

dem Personalrat der Universität Augsburg,
vertreten durch den stellvertretenden Vorsitzenden,

wird gem. Art. 73 Abs.1 Satz 1 i. V. mit Art. 75a Abs.1 Nr. 2 des Bayerischen Personalvertretungsgesetzes (BayPVG) nachfolgende

Dienstvereinbarung

über die Einführung und den Betrieb des Identity Management Systems mit den daran angeschlossenen Quell- und Zielsystemen (nachfolgend als IdM-System bezeichnet)

vom 25.10.2011 mit den geänderten Anlagen vom 20.03.2013
abgeschlossen:

§ 1 Geltungsbereich

(1) Diese Dienstvereinbarung mit ihren Anlagen 1 (Systembeschreibung und Datenfelder des IdM-Systems), 2 (Beschreibung der Zielsysteme) und 3 (Datenschutzfreigabe – Verfahrensbeschreibung nach Art. 26 Abs. 3 Satz 1 Bayerisches Datenschutzgesetz (BayDSG) in den jeweils geltenden Fassungen gilt für alle Beschäftigte der Universität Augsburg.

(2) Diese Dienstvereinbarung regelt die Bedingungen für Einführung, Betrieb und Weiterentwicklung des IdM-Systems an der Universität Augsburg sowie den Umfang der vom Personalverwaltungssystem VIVA (Quellsystem) übernommenen Datenfelder und deren Speicherung, Verarbeitung und Übermittlung an die angeschlossenen Zielsysteme (Anlage 2).

(3) Diese Dienstvereinbarung bezieht sich nicht auf die Einführung und den Betrieb der Systeme, die an das IdM-System angeschlossen werden. Diese haben eigene Begründungen und Grundlagen für ihren Betrieb.

§ 2 Aufgaben und Ziele des IdM-Systems

(1) Das IdM-System ordnet jeder/jedem Universitätsangehörigen auf der Basis autoritativer, tagesaktueller Personen- und Organisationsdaten eine eindeutige digitale Identität zu. Diese digitale Identität repräsentiert Universitätsangehörige in den IuK-Systemen der Universität

Augsburg und liefert die Grundlage für die automatisierte Zuteilung von Zugriffsberechtigungen. Die Universitätsangehörigen können durch Nachweis ihrer jeweiligen digitalen Identität und entsprechend ihrer Berechtigungen auf sämtliche personalisierten IuK-Dienste der Universität zugreifen.

(2) Um über autoritative, tagesaktuelle Informationen zu allen Beschäftigten zu verfügen, bezieht das IdM-System täglich personenbezogene Daten aus dem Personalverwaltungssystem VIVA.

(3) Mit dem Betrieb des IdM-Systems werden darüber hinaus insbesondere folgende Ziele verfolgt:

a) Standardisierung von Administrations- und Verwaltungsvorgängen bzgl. der Zugangsverwaltung zu den personalisierten IuK-Systemen.

b) Erhöhung der Datenqualität der Identitätsdaten.

c) Erhöhung des Datenschutzes durch Transparenz bzgl. der Speicherung von Personendaten und der zugrundeliegenden Datenflüsse.

e) Erhöhung des Datenschutzes durch gezielte Verwaltung von Nutzungsrechten.

f) Erhöhung der Sicherheit durch eindeutige digitale Identitäten.

g) Vermeidung von Mehrfachdatenhaltung in den verschiedenen IuK-Systemen.

§ 3 Ausschluss der Leistungs- und Verhaltenskontrolle

Das IdM-System wird nicht zur Leistungs- und Verhaltenskontrolle genutzt. Statistische Auswertungen sind ausschließlich anonymisiert zulässig. Der Systembetreiber gewährt dem Personalrat auf Verlangen Einsicht in die Systemdaten.

§ 4 Änderung und Erweiterung des Systems

(1) Bei der Entwicklung neuer oder wesentlichen Erweiterung bestehender Schnittstellen der Quell- und Zielsysteme zum IdM-System ist deren Inbetriebnahme nur unter Einhaltung der datenschutzrechtlichen Bestimmungen und nach rechtzeitiger Einbeziehung des Personalrates durch den Systembetreiber zulässig.

(2) Die Anlagen sind durch den Systembetreiber entsprechend anzupassen.

§ 5 Datenschutz und Datensicherheit

(1) Die Universität sichert personenbezogene Daten gegen Verlust, Ausspähung, Manipulation usw. durch entsprechende technische und organisatorische Maßnahmen. Personenbezogene Daten dürfen im IdM-System nur verarbeitet werden, wenn diese Verarbeitung unter Beachtung des BayDSG in der jeweils geltenden Fassung geregelt ist. Art und Umfang der zu verarbeitenden personenbezogenen Daten ergeben sich aus der Anlage 1.

(2) Wird eine missbräuchliche Nutzung festgestellt, ist die Universität verpflichtet, die Ursachen dafür umgehend abzustellen und den Personalrat, sowie die Datenschutzbeauftragte/den Datenschutzbeauftragten zu informieren. Besteht ein ausreichend begründeter Verdacht der missbräuchlichen Datenerhebung oder missbräuchlichen Nutzung des IdM-Systems, findet im Einvernehmen mit dem Personalrat eine gezielte Überprüfung statt.

(3) Die Beschäftigten werden rechtzeitig und in geeigneter Art und Weise durch den Systembetreiber über die Einführung und Funktionsweise des IdM-Systems informiert. Sie erhalten auf Anfrage Auskunft über alle zu ihrer Person im IdM gespeicherten Daten. Beschäftigte erhalten bei ihrer Einstellung ein entsprechendes Formblatt.

(4) Die Löschungsfristen richten sich nach den geltenden gesetzlichen, insbesondere datenschutzrechtlichen Bestimmungen.

(5) Verarbeitungs- und nutzungsberechtigte Personengruppen sind in der aktuell geltenden Datenschutzfreigabe (Verfahrensbeschreibung nach Art. 26 Abs. 3 Satz 1 BayDSG) festgelegt. (Anlage 3)

§ 6 Anschluss von Zielsystemen

(1) Jedes Zielsystem ist in der Anlage 2 dieser Dienstvereinbarung in einem eigenen Abschnitt zu dokumentieren.

(2) Die Systemadministratorinnen/Systemadministratoren der Zielsysteme werden in einer vom Systembetreiber geführten Liste erfasst.

§ 7 Inkrafttreten, Laufzeit, Kündigung

(1) Die Dienstvereinbarung tritt mit ihrer Unterzeichnung in Kraft.

(2) Für die Kündigung dieser Vereinbarung gilt Art. 73 Abs. 4 des Bayerischen Personalvertretungsgesetzes in der jeweils geltenden Fassung. Die Parteien haben unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufzunehmen. Bis zum Abschluss einer neuen Dienstvereinbarung gilt die bisherige fort.

(3) Einvernehmliche Änderungen bedürfen der Schriftform und sind jederzeit ohne Kündigung möglich.

Anlagen:

1. Systembeschreibung und Datenfelder des IdM-Systems (mit Grundsätzen für ein Sicherheitskonzept)
2. Beschreibung der Zielsysteme
3. Datenschutzfreigabe (Verfahrensbeschreibung nach Art. 26 Abs. 3 Satz 1 BayDSG)

Augsburg, den 20.03.2013

Präsidentin der Universität (Prof. Dr. Sabine Doering-Manteuffel)	Kanzler der Universität (Alois Zimmermann)	Stellv. Vorsitzender des Personalrats der Universität (Joachim Lutz)

Anlage 1

zur

Dienstvereinbarung über die Einführung und den Betrieb des Identity Management Systems mit den daran angeschlossenen Quell- und Zielsystemen (nachfolgend als IdM-System bezeichnet)

Systembeschreibung und Datenfelder des IdM-Systems
(mit Grundsätzen für ein Sicherheitskonzept)

Stand 20.03.2013

*) siehe 8.1 Glossar

Inhaltsverzeichnis

*) siehe 8.1 Glossar

1 Vorbemerkungen

Diese Anlage beschreibt im Überblick das IdM-System der Universität Augsburg sowie die darin verwendeten Datenfelder. Diese Anlage reflektiert den aktuellen Stand unter Berücksichtigung der Anforderungen der beteiligten Systeme und konzentriert sich auf die für die Dienstvereinbarung wesentlichen Aspekte.

Das Rechenzentrum übernimmt stellvertretend für die Universität Augsburg (Systembetreiber) die Einführung und den Betrieb des IdM-Systems.

2 Aufgaben des IdM-Systems

Das IdM-System ist ein „Filter“ zwischen den Quellsystemen und den Zielsystemen mit den darauf zugreifenden Endsystemen*). Es ist nicht die Aufgabe des IdM-Systems, Daten selbst zu erfassen oder zu veröffentlichen. Es soll anderen Systemen als Quelle dienen.

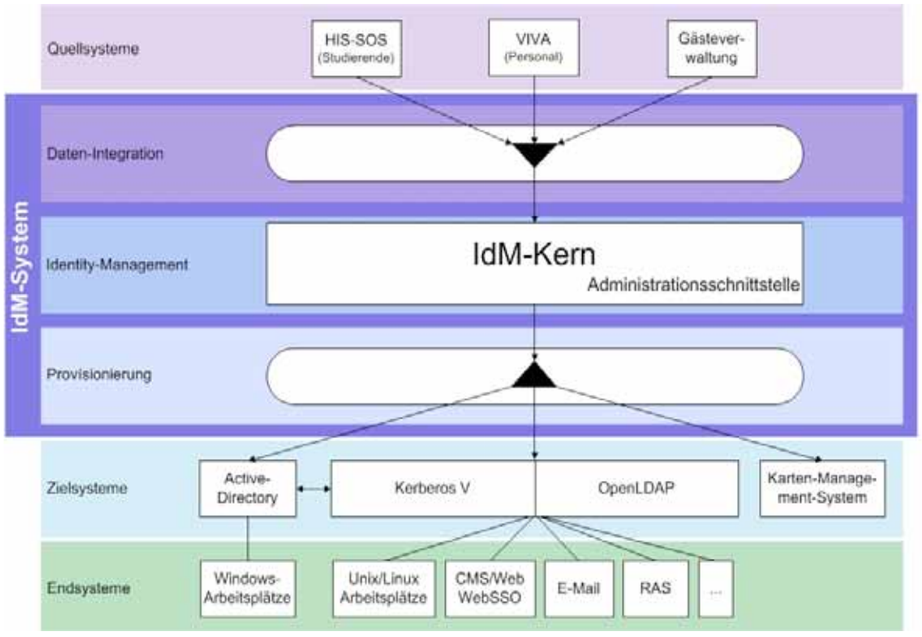
Das IdM-System hat folgende Aufgaben:

- Die weitgehend automatische Verwaltung persönlich zugeordneter EDV-Ressourcen anzustoßen.
- Die Grundlage für die Zuteilung von Zugriffsberechtigungen zu liefern.
- Dafür Sorge zu tragen, dass angeschlossene EDV-Systeme verlässliche und aktuelle Daten über die Mitglieder der Universität erhalten.

Den Endsystemen werden dann nur diejenigen Informationen zur Verfügung gestellt, die für die Authentifizierungs-*) und Namensdienste notwendig sind.

3 Struktur des IdM-Systems

Die Abbildung zeigt einen schematischen Überblick über die Integration des IdM-Systems in die bestehende IT-Infrastruktur an der Universität Augsburg.



Das aus drei Schichten (Daten-Integration, Identity-Management und Provisionierung) bestehende IdM-System versorgt die Zielsysteme mit Schnittstellen zur Authentifizierung*) sowie den benötigten Benutzer- und Gruppeninformationen (Namensdienste).

*) siehe 8.1 Glossar

- Quellsysteme: Zur Gewinnung der Identitätsinformationen werden die verschiedenen Datenbanken der Quellsysteme, Personalverwaltung (VIVA*)), Studierendenverwaltung (HIS-SOS*)) sowie die Gästeverwaltung*), durch automatische Prozesse über die Daten-Integrationsschicht an den IdM-Kern*) angebunden.
- Daten-Integration: Die Daten-Integrationsschicht hat die Aufgabe, unterschiedliche digitale Identitäten zu einer digitalen Identität zusammen zu führen. Wenn z.B. eine Person sowohl Beschäftigte/Beschäftigter als auch Studierende/Studierender ist, dann wird somit nur ein Datensatz für diese Person im IdM-Kern angelegt.
- Identity-Management: Im IdM-Kern werden die vom IdM-System verwalteten personenbezogenen Daten gespeichert. Zugriff auf die im IdM-Kern gespeicherten Daten hat nur der in Anlage 3 der Dienstvereinbarung genannte Personenkreis.
- Provisionierungsschicht: Die Provisionierungsschicht hat die Aufgabe, die im IdM-Kern verwalteten RZ-Benutzerkennungen*) und Gruppeninformationen automatisiert an die Zielsysteme zu liefern. Als Zielsysteme gibt es Microsoft Active Directory*) für die Versorgung der Windows-Arbeitsplätze, die OpenLDAP/Kerberos-Infrastruktur*) für alle anderen Endsysteme*) und das Karten-Management-System (KMS) zur Bereitstellung der Campus Card Augsburg für Studierende und Beschäftigte.

4 Personenbezogene Datenfelder des IdM-Systems und ihre Anwendungen

Die zahlreichen durch das IdM-System unterstützten Anwendungen erfordern auch die Speicherung personenbezogener Daten im IdM-System. Die benötigten Datenfelder werden im Folgenden näher erläutert.

4.1 Personenbezogene Daten im Überblick

Datenfeld	Kurzbeschreibung	Quellen			IdM
		HIS-SOS	VIVA	Gästeverwaltung	
Nachname	kompletter Nachname der Person	x	x	x	x
Namenzusätze	Namenszusätze der Person, z.B. von, van der	x	x	x	x
Vorname	kompletter Vorname der Person	x	x	x	x
Vorgestellte Titel	Titel der Person, z. B. Dr.	x	x	x	x
Nachgestellte Titel	z.B. Ph.D.	x	x	x	x
Geburtsname	Geburtsname der Person	x	x		x
Geburtsdatum	Geburtsdatum der Person	x	x	x	x
Geschlecht	Geschlecht der Person	x	x	x	x
Quellsystem	dient interner technischer Zwecke; mögliche Werte: HIS-SOS, VIVA, Gast				x
Identifikator	universell eindeutiger Schlüssel für einen Eintrag, vom IdM intern generiert				x
Matrikelnummer	Matrikelnummer der Studierenden/des Studierenden	x			x
Datum der Immatrikulation	Immatrikulationsdatum	x			x
Datum der Exmatrikulation	Exmatrikulationsdatum	x			x
Semesterstatus	rückgemeldet, exmatrikuliert, beurlaubt, Neueinschreibung	x			x
Studiengang, -Nr., Fakultät, Fachsemester, Angestrebter Abschluss, Kennzeichen für Haupt- oder Nebenfach	Bei Studierenden für die Ableitung von Gruppenmitgliedschaften als Voraussetzung für spezielle Berechtigungen	x			x
Identnummer	eindeutiger Schlüssel für einen Eintrag in HIS-SOS	x			x
Studienbeginn	erster Tag des Studiums des Studierenden	x			x
Rückgemeldet bis	letzter Tag des Semesters bis zu dem der Studierende zurückgemeldet ist	x			x
VIVA-Nummer	VIVA-Nummer einer Beschäftigten/eines Beschäftigten		x		x
Mitarbeiterart	Angabe ob Univ. Prof., PD., wissensch., techn., Verw.- oder sonstiges Personal		x		x
Vertragsbeginn	Datum des Vertragsbeginns		x		x
Vertragsende	Datum des Vertragsendes		x		x
Organisationseinheit	Organisationszugehörigkeit einer Person, entspricht einer Objekt-ID		x		x
Objektbezeichner	Textbeschreibung einer Organisationseinheit, z.B. Rechenzentrum		x		x
Objekt-ID	ID einer Organisationseinheit		x		x
Gastnummer	Gast-ID des Gastes			x	x
Gaststatusbeginn	Startdatum der Gastzugehörigkeit			x	x
Gaststatusende	Enddatum der Gastzugehörigkeit			x	x
Gasteinrichtung	Einrichtung, welcher der Gast zugeordnet ist			x	x
RZ-Benutzerkennung	Login-Name einer Person für die Benutzung von IT-Diensten der Universität				x
Initialpasswort	Startpasswort, das bei der Erstellung der RZ-Benutzerkennung generiert wird				x

*) siehe 8.1 Glossar

Primärgruppe	Primäre Gruppe, der die RZ-Benutzerkennung zugeordnet ist				x
Status eines Accounts	gibt an ob die RZ-Benutzerkennung aktiv ist				x
Startdatum eines Accounts	gibt an ab wann eine RZ-Benutzerkennung gültig ist				x
Enddatum eines Accounts	gibt an bis wann eine RZ-Benutzerkennung gültig ist				x
Gruppen mit Gruppenmitgliedern	Gruppenzugehörigkeiten				x

Die benötigten personenbezogenen Daten lassen sich prinzipiell in drei Kategorien einteilen.

- Daten zur Identifizierung von Personen
  - Nachname, Namenszusätze, Vornamen, Titel, Geburtsname, Geburtsdatum
  - Matrikelnummer, Identnummer, VIVA-Nummer*), Gastnummer
  - Identifikator
- Anwendungsorientierte personenbezogene Daten
  - RZ-Benutzerkennung*)
  - Initialpasswort
  - Primärgruppe und weitere Gruppen
  - Studiengang, -Nr., Fakultät, Fachsemester, angestrebter Abschluss, Kennzeichen für Haupt- oder Nebenfach und Semesterstatus
  - Mitarbeiterart, Organisationseinheit, Gasteinrichtung
  - Objektbezeichner und Objekt-ID
  - Datum der Immatrikulation und Exmatrikulation, Studienbeginn, Rückgemeldet bis, Vertragsbeginn und Vertragsende, Gaststatusbeginn und -ende
  - Geschlecht
- Technisch orientierte Daten zum Aufbau der verzeichnisinternen Strukturen.
  - Quellsystem
  - Gültigkeitsstatus einer RZ-Benutzerkennung
  - Beginn- und Enddatum einer RZ-Benutzerkennung

5 Schnittstellen zu den Quellsystemen

Programme, die die Verbindung von Quell- und Zielsystemen zum IdM-System herstellen und die den Datenfluss durch definierte Regeln festlegen, werden Schnittstellen oder Konnektoren*) genannt. Dabei muss von den Quellsystemen nur der lesende Zugriff und ein aktueller Export der betreffenden Datenfelder gewährt werden. Der Konnektor liest in regelmäßigen Abständen diesen Export ein und errechnet Änderungen durch einen Vergleich mit dem vorhergehenden Datenbestand. Diese Änderungen werden dann automatisch entsprechend definierter Regeln verarbeitet. Die Daten werden bei diesem Vorgang zum IdM-System verschlüsselt übertragen, wodurch ein Ausspähen der Daten verhindert wird.

6 Administrationskonzept

Die vollen und ausschließlichen Administrationsrechte auf Hard- und Software des IdM-Systems (inkl. IdM-Kern*), Konnektoren*) und Service- und Administrationsapplikationen) werden nur die zuständigen IdM-Administratorinnen/IdM-Administratoren im Rechenzentrum innehaben. Im IdM-Kern muss man zwischen Personen- und Gruppendaten unterscheiden, die in jeweils eigenen Bereichen liegen. Im Gruppenbereich werden Administrationsrechte an Gruppen-Administratorinnen/Gruppen-Administratoren (in der Regel die DV-Betreuerinnen/DV-Betreuer) delegiert. Sie beziehen sich rein auf das Anlegen, Ändern und Löschen von Gruppen. Die Gruppen-Administratorinnen/Gruppen-Administratoren haben im Personenbereich hingegen keinerlei Administrationsrechte. Sie können dort lediglich die betrieblich notwendigen Attribute einsehen. Später werden eingeschränkte Rechte an die Mitarbeiterinnen/Mitarbeiter des Beratungs- und Servicezentrums vergeben, soweit dies für den regelmäßigen Betrieb notwendig ist. Die aktuell zuständigen Administratorinnen/Administratoren des IdM-Systems werden auf einer Liste im Rechenzentrum erfasst (siehe § 6 Abs. 2 Dienstvereinbarung).

*) siehe 8.1 Glossar

7 Protokollierung der Konnektoraktivitäten*)

Sämtliche Identity Management Konnektoren*) erstellen in geschützten Verzeichnissen auf dem Identity Management Server detaillierte Logdateien. Diese werden regelmäßig archiviert und in die Datensicherung einbezogen.

8 Grundsätze zum Sicherheitskonzept des IdM-Systems

Das IdM-System mit sämtlichen darin enthaltenen Daten ist entsprechend der jeweils aktuellen technischen und organisatorischen Möglichkeiten vor Missbrauch, Manipulation und Ausspähung zu schützen.

Im IdM-System werden sogenannte funktionsbezogene Accounts, zum Beispiel für den Zugriff der Konnektoren, verwaltet. Diese funktionsbezogenen Accounts stellen keine zu verwaltenden Personen im herkömmlichen Sinne dar und greifen lesend und schreibend auf den IdM-Kern*) zu. Die Art und Weise des Zugriffs dieser funktionsbezogenen Accounts ist so gestaltet, dass sich die Kommunika–tionsbeziehungen und der Datenaustausch mit dem IdM-System auf das erforderliche Mindestmaß beschränken.

8.1 Anhang: Glossar

Active Directory: Das Microsoft Active Directory System des Rechenzentrums ist die Grundlage für den Betrieb von Windows-Arbeitsplätzen und Windows-Diensten an der Universität Augsburg sowie die Authentifizierung und Autorisierung der Benutzerinnen/Benutzer gegenüber diesen Systemen.

Authentifizierung: Authentifizierung (v. griech. *authentikos* für „Anführer“) ist der Vorgang der Überprüfung (Verifikation) einer behaupteten Identität, beispielsweise einer Person oder eines Objekts. Dies erfolgt im einfachsten Fall durch Angabe eines Anmeldenamens und des zugehörigen Passworts.

Endsysteme: Endsysteme sind die diversen personalisierten IT-Systeme der Universität Augsburg (Unix/ Linux/Windows-Arbeitsplätze, Mailsystem, Content Management System, Web-Dienste, QIS-Portal der Universitätsverwaltung u.v.m.).

Gästeverwaltung: In der Gästeverwaltung werden die Personen verwaltet, die weder in HIS-SOS noch in VIVA erfasst werden, z. B. Tagungs- oder Forschungsgäste. Die Gästeverwaltung wird vom Rechenzentrum gepflegt.

HIS-SOS: HIS-SOS ist die Studierendenverwaltung, die von der Studentenkanzlei gepflegt wird.

IdM-Kern: Der IdM-Kern ist ein Verzeichnisdienst, der die Daten von anderen Verzeichnisdiensten zusammenfasst. Dies ermöglicht es, mehrere Verzeichnisdienste zu synchronisieren.

Kerberos V: Kerberos V (v. griech. *Cerberus*, ist in der griech. Mythologie der Höllenhund und Torhüter, der den Eingang zur Unterwelt bewacht) ist ein sicherer Authentifizierungsdienst, der die Passwörter der Benutzer verschlüsselt speichert. Kerberos V ist zusammen mit OpenLDAP die Grundlage zur Authentifizierung und Autorisierung der meisten IT-Dienste der Universität Augsburg (Endsysteme).

Konnektor: Programme, die die Verbindung von Quell- und Zielsystemen zum IdM-System herstellen und die den Datenfluss durch definierte Regeln festlegen, werden Konnektoren oder Schnittstellen genannt.

LDAP: Das Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll, das die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes ermöglicht.

OpenLDAP: OpenLDAP ist ein offener Verzeichnisdienst, in dem die Benutzer- und Gruppeninformationen abgelegt werden. OpenLDAP ist zusammen mit Kerberos V die Grundlage zur Authentifizierung und Autorisierung der meisten IT-Dienste der Universität Augsburg (Endsysteme).

RZ-Benutzerkennung: Die RZ-Benutzerkennung ist die persönliche Benutzerkennung der Universitätsangehörigen (und Gäste) zu den personalisierten IT-Systemen der Universität Augsburg. Sie dient dem Nachweis der persönlichen Identität.

VIVA: VIVA ist die Personalverwaltung, die von der Personalabteilung gepflegt wird.

*) siehe 8.1 Glossar

Anlage 2

zur

Dienstvereinbarung über die Einführung und den Betrieb des Identity Management Systems mit den daran angeschlossenen Quell- und Zielsystemen (nachfolgend als IdM-System bezeichnet)

Beschreibung der Zielsysteme

Stand 20.03.2013

Inhaltsverzeichnis

1. Übersicht Zielsysteme

Bei der Anbindung der Zielsysteme wird pro Zielsystem ein Abschnitt mit folgenden Informationen erstellt:

1) Eine grundsätzliche Beschreibung des Systems (Systembeschreibung)

2) Eine Darlegung der Ziele, die mit dem System verfolgt werden (Ziele)

3) Eine Aufstellung der vom IdM-System weitergegebenen Datenfelder (Benötigte Daten)

4) Eine Beschreibung und Begründung der Regeln, die der Weitergabe der Daten oder der Zuteilung einer Ressource oder einer Berechtigung zugrunde liegen. Insbesondere ist darzulegen, ob die Regeln grundsätzlich auf einem Automatismus basieren oder durch einen zusätzlichen Administrationsvorgang beeinflusst werden. (Art der Datenweitergabe und -verwendung)

2. Aktuelle Zielsysteme

Aktuell sollen folgende Systeme an das IdM-System angebunden werden:

2.1 OpenLDAP/Kerberos Infrastruktur des Rechenzentrums

2.1.1 Systembeschreibung

OpenLDAP ist ein offener Verzeichnisdienst in den Informationen zu den Benutzeraccounts und Gruppen abgelegt werden. Kerberos ist ein sicherer Authentifizierungsdienst in dem die Passwörter der Benutzerinnen/Benutzer verschlüsselt gespeichert werden. Die OpenLDAP/Kerberos-Infrastruktur basiert auf dem OpenSource-Produkt OpenLDAP und MIT Kerberos V. Diese Infrastruktur des Rechenzentrums wird zur Authentifizierung und Autorisierung diverser IT-Dienste genutzt. Dazu zählen unter anderem alle Unix-/Linux-Arbeitsplatzrechner, die Bereitstellung von Netzwerkspeicherplatz und Netzwerkdrucker, das Mailsystem, diverse personalisierte Web-Anwendungen (u.a. CMS), die Zugangsnetze (VPN, WLAN, Wählzugänge) des Rechenzentrums und das Web-Single-Sign-On-System. Außerdem ist von außerhalb des Universitäts-Campus E-Mail-Zugriff über Webmail, SFTP- und SSH-Zugriff auf die eigenen Daten (bekannt als Home- oder H:-Laufwerk) sowie zu den personalisierten Web-Anwendungen möglich.

2.1.2 Ziele

Ziel der OpenLDAP/Kerberos-Infrastruktur ist der Zugang zu allen Unix-/Linux Arbeitsplätzen sowie die Bereitstellung von EDV-Ressourcen für Beschäftigte, Studierende und Gäste.

2.1.3 Benötigte Daten

Folgende Datenfelder werden aus dem IdM-Kern in der OpenLDAP/Kerberos-Infrastruktur benötigt: Nachname, Namenszusätze, Vorname, Identifikator, RZ-Benutzerkennung, Initialpasswort, Primärgruppe, Status des Accounts, Start- und Enddatum des Accounts, Gruppen mit Gruppenmitgliedern.

2.1.4 Art der Datenweitergabe und -verwendung

Datenfluss besteht hauptsächlich vom IdM-System in die OpenLDAP/Kerberos-Infrastruktur. Eine Ausnahme stellt hier das Passwort dar, das mit Microsoft Active Directory (siehe Abschnitt 2.2) synchronisiert wird. Änderungen in der OpenLDAP/Kerberos Infrastruktur werden nicht ins IdM-System übernommen. Grundsätzlich handelt es sich bei Neuanlage und Ablauf der Benutzerkonten von Beschäftigten, Studierenden und Gästen um automatisch ablaufende Prozesse. Nur im Ausnahmefall soll ein manueller Eingriff durch die Administratoren erfolgen. Die Ableitung der

Berechtigungen des Benutzerkontos erfolgt in den Endsystemen die an die OpenLDAP/Kerberos Infrastruktur angebunden sind (z.B. CMS, Digicampus, Studentenforum) anhand der Zugehörigkeit zu Gruppen.

Sofern für die an die OpenLDAP/Kerberos-Infrastruktur angebundenen Endsysteme eine Synchro–nisation der Benutzerkonten notwendig ist, werden diese von der Provisionierungsschicht über die Einrichtung und Löschung von Benutzerkonten explizit informiert.

2.2 Microsoft Active Directory des Rechenzentrums

2.2.1 Systembeschreibung

Das Microsoft Active Directory System des Rechenzentrums wird zur Authentifizierung und Autori-sierung von Windows Arbeitsplätzen und Windows Diensten genutzt. Der Basisdienst „Active Directory“ ermöglicht die Authentifizierung von Benutzerinnen/Benutzern und Computern gegenüber Windows Systemdiensten über die Active Directory Domäne „uni-augsburg.de“.

2.2.2 Ziele

Ziel und Hauptaufgabe des Microsoft Active Directory Systems ist die Bereitstellung des Zugangs zu allen Windows-Arbeitsplätzen und zu allen Windows-Diensten für Beschäftigte, Studierende und Gäste.

2.2.3 Benötigte Daten

Folgende Datenfelder werden aus dem IdM-Kern im Active Directory benötigt: Nachname, Namenszusätze, Vorname, Identifikator, RZ-Benutzerkennung, Initialpasswort, Primärgruppe, Status des Accounts, Start- und Enddatum des Accounts, Gruppen mit Gruppenmitgliedern.

2.2.4 Art der Datenweitergabe und -verwendung

Der Datenfluss besteht hauptsächlich vom IdM-System in das Active Directory. Eine Ausnahme stellt hier das Passwort dar, das mit der OpenLDAP/Kerberos-Infrastruktur (siehe Abschnitt 2.1) synchronisiert wird. Änderungen im Active Directory werden nicht ins IdM-System übernommen. Grundsätzlich handelt es sich bei Neuanlage und Ablauf der Benutzerkonten von Beschäftigten, Studierenden und Gästen um automatisch ablaufende Prozesse. Nur im Ausnahmefall soll ein manueller Eingriff durch die Administratoren erfolgen. Die Ableitung der Berechtigungen des Benutzerkontos erfolgt anhand der Zugehörigkeit zu Gruppen.

2.3 Karten-Management-System

2.3.1 Systembeschreibung

Das Karten-Management-System wird zur Speicherung der notwendigen Daten für die Campus Card Augsburg (CCA) für Studierende und Beschäftigte und zur Verwaltung der CCA (Erstausgabe, Ersatzausgabe, Sperrung) genutzt. Die Campus Card Augsburg ist eine multifunktionale Chipkarte für den Hochschulbereich Augsburg.

2.3.2 Ziele

Über das Karten-Management-System wird die Campus Card Augsburg für Studierende und Beschäftigte bereitgestellt.

2.3.3 Benötigte Daten

Folgende Datenfelder werden aus dem IdM-Kern im Karten-Management-System benötigt: Nachname, Namenszusätze, Vorname, Vorgestellte Titel, Geburtsdatum, Geschlecht, Identifikator,

Matrikelnummer, Datum der Exmatrikulation, Identnummer, Studienbeginn, Rückgemeldet bis, Mitarbeiterart, Vertragsbeginn, Vertragsende.

2.3.4 Art der Datenweitergabe und -verwendung

Der Datenfluss besteht vom IdM-System in das Karten-Management-System. Grundsätzlich handelt es sich bei Neuanlage und Modifizierung von Einträgen um automatisch ablaufende Prozesse. Nur im Ausnahmefall soll ein manueller Eingriff durch die Administratoren erfolgen. Über das KMS selbst werden keine personenbezogenen Daten zur Erstellung von personalisierten Chipkarten erfasst, geändert oder ergänzt, hierfür sind das Personalverwaltungssystem VIVA und das Studierendenverwaltungssystem HIS-SOS die einzigen autoritativen Quellen.

Anlage 3

zur

Dienstvereinbarung über die Einführung und den Betrieb des Identity Management Systems mit den daran angeschlossenen Quell- und Zielsystemen (nachfolgend als IdM-System bezeichnet)

Freigabeantrag
(Verfahrensbeschreibung nach Art. 26 Abs. 3 Satz 1 BayDSG)

Stand 22.02.2011
Maria Schmaus
Rechenzentrum
Universität Augsburg

Freigabeantrag
(Verfahrensbeschreibung nach Art. 26 Abs. 3 Satz 1 BayDSG)

Diese Beschreibung dient					
	der erstmaligen Beschreibung des Verfahrens				
x	der Änderung der Verfahrensbeschreibung vom:	02.04.2009	Aktenzeichen:	09/01	

Diese Beschreibung hat erstellt:	Maria Schmaus	am:	24.11.2009

Zu dieser Beschreibung erteilt nähere Auskunft:	Maria Schmaus		
Tel.:	0821/598-2041	E-Mail:	maria.schmaus@rz.uni-augsburg.de

1.	**Bezeichnung des Verfahrens und allgemeine Angaben**
1.1	Bezeichnung des Verfahrens
Betrieb eines universitätsweiten Identity-Management-Systems	
1.2	Dienststelle bzw. Dienststellen, in der bzw. in denen das Verfahren eingesetzt wird
Rechenzentrum	

2.	**Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung**
2.1	Aufgaben, zu deren Erfüllung die personenbezogenen Daten erhoben, verarbeitet oder genutzt werden

An der Universität Augsburg wird eine Vielzahl von personalisierten IT-Diensten (z.B. E-Mail, VPN, Web-Anwendungen) betrieben, zu denen die Nutzer (Angehörige und Gäste der Universität Augsburg) über eine persönliche Benutzerkennung und ein persönliches Passwort Zugang erhalten. Mit der Hilfe von Identity-Management-Systemen können die verschiedenen digitalen Identitäten der Nutzer dienste-übergreifend verwaltet werden. Im Idealfall ist einer realen Person nur noch eine einzige digitale Identität und damit ein einziges Paar aus Benutzername und Passwort zugeordnet.

Das Identity-Management-System hat also die Aufgabe, dass einer Person genau die IT-Dienste zur Verfügung stehen, für welche sie die Berechtigungen besitzt, und das nicht früher und nicht länger als sie der Universität angehört. Dies soll durch einen automatischen Mechanismus gewährleistet werden. Es wird hierzu nur ein absolutes Minimum an Daten gespeichert, nämlich genau die Daten, die zur (möglichst) eindeutigen Feststellung der Identität einer Person und damit der Zuweisung einer eindeutigen digitalen Identität benötigt werden. Außerdem werden zusätzlich diejenigen Daten gespeichert, die zur Gruppierung von Personen notwendig sind. Gruppen sind notwendig, um in den Endsystemen (z.B. Web-Anwendungen, Jura-Fachdatenbank) die Rollen- und Rechtevergabe regeln zu können.

2.2	Rechtsgrundlagen
Art. 15 I Nr. 2, II, III, 16 I, 17 I BayDSG	

3.	**Art der gespeicherten Daten**
Lfd. Nr.	Bezeichnung der Daten
1	Vorname(n)
2	Nachname
3	Vorgestellte Titel, z.B. Dr.
4	Namenszusätze, z.B. von, van der
5	Nachgestellte Titel, z.B. Ph.D.
6	Geburtsname
7	Geburtsdatum
8	Quellsystem (HIS-SOS, VIVA-PRO oder Gästeverwaltung)
9	Universell-eindeutige ID (intern generierter und zugewiesener Schlüssel)

10	Matrikelnummer
11	Datum der Immatrikulation
12	Datum der Exmatrikulation
13	Status (Rückmeldestatus des Studenten)
14	Angestrebter Abschluss
15	Fachkombination des Studiengangs (bzw. der Studiengänge)
16	Fachkennzeichen für Haupt-/Nebenfach
17	Fakultät
18	Fachsemester
19	Personalnummer
20	Mitarbeitertyp, z.B. Professor
21	Vertragsbeginn
22	Vertragsende
23	Beschäftigungsstelle(n)
24	Gäste-ID
25	Gaststatusbeginn
26	Gaststatusende
27	Zugeordnete Einrichtung
28	RZ-Benutzerkennung(en) mit Initialpasswort einer Person
29	Gruppen mit Gruppenmitgliedern (RZ-Benutzerkennungen und Gruppen)

4.	**Kreis der Betroffenen**
Alle Universitätsangehörigen; Gäste, die Zugang zu personalisierten IT-Diensten der Universität Augsburg benötigen	

5.	**Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung**
6 Monate nach Datum der Exmatrikulation, Vertragsende oder Gaststatusende	

6.	**Verarbeitungs- und nutzungsberechtigte Personengruppen**
- Identity-Management Administratoren: verarbeitungs- und nutzungsberechtigt auf allen Daten - DV-Betreuer: Nutzungsberechtigt auf folgenden Daten: RZ-Benutzerkennung, Vor- und Nachname, Namenszusätze, vor- und nachgestellte Titel, universell-eindeutige ID, Geburtsdatum, Matrikelnummer, Personalnummer, Initialpasswort, Gruppenzugehörigkeiten - Gruppenverwalter: verarbeitungs- und nutzungsberechtigt auf zugeordneten Gruppen und Gruppenmitgliedschaften; Nutzungsberechtigt auf folgenden Daten: RZ-Benutzerkennung, Vor- und Nachname, Namenszusätze, vor- und nachgestellte Titel, universell-eindeutige ID, Gruppenzugehörigkeiten - Betreuer und Benutzer der Endsysteme: nutzungsberechtigt auf folgenden Daten: RZ-Benutzerkennung, Vor- und Nachname, Namenszusätze, vor- und nachgestellte Titel, Gruppenzugehörigkeiten - Alle: Selbstauskunft ihrer eigenen gespeicherten Daten	

Von: Der Datenschutzbeauftragte der Universität Augsburg <datenschutzbeauftragter@uni-augsburg.de>
Betreff: Freigabe 09/01 - Änderung 1
Datum: Di, 24.11.2009, 18:20
An: "Maria Schmaus" <maria.schmaus@its.uni-augsburg.de>
Cc: "Markus Zahn" <markus.zahn@rz.uni-augsburg.de>

Sehr geehrte Frau Schmaus,

ich komme zurück auf Ihren Antrag vom 24.11.2009 und gebe hiermit das geänderte Verfahren "Betrieb eines universitätsweiten Identity-Management-Systems" gem. Art. 26 Abs. 1 S. 1 BayDSG wie aus der Anlage ersichtlich frei (Az. 09/01).

Mit freundlichen Grüßen

Ulrich M. Gassner
****
Prof. Dr. iur. Ulrich M. Gassner, Mag. rer. publ., M. Jur. (Oxon.)
Der Datenschutzbeauftragte der Universität Augsburg
Juristische Fakultät
Universitätsstr. 24
86159 Augsburg
Briefanschrift: 86135 Augsburg
Tel. (0821) 598-4600
(0821) 598-4590 (Sekr.)
Fax (0821) 598-4591
E-Mail datenschutzbeauftragter@uni-augsburg.de
Website www.uni-augsburg.de/einrichtungen/datenschutz