Karlsruhe Institute of Technology

Identitätsmanagement am KIT

Kurzbeschreibung (Stand: August 2009)

Dipl.-Inform. Thorsten Höllrigl
Dipl.-Inform. Sebastian Labitzke
Dipl.-Inform. Frank Schell
Dr.-Ing. Jochen Dinger
Dipl.-Inform. Axel Maurer
Prof. Dr. Hannes Hartenstein

STEINBUCH CENTRE FOR COMPUTING (SCC)

KIT – die Kooperation von
Forschungszentrum Karlsruhe GmbH
und Universität Karlsruhe (TH)

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft

Universität Karlsruhe (TH)
Forschungsuniversität • gegründet 1825

Inhaltsverzeichnis

Identitätsmanagement am KIT

Kurzbeschreibung (Stand: August 2009)

Das Projekt KIM-IDM[1] (Phase 2006 bis 2008) ist mit der Konzeption und technischen Realisierung eines zunächst Universitäts-weiten (später KIT-weiten) integrierten Identitäts- und Zugriffsmanagements betraut worden. Das vorgeschlagene Konzept verfolgt eine Ausgewogenheit zwischen zentralen und dezentralen Verfahren und betrachtet die Universität bzw. das Karlsruher Institut für Technologie (KIT)[2] als eine Föderation von Einrichtungen, in der Identitätsmanagementdienste im Rahmen einer Dienst-orientierten Architektur angeboten werden. Eines der hierbei verfolgten Ziele war es, eine Datenkonsistenz kongruenter personenbezogener Daten zu erreichen, ohne die Autarkie einzelner Einheiten einzuschränken. Zunächst wurde ein Identitätsmanagement, das sowohl Institutionen an der Universität als auch am Forschungszentrum (FZK) integriert, in Betrieb genommen und damit das Fundament für KIT-weite Diensterbringung gelegt.

In der vorliegenden Kurzbeschreibung wird in Ergänzung zur Dokumentation des Projekts KIM-IDM[1] die aktuelle Architektur und Konfiguration des Identitätsmanagementsystems am KIT zusammenfassend dargestellt und auf wesentliche Änderungen eingegangen, die seit dem Projektende im März 2009 durchgeführt wurden.

Zunächst wird im Abschnitt 1 ein Überblick über das verteilte Identitätsmanagementsystem gegeben. Im Abschnitt 2 wird anschließend näher auf die Provisionierungsprozesse[3] sowie die involvierten personenbezogenen Attribute eingegangen. Portal- und Infrastrukturdienste, die im Rahmen des Projektes implementiert wurden und in der Projektdokumentation ausführlich beschriebenen sind, werden in Abschnitt 3 skizziert. Wesentliche Änderungen, die sich seit dem Projektende ergeben haben, werden in Abschnitt 4 erläutert. Abschließend werden die Attribute

[1] T. Höllrigl, S. Labitzke, F. Schell, J. Dinger, A. Maurer und H. Hartenstein, KIM-Identitätsmanagement: Projektdokumentation, Technischer Bericht, SCC-TB-2009-1, Steinbuch Centre for Computing (SCC), 2009.

[2] Im Karlsruher Institut für Technologie (KIT) schließen sich das Forschungszentrum Karlsruhe (FZK) und die Universität Karlsruhe (TH) zusammen. Aufgrund ihrer geographischen Lage wird die Universität auch als Campus Süd und das Forschungszentrum als Campus Nord bezeichnet.

[3] Provisionierung beschreibt die Automatisierung aller Prozesse bezüglich der Erstellung, Verwaltung, Verteilung, Deaktivierung und Löschung digitaler Identitäten, sowie deren Attribute und Berechtigungen (Definition nach http://www.iam-wiki.org).

der angeschlossenen Systeme im Anhang A, Auslöser (engl. Trigger) für Provisionierungsprozesse sowie die resultierenden Datenflüssen im Anhang B in tabellarischer Form beschrieben.

1. Überblick über das Identitätsmanagementsystem am KIT

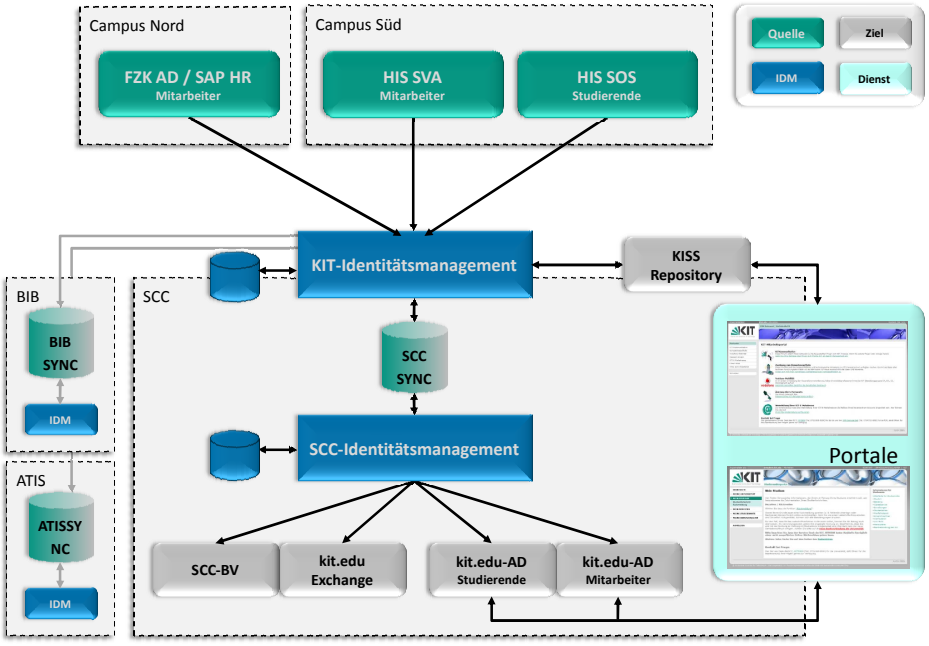

Abbildung 1.1: Überblick über das Identitätsmanagementsystem

Das realisierte Identitätsmanagementsystem am KIT und die angekoppelten Systeme sind in Abbildung 1.1 überblicksartig dargestellt. Die Systeme können dabei in Quell- und Zielsysteme eingeordnet werden. Die grau gezeichneten Verbindungen zur Bibliothek und zur ATIS (Abteilung Technische Infrastruktur der Fakultät für Informatik) deuten derzeit noch nicht produktiv geschaltete Verbindungen an.

1.1 Quellsysteme

Das KIT-weite Identitätsmanagementsystem (*KIT-IDM*), welches zentral skizziert ist, bezieht die Daten für Mitarbeiter des Campus Nord, Mitarbeiter des Campus Süd und Studierende aus jeweils einer eigenen Datenquelle. Diese drei Datenquellen sind autoritativ für jeweils eine dieser Nutzergruppen am KIT und werden tagesaktuell auf Änderungen überprüft.

Aus dem HIS-System werden die Daten der Mitarbeiter des Campus-Süd (*HIS-SVA*) und Studierendendaten (*HIS-SOS*) bezogen. Die Daten für Mitarbeiter des Campus Nord werden aktuell aus dem dortigen Active Directory (*FZK-AD*) bezogen. Das SAP-HR-System des Campus Nord wird in Zukunft das FZK-AD als autoritative Quelle ablösen. Dies wird derzeit vorbereitet und die Fertigstellung ist bis zum Ende des Jahres 2009 geplant.

Das KIT-IDM verteilt die Daten an die einzelnen Institutionen des KIT, die so genannten Satelliten. Hierzu wird das Produkt Sun Identity Manager eingesetzt. Im Folgenden wird detailliert auf die Anbindung der Quellressourcen und im Abschnitt 1.2 auf die einzelnen Zielsysteme eingegangen.

FZK-AD

Das FZK Active Directory (FZK-AD) dient als Quelle für die Mitarbeiter des Campus Nord. Es werden hier alle Benutzerkonten aus dem so genannten FZK-Forest synchronisiert, denen ein Postfach zugewiesen wurde. Der Export der Daten erfolgt über ein Skript, das eine .csv-Datei[1] anlegt, ein „Flatfile“. Diese Datei dient als Quelle für den Sun Identity Manager. Tabelle A.1 gibt eine Übersicht der Attribute der Datenquelle FZK-AD. In Anhang B.1 werden weiterhin die zugehörigen Provisionierungsprozesse benannt und tabellarisch dargestellt.

HIS-SVA

In der Ressource HIS-SVA werden die Identitätsdaten von Mitarbeitern der Universität Karlsruhe (TH) gepflegt. Der Sun Identity Manager hat keinen direkten Zugriff auf die HIS-SVA Datenbank der HIS-Software. Stattdessen wird ebenfalls regelmäßig ein Abzug der Datensätze in ein Flatfile erzeugt. Diese Datei dient wiederum als eigentliche Quelle für den Sun Identity Manager. In Tabelle A.2 bzw. Anhang B.2 werden die darin enthaltenen Attribute und die Provisionierung tabellarisch beschrieben.

HIS-SOS

Die Quelle für Studierendeninformationen ist die Datenbank HIS-SOS der Universitätsverwaltung. In diese Datenbank werden die Identitätsdaten von Studierenden nach deren Immatrikulation eingepflegt. Analog der Quelle HIS-SVA ist die Quelle

[1] Bei der .csv-Datei (Comma-Separated Values) handelt es sich um eine Datei, in welcher die Datensätze zeilenweise enthalten sind.

HIS-SOS über ein Flatfile angebunden, das die Universitätsverwaltung aus der HIS-SOS Datenbank extrahiert. Eine Übersicht der Attribute dieser Ressource und die Provisionierung bietet Tabelle A.3 und Anhang B.3.

Der Datenabgleich zwischen den Quellsystemen des FZK bzw. der Universitätsverwaltung per Flatfile erfolgt jeweils täglich. Die Übertragung der Datei bzw. die Datei selbst wird dabei gegen unbefugtes Mitlesen und Verändern durch Verschlüsselung geschützt.

1.2 Zielsysteme

Für jede Institution, respektive jeden Satelliten, ist eine ausgewiesene Datenbank als Schnittstelle zum KIT-IDM (*SYNC*) vorgesehen. Exemplarisch ist dies in Abbildung 1.1 für das am Steinbuch Centre for Computing (SCC) in diesem Jahr in Betrieb genommene Identitätsmanagementsystem (*SCC-IDM*) dargestellt. Das SCC-IDM wurde auf Basis der im Projekt KIM-IDM gewonnenen Erfahrungen konzipiert und implementiert.

Hierbei werden die vom KIT-IDM in der Schnittstelle des SCC, der Synchronisationsdatenbank (*SCC SYNC*), angelegten Nutzerdaten vom SCC-IDM ausgelesen, weiter verarbeitet, mit Daten angereichert (bspw. Unix-spezifischen Nutzerkontodaten) und in die am SCC-IDM angekoppelten Zielsysteme überführt. Weiterhin können vom SCC-IDM wiederum Daten, die über das KIT-IDM an Systeme anderer Institutionen bzw. Satelliten verteilt werden müssen, wie die *kit.edu*-E-Mail-Adresse, mittels der Synchronisationsdatenbank provisioniert werden. Demnach kann aus Sicht des KIT-IDM die SCC SYNC sowohl eine Quelle als auch ein Ziel für Identitätsdaten darstellen.

Ähnliche Entwicklungen können künftig zur Integration weiterer Satelliten wie der Abteilung Technische Infrastruktur (ATIS) und der KIT-Bibliothek (BIB) genutzt werden. Die Anbindung der Bibliothek befindet sich derzeit noch in der Planungsphase. Die Anbindung der ATIS mittels einer Synchronisationsdatenbank (*ATIS SYNC*) wurde bereits in einer Testumgebung erfolgreich umgesetzt.

Eine besondere Stellung nimmt die als KISS Repository[2] bezeichnete Datenbank ein. Das KISS Repository enthält Nutzerinformationen, die KIT-weite Prozesse ermöglichen, wie sie im Mitarbeiterportal[3] und Studierendenportal[4] bereits realisiert wurden.

Derzeit werden vom KIT-IDM die Daten für das SCC mit Hilfe der Synchronisationsdatenbank (*SCC SYNC*) abgeglichen und das KISS Repository mit den für die Portale benötigten personenbezogenen Daten versorgt. Die Provisionierung SCC-spezifischer Identitätsspeicher, wie zum Beispiel das *kit.edu*-Active Directory (kit.edu-AD), wurde an das SCC-IDM abgegeben. Diese Übergabe ist in dem

[2]KISS: KIM Identity Shared Services - Das KISS Repository stellt zum Beispiel die Hintergrunddatenbank für personenbezogene Daten für die Portale dar.

[3]Das Mitarbeiterportal ist unter https://intra.kit.edu erreichbar.

[4]Das Studierendenportal ist unter https://studium.kit.edu erreichbar.

Bestreben begründet eine logische Trennung zwischen Satelliten-Datenbanken wie dem Active Directory und den Satelliten-übergreifenden Prozessen zu schaffen. Ohne diese Trennung würde das Anbinden weiterer Satelliten an das KIT-IDM zu einer ungewollten Unübersichtlichkeit führen.

2. Provisionierungsprozesse

Der aktuelle Stand der implementierten Provisionierungsprozesse für die angekoppelten Quell- und Zielsysteme ist in Tabelle 2.1 als Übersicht dargestellt. Die Prozesse können wie folgt gegliedert werden:

- **Create (C)** – Falls in einer angekoppelten Ressource ein neuer Datensatz erkannt wird, bspw. ein neuer Eintrag in einer Datenbank, kann im Identitätsmanagementsystem ein Create-Prozess gestartet werden, der in den hierfür definierten Zielsystemen ein Nutzerkonto mit den entsprechenden Identitätsdaten und Rechten anlegt.
- **Update (U)** – Änderungen von Nutzerdaten in einem Quellsystem werden durch einen Update-Prozess behandelt. Dieser sorgt für die Aktualisierung dieser Daten basierend auf den im Identitätsmanagementsystem hinterlegten Regeln.
- **Disable (Di)** – Anstatt einen Nutzer sofort nach Erkennen eines Löschvorgangs in einem Quellsystems von allen Systemen zu entfernen, können zunächst in einem Disable-Prozess die Konten des Nutzers deaktiviert werden. Hierbei werden einem Nutzer Zugriffsrechte entzogen, ohne dass alle Daten gelöscht werden müssen. Das Auslösen eines Delete-Prozesses kann anschließend basierend auf Regeln wie dem Ablauf einer Frist durchgeführt werden.
- **Enable (E)** – Falls ein Nutzer durch einen Disable-Prozess deaktiviert wurde, kann mit Hilfe eines Enable-Prozesses der Nutzer wieder aktiviert werden, indem der Nutzer die entzogenen Rechte in den angekoppelten Systemen wieder zugewiesen bekommt.
- **Delete (D)** – Die Erkennung eines gelöschten Nutzers in einem Quellsystem kann auch zum sofortigen Löschen der entsprechenden Nutzerdaten in den angeschlossenen Systemen durch einen Delete-Prozess führen. Anschließend ist dem Identitätsmanagementsystem dieser Nutzer nicht mehr bekannt.

	Zielsysteme		
Quellsysteme	SCC	ATIS	KISS Repository
HIS-SOS	C,U,Di,E	U,Di,E,D	C,U,Di,E
HIS-SVA	C,U,Di,E	-	C,U,Di,E
FZK-AD	C,U,Di,E	-	C,U,Di,E
SCC	-	-	U
Portale (via SPML)	U	-	U
ATIS-IDM (via SPML)	-	C,U	-

Tabelle 2.1: Angekoppelte Quell- und Zielsysteme in KIT-IDM und implementierte Provisionierungsprozesse

So werden bspw. beim Erkennen einer Änderung eines Attributes im Quellsystem HIS-SOS entsprechend die Nutzerdaten in der SCC- und ATIS-Schnittstelle und im KISS Repository aktualisiert. Beim Anlegen eines Nutzers im FZK-AD wird ein Eintrag im KISS Repository angelegt und später mit der E-Mail-Adresse angereichert, die das SCC-IDM generiert und zurück in die Datenbank SCC SYNC schreibt. Das SCC-IDM führt darüber hinaus die Provisionierung des *kit.edu*-Active Directory und *kit.edu*-Exchange Servers durch.

Darüber hinaus steht mit einer SPML-Schnittstelle[1] eine standardisierte Möglichkeit zum Anstoßen von Prozessen zur Verfügung. Diese Schnittstelle wird vom Mitarbeiter- und Studierendenportal und vom Identitätsmanagementsystem der ATIS verwendet, um Prozesse im KIT-IDM auszulösen. Zur Wahrung der Nachweisbarkeit und Konsistenz werden bisher Nutzer nur automatisiert deaktiviert. Das Löschen der Daten ist technisch unproblematisch, jedoch bedarf es hierfür entsprechender organisatorischer Festlegungen.

Die vorgestellten Prozesse können jeweils grundsätzlich in zwei getrennte Phasen unterteilt werden. Zunächst können Bestätigungen (so genannte *Approvals*) von den zuständigen *Approver*, bspw. Managern oder Vorgesetzten, eingeholt werden, so dass für diese Person tatsächlich in den gewünschten Systemen ein Nutzerkonto mit entsprechenden Identitätsdaten und Rechten angelegt werden darf. Hierfür werden die Approver benachrichtigt, worauf diese sich im Identitätsmanagementsystem anmelden und den Approval akzeptieren oder ablehnen können. Diese Phase kann bspw.

[1]SPML (Service Provisioning Markup Language) dient dazu Provisionierungsaufgaben interoperabel zu gestalten sowie diese Standard-basiert integrieren zu können. Hierfür werden mit Hilfe von XML Nachrichtentypen und ein Protokoll zum Austausch dieser Nachrichten spezifiziert. Die Entwicklung von SPML wird durch das Standardisierungsgremium OASIS getrieben. Weitere Informationen zu SPML finden sich auf der OASIS-Website unter http://www.oasis-open.org/committees/provision.

durch die Berücksichtigung von Urlaubsvertretungen für die Approver komplexer gestaltet werden. Sie wird zurzeit jedoch in den Prozessen des KIT-weiten Identitätsmanagementsystems noch nicht implementiert. Die zweite Phase besteht in der eigentlichen Durchführung der Anlege-, Änderungs- und Lösch-Operation. Im Fehlerfall kann diese mehrmals Durchlaufen werden. Bei einer dauerhaften Störung sollte dementsprechend der Prozess angehalten werden, eine Lösung durch den Support des Zielsystems erfolgen und eine Wiederholung der fehlgeschlagenen Operationen durchgeführt werden.

Entscheidend für die korrekte Durchführung der Prozesse ist das Vorhandensein einer Abbildung der Informationsmodelle der angekoppelten Ressourcen. Hierfür werden in Identitätsmanagementsystemen Abbildungen zwischen den lokalen Nutzerattributen definiert. Solch eine Abbildung kann auch die Umwandlung eines Attributs in einen anderen Datentyp beinhalten. Die resultierenden Datenflüsse werden in den Tabellen B.3, B.6 und B.9 dargestellt.

3. Portal- und Infrastrukturdienste

Neben der Bereitstellung personenbezogener Daten für Nutzerkonten der einzelnen Satelliten und der Portale wurden im Projekt KIM-IDM verschiedene Portal- und Infrastrukturdienste entwickelt. Diese haben unmittelbaren Bezug zum Identitätsmanagement und sind daher im Folgenden aufgeführt und kurz erläutert. Eine detaillierte Beschreibung der nachgelagerten Prozesse findet sich in der Dokumentation[1] zum Projekt KIM-IDM.

3.1 Portaldienste

Mitarbeiterportal

Um ein Portal anbieten zu können, muss für dieses der Login-Prozess auf das darunter liegende IDM-System angepasst und auf die in den Nutzer-Sessions vorgehaltenen Attribute konfiguriert werden. Das Mitarbeiterportal authentifiziert Nutzer über einen Sharepoint Membership Provider, welcher wiederum die Nutzeridentität mittels eines so genannten LDAP-Bind zur LDAP-Schnittstelle des *kit.edu*-Active Directory überprüft. Mittels eines Role Provider werden personenbezogene Attribute beim Login-Vorgang aus dem KISS Repository in die entsprechende Sharepoint-Session geladen und Nutzerrollen sowie zugehörige Zugriffsrechte zugewiesen.

Bevor ein Mitarbeiter einen Portaldienst nutzen kann, muss er sich zunächst über den Aktivierungsdienst im Portal aktivieren. Diesem Dienst ist der Weiterleitungsdienst nachgelagert, den Mitarbeiter des Campus Süd zur Vervollständigung ihrer Aktivierung ebenfalls durchlaufen müssen. Der Aktivierungsdienst wird nach der ersten Anmeldung gestartet und verlangt zunächst die Eingabe des Geburtsdatums, das mit den Daten des Nutzers im System HIS-SVA verglichen wird. Stimmt dieses mit

[1] T. Höllrigl, S. Labitzke, F. Schell, J. Dinger, A. Maurer und H. Hartenstein, KIM-Identitätsmanagement: Projektdokumentation, Technischer Bericht, SCC-TB-2009-1, Steinbuch Centre for Computing (SCC), 2009.

dem gespeicherten Datum überein, muss der Nutzer sein per Brief erhaltenes Initial-Passwort ändern. Hat er auch diesen Schritt erfolgreich durchgeführt ist er aktiviert. Zur Nutzung der *kit.edu*-E-Mail-Adresse ist für Mitarbeiter des Campus Süd über den Weiterleitungsdienst noch das SCC-Nutzerkonto mit entsprechendem Passwort einzutragen. Hierdurch wird die Verknüpfung von Mitarbeiterdaten des Systems HIS-SVA und den Nutzerkonten des SCC ermöglicht. Alle auf die *kit.edu*-E-Mail-Adresse eingehenden E-Mails werden anschließend auf das hinterlegte Nutzerkonto weitergeleitet.

Der Passwortänderungsdienst erlaubt es das *kit.edu*-Passwort über das Mitarbeiterportal zu ändern. Dieser Dienst ist analog zum Aktivierungsdienst realisiert worden.

Ein E-Mail-Alias-Dienst gibt den KIT-Mitarbeitern die Möglichkeit, für die bereits eingerichtete kit.edu-E-Mail-Adresse einen E-Mail-Alias zu generieren und automatisiert freischalten zu lassen. Ein E-Mail-Alias ist eine weitere E-Mail-Adresse, die alle eingehenden E-Mails an die Haupt-E-Mail-Adresse weiterleitet. Als Namenskonvention für *kit.edu*-E-Mail-Aliase und -Adressen wurde mit Beschluss des KIT-Senatsausschusses IV-A eine Richtlinie zum Anlegen eingesetzt[2].

Um den Mitarbeitern die Möglichkeit zu geben sich in die Kompetenzbereiche und -felder des KIT einzuordnen, wurde der Kompetenzfeldzuordnungsdienst implementiert. Hier kann neben der Zuweisung von drei Kompetenzfeldern auch jenes ausgewählt werden, für das ein Mitarbeiter ein Wahlrecht wünscht.

Professoren und Mitarbeiter im Bereitschaftsdienst können durch eine Kooperation des KIT mit Vodafone ein mobiles Endgerät nebst entsprechender SIM-Karte erhalten. Um ein mobiles Endgerät zu bestellen, wurde der Vodafone-Beantragungsdienst eingerichtet und den entsprechend berechtigten Personen im Mitarbeiterportal angezeigt.

Studierendenportal

Ein Student führt die Aktivierung im Studierendenportal durch. Hierzu ist der Dienst zur Überprüfung der Nutzungsbedingungen implementiert worden. Akzeptiert ein (angehender) Studierender die Nutzungsbedingungen des SCC und ändert er anschließend sein Passwort über den nachgelagerten Passwortänderungsdienst, ist er für das Portal aktiviert und kann die dort angebotenen Dienste, wie zum Beispiel die Selbstbedienungs-Funktionalität nutzen. Mit der Einwilligung in die Nutzungsbedingungen wird auch ein Postfach im Exchange Server für den Studierenden freigeschaltet. Dieses Postfach wurde bereits bei der initialen Provisionierung mit einer E-Mail-Adresse mit dem Suffix „.local“ angelegt. Durch dieses Suffix können bis zur Aktivierung keine Dienste des Exchange Servers genutzt werden.

Der Passwortänderungsdienst dient auch im Studierendenportal als Möglichkeit das Passwort zu ändern.

[2]Details hierzu finden sich in der Projektdokumentation (vgl. Fn. 1).

3.2 Infrastrukturdienste

Infrastrukturdienste wurden im Projekt KIM-IDM als Web Services realisiert. Im Zuge der Nachhaltigkeitsarbeiten wurde die Anzahl der benötigten Web Services deutlich reduziert[3]. Dies begründet sich zum einen in der gewachsenen Komplexität und zum anderen den negativen betrieblichen Erfahrungen hinsichtlich Wartbarkeit und Robustheit, die sich durch die tiefe Verschachtelung der Web Services ergeben haben.

Für die Portaldienste und das Identitätsmanagement sind im Wesentlichen nun vier Dienste notwendig. Davon ist ein Web Service eine JAVA Implementierung zur Kommunikation mit der SPML-Schnittstelle des SUN Identity Managers. Hierüber werden zum Beispiel die Updates der Passwörter eingespielt. Das Portal ruft dazu die Passwort-Update Funktion des in C#.NET implementierten *Coreset Service* auf, der seinerseits den JAVA-Web Services des KIT-IDM-System anstößt. Außerdem können vom Portal über den Coreset Service die Attribute des KISS Repository ausgelesen werden. Attribute der Verwaltung können über den *Administration Attribute Service* und die des SCC über den Service *SCC Attribute Service* abgefragt werden.

Neben den Infrastrukturdiensten für die Portaldienste soll der Authentifikations- und Attributlieferungsdienst *Shibboleth* Anwendern von KIT-Diensten künftig eine zentrale Authentifikationsmöglichkeit und Möglichkeit zum Single Sign-On zwischen einzelnen Diensten bieten. Hierzu wurden bereits entsprechende Systeme aufgesetzt, die um das im Hauptdokument beschriebene und prototypisch umgesetzte KIT-AuthN-Modul erweitert wurden. Dieses Modul ermöglicht den Zugriff auf mehrere Datenbanken mit Nutzerkonten im Backend des Shibboleth Identity Provider. Zudem stößt das Modul beim ersten Login eines Nutzers einen Provisionierungsprozess im SUN Identity Manager an, um die Shibboleth Attributdatenbank mit Nutzeratributen zu füllen. Diese Datenbank dient der Shibboleth Attributlieferung für dafür freigeschaltete Dienste.

Außerdem soll die Shibboleth-Installation nach erfolgter Produktivschaltung in die Föderation DFN-AAI des Deutschen Forschungsnetzes (DFN) aufgenommen werden. Mitarbeiter und Studierende des KIT können dann mit Hilfe ihres KIT-Nutzerkontos Dienste anderer Hochschulen in Deutschland nutzen. Ebenso können Mitglieder anderer Hochschulen auf geschützte Dienste des KIT zugreifen. Dies wird durch eine Vertrauensstellung zwischen der DFN-AAI und dem KIT-Identity Provider erreicht. Nach einer erfolgreichen Authentifikation kann den Diensten sodann auch Zugriff auf benötigte Attribute gewährt werden.

[3]Eine Beschreibung der ursprünglich genutzten Web Services findet dich in der Projektdokumentation (vgl. Fn. 1).

4. Anpassungen des Identitätsmanagement am KIT

Im Vergleich zur Dokumentation[1] des Projektes KIM-IDM hat sich das Identitätsmanagement am KIT weiterentwickelt. Dabei haben sich insbesondere aus betrieblichen Gründen Änderungen ergeben, die im Folgenden aufgelistet sind. Des Weiteren wird die Entwicklung der Shibboleth-Infrastruktur sowie die Anbindung des SAP-HR-Systems des Campus Nord voran getrieben.

- Im Zuge der Nachhaltigkeitsarbeiten des Projektes KIM-IDM wurde die Provisionierung von Datenquellen, deren Verantwortung und Betreuung innerhalb der Domäne des SCC liegen, zum SCC-Identitätsmanagementsystem (SCC-IDM) portiert. Das SCC-IDM versorgt nun neben der SCC-Benutzerverwaltung auch das *kit.edu*-Active Directory sowie die Exchange Server mit Daten. Die Migration wurde im August 2009 abgeschlossen. Das KIT-IDM provisioniert derzeit die Synchronisationsdatenbank SCC SYNC als Schnittstelle zum SCC und das KISS Repository als Datenquelle für die Portale. Eine entsprechende Übersicht findet sich in Abschnitt 1. Durch die Anpassungen ist das KIT-IDM von Satelliten-spezifischen Provisionierungsprozessen befreit, so dass sich die Anbindung von neuen Satelliten, d.h. neuen Organisationseinheiten, nun noch effizienter durchführen lässt. Ein solcher Satellit ist bspw. die bereits testweise angebundene ATIS.

- Auch die Infrastrukturdienste wurden neu strukturiert und gebündelt, so dass die Anzahl der Web Services deutlich reduziert werden konnte (vgl. auch Abschnitt 3.2). Nunmehr sind drei Web Services implementiert, die Daten aus dem SCC, der Universitätsverwaltung und dem KISS Repository abrufen können. Für jeden weiteren anzubindenden Satelliten kann in der nächsten Ent-

[1] T. Höllrigl, S. Labitzke, F. Schell, J. Dinger, A. Maurer und H. Hartenstein, KIM-Identitätsmanagement: Projektdokumentation, Technischer Bericht, SCC-TB-2009-1, Steinbuch Centre for Computing (SCC), 2009.

wicklungsphase bei Bedarf ein Web Service hinzu implementiert werden. Ein weiterer Web Services kapselt den SUN Identity Manager über dessen SPML Schnittstelle.

- Für die Shibboleth-Infrastruktur des KIT wurde ein speziell auf die Bedürfnisse des KIT angepasstes Authentifikationsmodul entworfen und prototypisch umgesetzt (vgl. Abschnitt 3.2). Dieses Modul erlaubt die Anbindung von mehr als einer Datenquelle für Nutzerkonten sowie eine „Live-Provisionierung“ von Attributen in die dafür vorgesehene Shibboleth-Datenbank. Ein produktiver Betrieb der Shibboleth-Infrastruktur ist noch für das Jahr 2009 vorgesehen.

- Derzeit befindet sich der Austausch der autoritativen Quelle für Mitarbeiter des Campus Nord in Planung. Dabei soll das FZK-Active Directory gegen das SAP-HR-System ausgetauscht werden. Ziel ist es, die Planungs- sowie die anschließende Entwicklungsphase bis zum Jahresende 2009 zu vollenden.

A. Attribute angeschlossener Systeme

In den nachfolgenden Tabellen werden die Attribute der folgenden autoritativen Datenquellen beschrieben:

- FZK-AD in Tabelle A.1 (Mitarbeiter des Campus Nord)
- HIS-SVA in Tabelle A.2 (Mitarbeiter des Campus Süd)
- HIS-SOS in Tabelle A.3 (Studierende)

Des Weiteren werden tabellarisch auch die Attribute der Zielsysteme präsentiert:

- Attribute der Ressource KISS Repository in Tabelle A.4 (Mitarbeiter)
- Attribute der Ressource KISS Repository in Tabelle A.5 (Studierende)
- Attribute der Ressource SCC SYNC in Tabelle A.6 (Mitarbeiter)
- Attribute der Ressource SCC SYNC in Tabelle A.7 (Studierende)

Attribut	Beschreibung	Beispiel
Distinguished Name	Distinguished Name (DN) eines Mitarbeiters	cn=Schell,...,dc=de
Nachname	Nachname eines Mitarbeiters	Schell
Vorname	Vorname eines Mitarbeiters	Hans
Telefonnummer	Telefonnummer eines Mitarbeiters	8000
DisplayName	Vornamen und Nachnamen eines Mitarbeiters zur Darstellung in Applikationen	Schell, Hans
ObjectSid	Eindeutiger Active Directory-Schlüssel eines Mitarbeiters	010...ab2000
SAMAccountName	Bisherhiger SAMAccountName eines Mitarbeiters	hans.schell
UserPrincipalName	Bisherhiger UserPrincipalName eines Mitarbeiters	hans.schell@ iai.fzk.de
E-Mail	Bisherige E-Mail-Adresse eines Mitarbeiters	hans.schell@ extern.fzk.de
OE	Organisationseinheit	SCC
Unix-Informationen	Abbildung der Unix-Attribute der Domänen ka.fzk.de und irs.fzk.de (msSFU30UidNumber, msSFU30GidNumber und msSFU30LoginShell)	/bin/ksh

Tabelle A.1: Attribute der Ressource FZK-Active Directory (FZK-AD)

Attribut	Beschreibung	Beispiel
SVA-Identifikator	Identifikator eines Mitarbeiters an der Universität Karlsruhe (TH)	123456
Geschlecht	Geschlecht eines Mitarbeiters	M
Anrede	Anrede eines Mitarbeiters	Prof.Dr.-Ing.
Vorname	Alle Vornamen eines Mitarbeiters	Hans Joachim
Nachname	Alle Nachnamen eines Mitarbeiters, auch Adelstitel	Muster
Instituts-Nummer	Nummer des Instituts, an dem ein Mitarbeiter beschäftigt ist	12312312
Adress-informationen	Adresse des Instituts oder der Einrichtung, in der der Mitarbeiter beschäftigt ist	Steinbuch Centre for Computing
Kostenstelle	Kostenstelle eines Mitarbeiters	12345678

Tabelle A.2: Attribute der Ressource HIS-SVA

Attribut	Beschreibung	Beispiel
Matrikelnummer	Identifikator eines Studierenden an der Universität Karlsruhe (TH)	1188888
Geschlecht	Geschlecht eines Studierenden	männlich
Vorname	Alle Vornamen eines Studierenden	Hans Joachim
Nachname	Alle Nachnamen eines Studierenden, auch Adelstitel	Muster
Studienfach	Studienfach eines Studierenden	1
Status	Beschreibt den aktuellen Zustand eines Studierenden an der Universität. Ein Studierender der sich nicht (mehr) im Flatfile des HIS-SOS befindet, gilt als exmatrikuliert. Es gibt hierbei keine Verzögerung seitens der Verwaltung. Mögliche Werte sind: Beurlaubung, Ersteinschreibung, Neueinschreibung, Rückmeldung	Rückmeldung
Straße	Straße inklusive Hausnummer der Postadresse eines Studierenden	Zirkel 2
Postleitzahl	Postleitzahl des Wohnsitzes	76128
Stadt	Ortsnamen des Wohnsitzes	Karlsruhe
Land	Länderkennung des Wohnsitzes	D
Adressnachtrag	Zusätzliche Informationen zur postalischen Adresse	K1 E201
Fricard-ID	Intern gespeicherte Nummer der FriCard eines Studierenden	1234567890
Fricardchip-ID	Aufgedruckte Nummer der FriCard eines Studierenden	158001188888

Tabelle A.3: Attribute der Ressource HIS-SOS

Attribut	**Beschreibung**	**Beispiel**
userid	Primary Key für das Mapping des KIT-IdM	0AA63508-604A-7214-B1E8-3F9809CF911E
firstname	Kontrollattribut für SCC-Support. Portalfunktionen benötigen Vorname, z.B. Generierung der E-Mail-Aliase.	Julia Sandra
lastname	Kontrollattribut für SCC-Support. Portalfunktionen benötigen Nachname, z.B. Generierung der E-Mail-Aliase.	Muster
email	Portalanmeldung und Portaldienste nutzen dieses Attribut als userPrincipalName	julia.muster@kit.edu
rzemail	Mapping der *kit.edu*-E-Mail-Adresse auf das bestehende E-Mail-Konto des SCC, freiwillige Angabe	xx01@rz.uni-karlsruhe.de
rzoldpassword	Systempasswort um initial die Verknüpfung mit den Attributen email und rzemail herzustellen; kein Nutzerpasswort	a-Gdg2/
status	Anhand dieses Attributs wird entschieden, was einem Mitarbeiter im Portal angezeigt wird.	created, activated, forwarding completed, deactivated
username	Alternativer Login, um eine Anmeldung ohne Angabe der E-Mail-Adresse zu ermöglichen.	xx0007
isactivated	Statusinformation für das KIT-IDM und die Portale	true, false
isrznew	Ein Mitarbeiter, der ein neues Nutzerkonto erhält, aber bereits ein Altes hat, kann die Konten verknüpfen. Das Ergebnis der Entscheidung spiegelt sich hier wider.	true, false
localidentifier1	Schlüssel zum HIS-SVA für Portale. Dies wird für Attribute genutzt, die nicht persistent provisioniert werden.	654321
localidentifier2	KIT-IDM benutzt diesen Wert als Schlüssel zur Quelle SCC / Einrichtung der Weiterleitung von *kit.edu*- auf SCC-E-Mail-Adresse	xx01
localidentifier3	Schlüssel zur Quelle FZK-AD für KIT-IDM	julia.muster@xy.fzk.de
dateofcreation	Statusinformation für KIT-IDM	12.02.2008 17:09
dateofdeletion	Statusinformation für KIT-IDM	24.05.2009

Tabelle A.4: Attribute der Ressource KISS Repository (Mitarbeiter)

Attribut	**Beschreibung**	**Beispiel**
id_kit	Portalanmeldung und Portaldienste nutzen id_kit als UPN für Login und Benachrichtigung.	julia.muster@ student.kit.edu
id_zuv	Schlüssel zum HIS-SOS für Portale. Dies wird für Attribute genutzt, die nicht persistent provisioniert werden, und für die Selbstbedienungsfunktionalität der Verwaltung.	1188888
id_scc	Alternativer Login, um eine Anmeldung ohne Angabe der E-Mail-Adresse zu ermöglichen.	uxyz
Guid	Primary Key für das Mapping des KIT-IDM	0AA63508-604A-7214-B1E8-3F9809CF911E
date_created	Statusinformation für KIT-IDM	12.02.2008 17:09
date_deleted	Statusinformation für KIT-IDM	24.05.2009

Tabelle A.5: Attribute der Ressource KISS Repository (Studierende)

Attribut	**Beschreibung**	**Beispiel**
sex	Geschlecht	W
firstname	Vorname	Julia Sandra
lastname	Nachname	Muster
username	KIM Login	xx0001
email	*kit.edu*-E-Mail-Adresse	julia.muster@kit.edu
campus	Campuszugehörigkeit	NORD / SUED
fzk_distin guishedname	Distinguished Name im FZK-AD	CN=Schell,...,DC=de
fzk_email	FZK-E-Mail-Adresse	julia.muster@ iwr.fzk.de
fzk_userprin cipalname	FZK-UserPrincipalName	muster@ka.fzk.de
fzk_objectsid	Schlüssel zum FZK-AD	X'01050000...3a0000'
fzk_physical delivery officename	FZK-Organisationseinheit	IWR
fzk_sam accountname	sAMAccountname FZK-AD	muster
fzk_telefon	Telefonnummer im Campus Nord	1234
uni_kostenstelle	Kostenstelle	12345678
uni_orgeinheit	Organisationseinheit	12312312
status	Synchronisationsstatus zwischen KIT-IdM und BV	KIT-IDM:Forwarding abgeschlossen/ SCC-IDM:zugeordnet
created_by	Create-Auslöser	kimidm
created_at	Create-Datum	06.07.2009 15:32
modified_by	Auslöser der letzten Modifikation	dbo
modifiedat	Datum der letzten Modifikation	13.08.2009 13:07
uni_adresse1	Institutsadressdaten für Uni-Mitarbeiter	Steinbuch Centre for Computing (ehem. RZ)
uni_adresse2	Institutsadressdaten für Uni-Mitarbeiter	Geb. 20.21
uni_adresse3	Institutsadressdaten für Uni-Mitarbeiter	
uni_adresse4	Institutsadressdaten für Uni-Mitarbeiter	
scc_id	ID im SCC	ka888
kit_employee_id	E-Mail-Präfix	julia.muster
guid	GUID des KIT-IdM	0AA63508-604A-7214-B1E8-3F9809CF911E

Tabelle A.6: Attribute der Ressource SCC SYNC (Mitarbeiter)

Attribut	**Beschreibung**	**Beispiel**
guid	KIM-GUID (Globally Unique Identifier)	0AA63508-604A-7214-B1E8-3F9809CF911E
firstname	Vorname	Julia Sandra
lastname	Nachname	Muster
sex	Geschlecht	W
courseof studiesnumber	Studienrichtung	10
zuv_status	Rückmeldestatus	Rückmeldung
id_zuv	Matrikelnummer	1188888
id_scc	SCC-Login	uxxx
id_kit	*kit.edu*-E-Mail-Adresse	julia.muster@ student.kit.edu
id_fricard	FriCard-Nummer	1234567890
id_fricardchip	FriCard-Chipkey	158001188888
created_by	Create-Auslöser	kimidm
created_at	Create-Datum	06.07.2009 15:32
modified_by	Auslöser der letzten Modifikation	dbo
modifiedat	Datum der letzten Modifikation	13.08.2009 13:07
street	Straße	Musterstraße 26
postcode	PLZ	76131
city	Ort	Karlsruhe
country	Land	D
address supplement	Adresszusatz	App.123
accepted termsofuse	Datum der Bestätigung der Nutzungsbedingungen	22.08.2009 14:04:32
briefgesendet	Datum des Briefversandes mit Initialpasswort für *kit.edu*-Nutzerkonto	22.08.2009 16:27:15

Tabelle A.7: Attribute der Ressource SCC SYNC (Studierende)

B. Provisionierung personenbezogener Daten

B.1 Provisionierung der Mitarbeiter des Campus Nord

Proxy User	FZK Synchronizer
Synchronizer Form:	KIM FZK Synchronizer Form
ActiveSync Form:	KIM FFAS FZK Active Sync Form
Correlation Rule:	<Match ObjectSid>
PrePoll:	KIM FFAS-FZK Pre-Poll WF

Tabelle B.1: Konfiguration der Provisionierung der Mitarbeiter des Campus Nord im SUN Identity Manager

FFAS diffaction	Create		Update		Delete
CR.feedop	Create	Update	Create	Update	*
Trigger	Create (C)	Enable (E)	Create (C)	Update (U)	Disable (D)
Workflow	KIM FFAS-FZK Create User	KIM FFAS-FZK Enable User	KIM FFAS-FZK Create User	KIM FFAS-FZK Udate User	KIM FFAS-FZK Disable User

Tabelle B.2: Auslöser (engl. Trigger) für die Provisionierung der Mitarbeiter des Campus Nord im SUN Identity Manager

Ziel	**Zielattribut**	**Trigger**	**Quellsystem**
IDM	accountId	C	IDM
	roles	C	IDM
KISS Repository	userid	C	IDM
	firstname	C,U	FZK-AD
	lastname	C,U	FZK-AD
	email	C,U	SCC-IDM
	status	C,U	IDM/Portal
	username	C	SCC-IDM
	localidentifier3	C	FZK-AD
	Dateofcreation	C	IDM
	Dateofdeletion	D,E	IDM
SCC SYNC	guid	C	IDM
	sex	C,U	FZK-AD
	firstname	C,U	FZK-AD
	lastname	C,U	FZK-AD
	kit_email	C,U	SCC-IDM
	campus	C	IDM
	fzk_distinguishedname	C,U	FZK-AD
	fzk_email	C,U	IDM
	fzk_userprincipalname	C,U	FZK-AD
	fzk_objectsid	C	FZK-AD
	fzk_telefon	C,U	FZK-AD
	fzk_physicaldelivery officename	C,U	FZK-AD
	fzk_samaccountname	C,U	FZK-AD
	status	C,U	IDM, SCC-IDM
	created_by	C	IDM, SCC-IDM
	created_at	C	IDM, SCC-IDM
	modified_by	C,U	IDM, SCC-IDM
	modifiedat	C,U	IDM, SCC-IDM
	kit_employee_id	C,U	SCC-IDM

Tabelle B.3: Datenflüsse bei der Provisionierung der Mitarbeiter des Campus Nord

B.2 Provisionierung der Mitarbeiter des Campus Süd

Proxy User:	UKA Synchronizer
Synchronizer Form:	KIM SVA Synchronizer Form
ActiveSync Form:	KIM FFAS SVA Active Sync Form
Correlation Rule:	<Match SVAID>
PrePoll:	KIM FFAS-UKA Pre-Poll WF

Tabelle B.4: Konfiguration der Provisionierung der Mitarbeiter des Campus Süd im SUN Identity Manager

FFAS diffaction	Create		Update		Delete
CR.feedop	Create	Update	Create	Update	*
Trigger	Create (C)	Enable (E)	Create (C)	Update (U)	Disable (D)
Workflow	KIM FFAS-SVA Create User	KIM FFAS-SVA Enable User	KIM FFAS-SVA Create User	KIM FFAS-SVA Udate User	KIM FFAS-SVA Disable User

Tabelle B.5: Auslöser (engl. Trigger) für die Provisionierung der Mitarbeiter des Campus Süd im SUN Identity Manager

Ziel	Zielattribut	Trigger	Quellsystem
IDM	accountId	C	IDM
	roles	C	IDM
KISS Repository	userid	C	IDM
	firstname	C,U	HIS-SVA
	lastname	C,U	HIS-SVA
	email	C,U	SCC-IDM
	rzemail	C,U	Portal
	rzoldpassword	C,U	SCC-IDM
	status	C,U	IDM/Portal
	username	C	IDM
	isactivated	C,U	IDM/Portal
	isrznew	U	SCC-IDM/Portal
	localidentifier1	C	HIS-SVA
	localidentifier2	C,U	SCC-IDM/Portal
	Dateofcreation	C	IDM
	Dateofdeletion	D,E	IDM
SCC SYNC	guid	C	IDM
	sex	C,U	HIS-SVA
	firstname	C,U	HIS-SVA
	lastname	C,U	HIS-SVA
	kim_login	C	SCC-IDM
	campus	C	IDM
	uni_kostenstelle	C,U	HIS-SVA
	uni_orgeinheit	C,U	HIS-SVA
	status	C	IDM, SCC-IDM
	created_by	C	IDM, SCC-IDM
	created_at	C	IDM, SCC-IDM
	modified_by	C,U	IDM, SCC-IDM
	modifiedat	C,U	IDM, SCC-IDM
	uni_adresse1	C,U	HIS-SVA
	uni_adresse2	C,U	HIS-SVA
	uni_adresse3	C,U	HIS-SVA
	uni_adresse4	C,U	HIS-SVA
	uni_bvinitial	C,U	SCC-IDM
	scc_id	C,U	SCC-IDM

Tabelle B.6: Datenflüsse bei der Provisionierung der Mitarbeiter des Campus Süd

B.3 Provisionierung der Studierenden

Provisionierung der Studierenden

Proxy User:	CS Student Sync
Synchronizer Form:	KIM Synchronizer Campus Sued Studierende User Form
ActiveSync Form:	KIM FFAS-Campus Sued Studierende Active Sync Form
Correlation Rule:	<Match accountId (mtknr)>
PrePoll:	KIM FFAS-Campus Sued Studierende Pre-Poll WF

Tabelle B.7: Konfiguration der Provisionierung der Studierenden im SUN Identity Manager

FFAS diffaction	Create		Update		Delete
CR.feedop	Create	Update	Create	Update	*
Trigger	Create (C)	Enable (E)	Create (C)	Update (U)	Disable (D)
Workflow	KIM FFAS-SOS Create User	KIM FFAS-SOS Enable User	KIM FFAS-SOS Create User	KIM FFAS-SOS Udate User	KIM FFAS-SOS Disable User

Tabelle B.8: Auslöser (engl. Trigger) für die Provisionierung der Studierenden im SUN Identity Manager

Ziel	Zielattribut	Trigger	Quellsystem
IDM	accountId	C	IDM
	roles	C	IDM
KISS Repository	date_created	C	IDM
	date_deleted	D,E	IDM
	id_kit	C,U	SCC-IDM
	id_zuv	C	HIS-SOS
	id_rz	C,U	SCC-IDM
	guid	C	IDM
SCC SYNC	guid	C	IDM
	sex	C,U	HIS-SOS
	firstname	C,U	HIS-SOS
	lastname	C,U	HIS-SOS
	courseofstudiesnumber	C,U	HIS-SOS
	zuv_status	C,U	HIS-SOS
	id_zuv	C	HIS-SOS
	id_scc	C,U	SCC-IDM
	id_kit	C,U	SCC-IDM
	id_fricard	C,U	HIS-SOS
	id_fricardchip	C,U	HIS-SOS
	created_by	C	IDM, SCC-IDM
	created_at	C	IDM, SCC-IDM
	modified_by	C,U	IDM, SCC-IDM
	modifiedat	C,U	IDM, SCC-IDM
	street	C,U	HIS-SOS
	postcode	C,U	HIS-SOS
	city	C,U	HIS-SOS
	country	C,U	HIS-SOS
	addresssupplement	C,U	HIS-SOS
	acceptedtermsofuse	C,U	SCC-IDM/ Studierendenportal
	briefgesendet	C	SCC-IDM

Tabelle B.9: Datenflüsse bei der Provisionierung von Studierenden

C. Impressum

Projektleitung	Prof. Dr. Hannes Hartenstein
Projektmanagement	Dipl.-Inform. Axel Maurer
Projekt	KIM - Karlsruher Integriertes InformationsManagement http://www.kim.uni-karlsruhe.de/
Teilprojekt	KIM - Identitätsmanagement (KIM-IDM)
Autoren	Dipl.-Inform. Thorsten Höllrigl Dipl.-Inform. Sebastian Labitzke Dipl.-Inform. Frank Schell Dr.-Ing. Jochen Dinger Dipl.-Inform. Axel Maurer Prof. Dr. Hannes Hartenstein
Veröffentlichung	August 2009
Fotobasis Titelgrafik	© 2008 stormpic / aboutpixel.de / Motiv: „e-mail“

Die Wiederverwendung dieser Dokumentation oder von Teilen daraus bedarf der Angabe untenstehender oder entsprechender Referenz. Alle Rechte vorbehalten.


```
@TECHREPORT{KIM-IDM09,
  author = {Thorsten Höllrigl and Sebastian Labitzke and Frank Schell
            and Jochen Dinger and Axel Maurer and Hannes Hartenstein},
  title = {Identitätsmanagement am KIT -
            Kurzbeschreibung (Stand: August 2009)},
  institution = {Steinbuch Centre for Computing (SCC)},
  year = {2009},
  month = {August}
}
```

Steinbuch Centre for Computing (SCC)
76128 Karlsruhe
Tel: 0721/608-3754 oder 07247/82-5601

E-Mail scc@kit.edu

SCC-TB-2009-2