Der Weg von BYOE zum GYSE

Christopher Ritter, Patrick Bittner, Odej Kao

tubIT – IT-Service-Center der TU-Berlin
Technische Universität Berlin
Einsteinufer 17
10587 Berlin
christopher.ritter@tu-berlin.de
patrick.bittner@tu-berlin.de
odej.kao@tu-berlin.de

Abstract: Mit der zunehmenden IT-Unterstützung von Studium und Lehre unterliegen die Universitätsrechenzentren einem Paradigmenwechsel hin zum IT-Service-Center. Das Angebot an IT-Diensten und digitalen Medien im Bereich des Studiums unterliegt derzeit einem stetigen Wachstum. Durch BYOD (Bring Your Own Device) wurde dieser Wandel noch beschleunigt. Mit dem derzeitigen Umstieg von BYOD zum BYOE (Bring Your Own Environment) führt die Vielzahl an neuen IT-Diensten aber nicht nur zu einer Erleichterung für die Studierenden. Viele der Digital Natives verfügen zum Zeitpunkt der Immatrikulation nicht nur über eigene IT-Ausstattung, sondern haben auf dieser bereits alle von ihnen benötigen Dienste installiert und konfiguriert. Die Realisierung eines zentralen, umfassenden Identitätsmanagementsystems und der damit verbundenen Unterstützung von Single Logon und Single SignOn ermöglicht zwar die Nutzung der Dienste mit einer einzigen Benutzerkennung, in der existierenden Infrastruktur werden weitere, meist bereits in anderer Form vorhandene Dienste aber häufig als störend empfunden. Einige für das Studium benötigte Anwendungen sind unter Umständen nicht mit der vorhandenen Konfiguration kompatibel oder führen gar zu Störungen der gewohnten Umgebung. Die Erwartung an die IT der Universität ist, neben der Integration der eigenen, bestehenden IT-Umgebung in die von der Universität bereitgestellten Systeme für Studium und Verwaltung, unabhängig vom Provider oder der spezifischer Ausprägung, daher auch die Möglichkeit eine auf ihr Studium abgestimmte Umgebung auf ihren Geräten nutzen zu können.

Diese Aufgabe ist von den Universitäten zu leisten, erfordert jedoch ein frühzeitiges Umdenken und Flexibilität an der zentralen Stelle des Campus Management: bei den Systemen für Identity und Service Management. Diese müssen BYOE bereits bei der Provisionierung unterstützen und als Normalfall betrachten. Darüber hinaus müssen die für das Studium des Studierenden angebotenen Anwendungen und Medien gebündelt und als eine Umgebung zur Verfügung gestellt werden können.

In dem folgenden Beitrag wird ein System beschrieben, das als erster Ansatz zur Lösung der identifizierten Probleme dienen soll. Ausgehend von der nahtlosen

Erfassung aller Mitglieder der Universität und deren aktueller Kontexte, wird eine Arbeitsumgebung generiert, die sowohl bezogen auf enthaltene Dienste als auch auf die zur Verfügung stehenden Inhalte explizit auf die Bedürfnisse des Studierenden angepasst ist. Der aktuelle Stand der Entwicklung umfasst bisher eine Basisplattform mit entsprechender Grundfunktionalität, die in weiteren Iterationen sukzessive ausgebaut werden muss.

1 Einleitung

Während die Generationen vor den Digital Natives zum Zeitpunkt der Immatrikulation nur teilweise über eine eigene IT-Ausstattung (sowohl Hardware als auch Dienste) verfügten und folgerichtig von der Universität die Bereitstellung aller notwendigen IT-Komponenten für ein erfolgreiches Studium (E-Mail, Speicher, Webseite, WLAN, Verwaltungssysteme, ...) erwarteten, änderte sich diese Anforderung zunächst mit dem Aufkommen von BYOD (Bring Your Own Device).

Mit stark wachsender Zahl begannen die Studierenden bereits mit ihrer eigenen Hardware ihr Studium. Mittlerweile erleben die Universitäten den Umstieg vom BYOD zum BYOE (Bring Your Own Environment). Die aktuellen Generationen kommen komplett ausgestattet an die Universität. Dies betrifft nicht mehr nur bereits vorhandene Hardware, sondern auch eine vollständige Infrastruktur an Diensten inkl. vorhandener E-Mailkonten und mehreren Konten in sozialen Netzwerken.

Diese Ausstattung wird in Teilen bereits vor dem Studium vorausgesetzt, da schon der erste Schritt – die Onlinebewerbung um einen Studienplatz – eine funktionierende IT-Umgebung voraussetzt. Die zahlreichen frei verfügbaren IT-Dienste sowie der deutlich frühere Einstieg in die elektronische Kommunikation als vor Jahren üblich, führen dazu, dass die Studierenden gar keine neue – universitäre – IT-Umgebung haben wollen, die ihre alte Umgebung ersetzt. Sie sehen ihre eigene IT-Umgebung als lebenslang begleitend, die auch nach den 5-6 Jahren Universitätsaufenthalt bestehen bleiben wird. Häufig werden das zunehmende Angebot an IT-Diensten und die bestehende Notwendigkeit diese zu nutzen als störend empfunden. Zum einen liegt dies in der Tatsache begründet, dass man sich bereits an die Nutzung von Diensten mit ähnlichem oder gar gleichem Funktionsumfang gewöhnt hat, zum anderen an dem Umstand, dass einige Dienste in ihrer Bedienungsführung dem gewohnten Nutzerverhalten entgegen stehen.

Besondere Ablehnung gegen die angebotenen Dienste entsteht in den Fällen, in denen im Rahmen des Studiums spezielle Software genutzt werden muss und diese gegebenenfalls Inkompatibilitäten mit dem eigenen System aufweist, die unter Umständen sogar Auswirkungen auf das restliche System haben.

Neben den angebotenen Diensten wächst aber auch die Anzahl an Medien, wie Vorlesungsskripten, Büchern, Vorträgen etc. die in digitaler Form bereitgestellt werden. Diese sind häufig an unterschiedlichen Stellen zu finden.

Die Erwartung an die IT der Universität endet daher nicht bei der Integration der eigenen, bestehenden IT-Umgebung in die offiziellen Systeme für Studium und Verwaltung, unabhängig vom Provider oder spezifischer Ausprägung, sondern geht hin zu einer Studiums bezogenen Umgebung, die bereits alle relevanten Anwendungen installiert und konfiguriert hat, Zugriff auf benötigte Medien bietet und auf dem eigenen System ausgeführt werden kann.

Um diese Aufgabe leisten zu können, ist von den Universitäten ein frühzeitiges Umdenken sowie Flexibilität an der zentralen Stelle des Campus Management, den Systemen des Identity- und Service Management, unausweichlich. Diese müssen BYOE bereits bei der Provisionierung unterstützen und als Normalfall betrachten. Die Dienste müssen – jedenfalls für die nicht datenschutzrelevanten Sachverhalte – Providerneutral angeboten werden. Inhalte müssen gebündelt und Studiums bezogen verfügbar gemacht werden. Dabei muss dem Studierenden die Auswahl der benötigten Dienste und Inhalte erleichtert werden und möglichst zentral verwaltbar sein.

Als Basis für die Umsetzung dieser Aufgaben wird an der TU Berlin das Identity Management System TUBIS eingesetzt. Das personalisierte Dienstportal verfolgt den Ansatz einer rollenbasierten Zugangsregelung. Jedes Mitglied der TU Berlin wird automatisch erfasst und mit Standardrollen ausgestattet, die im Arbeitsalltag durch Delegation, Stellvertretung oder Übertragung von Funktionen um weitere Rollen ergänzt werden können. Das System wird von mehr als 37000 Mitgliedern der TU Berlin seit mehr als 5 Jahren täglich genutzt.

Als zweite zentrale Komponente hat die TU-Berlin den Cloudspeicherdienst ownCloud aufgesetzt und stellt diesen flächendeckend mehr als 37000 Mitgliedern zur Verfügung.

Der Rest des Beitrags ist wie folgt strukturiert:

Kapitel 2 bietet einen groben Hintergrund über das an der TU-Berlin entwickelte Identitätsmanagementsystem „TUBIS“ , während im Kapitel 3 ein Framework vorgestellt wird, mit dem eine Verknüpfung des IDM mit einem Cloudspeicherdienst sowie dessen Integration in den Prozess des Provisioning realisiert werden kann. Das letzte Kapitel gibt abschließend einen Ausblick über die weiterführende Entwicklung.

2 Identitätsmanagement als Grundlage

Die Veränderungen der letzten Jahre in der IT-Hochschullandschaft spiegeln den Trend zur Integration vielfältiger Universitätsbereiche wieder, die vorher weitgehend unabhängig voneinander gearbeitet haben. Der Bedarf für eine solche Integration entsteht durch die Erwartungen von Studierenden und Mitarbeitern, zahlreiche Dienste durch Selbstbedienungsfunktionen zu nutzen und somit mehr Zeit für Studium und Forschung zu gewinnen. Die Umsetzung eines integrierten Dienstangebots stellt die Hochschulen wiederum vor signifikante technische und organisatorische Herausforderungen. Geschäftsprozesse und Verantwortlichkeiten sind selten umfassend

dokumentiert, wodurch eine übergreifende Planung, Steuerung und Operationalisierung erschwert wird.

Jedes Mitglied der Universität muss eindeutig und mit allen Befugnissen, Kontexten wie etwa Status (Studierender, Mitarbeiter), Rolle (Dekan, FG-Leiter, Abteilungsleiter, …) oder Studiengang, bekannt sein, damit ein möglichst einfacher, einheitlicher Zugang zu allen für ihn relevanten Diensten möglich wird; und dies gleichgültig, ob sich die Person am Arbeitsplatz, zu Hause oder auf einer Dienstreise befindet.

Hierbei reifte in den letzten Jahren zunehmend die Erwartungshaltung, eigene, private Endgeräte zur Erfüllung der gestellten Aufgaben nutzen zu können. Dabei konnte es sich sowohl um leistungsstarke Notebooks als auch um leistungsbegrenzte Smartphones oder Tablets handeln. Dies führte zu einer verstärkten Verlagerung der Dienste hin zu webbasierten Angeboten.

Die TU-Berlin hat zur Erfüllung der Aufgaben eines Identitätsmanagementsystems das universitätsweite, rollenbasierte Autorisierungssystem TUBIS entwickelt [HKR08b, HR07]. Dieses integriert sich in die bestehende Infrastruktur der Campusmanagementsysteme und bietet den jeweiligen Einrichtungen die Möglichkeit der dezentralen Rechteverwaltung [RHK10]. Einen zentralen Baustein des Identitätsmanagementsystems bildet dabei eine Reihe von webbasierten Selbstbedienungsfunktionen. Durch die Plattformunabhängigkeit bildeten diese bereits die Voraussetzung zur besseren Unterstützung von BYOD. Durch gezielte Erweiterungen wurde das Paradigma des GYSE noch weiter unterstützt.

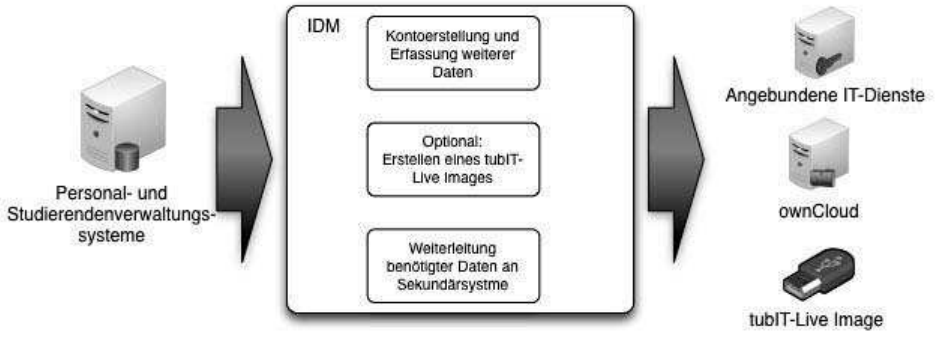

Abbildung 1 Auszug aus dem Provisioning

Zentraler Bestandteil des Identitätsmanagementsystems ist das Provisioning. Dieses ermöglicht das frühzeitige Erfassen eines neuen Mitglieds sowie dessen zentrale Versorgung mit allen benötigten Zugangsdaten und Rechten. Dieser Prozess wird auch im nachfolgend vorgestellten Framework eine zentrale Rolle spielen.

3 GYSE

Ziel war es, den Studierenden ein System zur Verfügung zu stellen welches ihnen ermöglicht, alle für ihr Studium relevanten Dienste zu verwenden. Das System sollte außerdem in der Lage sein, übersichtlichen Zugang zu allen für das Studium benötigten Inhalten (z.B. Vorlesungsskripte, Anleitungen, Veröffentlichungen) zu schaffen. Lange Installationsroutinen und Änderungen an der bestehenden IT-Infrastruktur der Studierenden sollten dabei vermieden werden. Das an der TU-Berlin hierfür entwickelte System teilt sich in zwei Bereiche auf: Dem Erstellen eines flexiblen OS-Images, auf welchem bereits alle benötigen Dienste installiert und konfiguriert sind, sowie die Verwaltung der für den Studenten verfügbaren Inhalte. Beide Bereiche werden dabei über das Identitätsmanagementsystem verwaltet und synchronisiert.

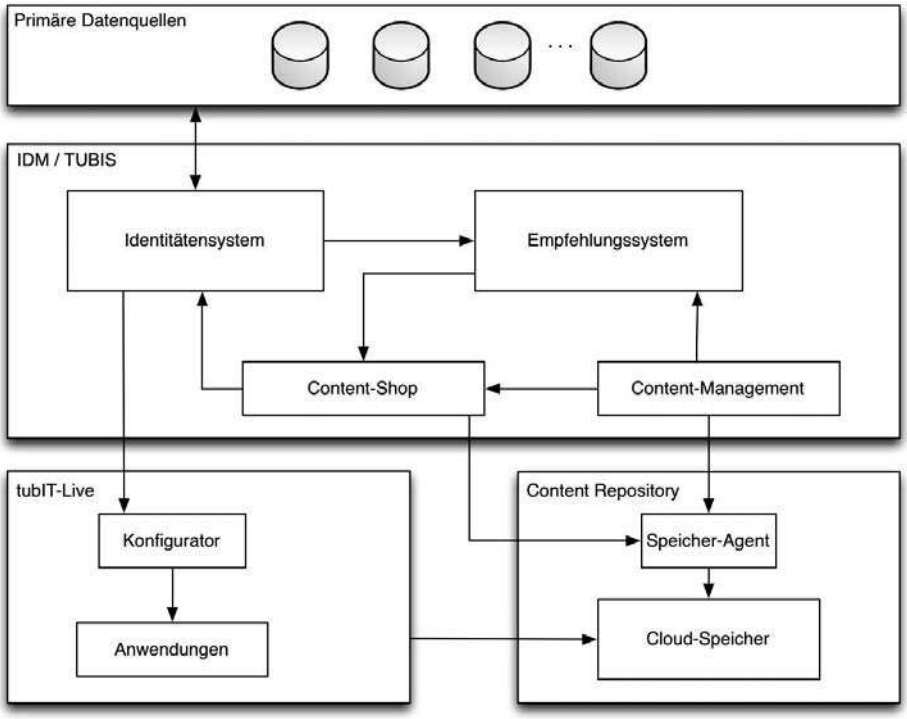

Abbildung 2 : GYSE Framework

Um sicherzustellen, dass das System allen Studierenden angeboten werden kann, wird ein zentraler Einstiegspunkt verwendet: Die Provisionierung.

Während dieses Prozesses registriert sich der Studierende mit seinen Daten, erstellt ein Benutzerkonto und wählt dafür ein persönliches Passwort aus. Zur Vermeidung redundanter oder fehlerhafter Daten, werden die Stammdaten der Studierenden für die Provisionierung direkt aus den Systemen der Studierendenverwaltung geladen.

Die meisten neu immatrikulierten Studierenden besitzen beim Eintritt in die TU-Berlin bereits ein privates E-Mailkonto. Um dem Studierenden die Möglichkeit zu geben, seine eigenen Dienste weiterzuverwenden, kann er während der Provisionierung entscheiden, ob er die Erstellung eines weiteren Postfaches wünscht oder stattdessen lediglich ein TU-Alias erstellt werden soll, um studienrelevante Nachrichten an ein bestehendes E-Mailpostfach versenden zu können. Im letzten Schritt der Provisionierung stehen dem System nun alle benötigten Daten wie z.B. der Kontoname, das Passwort und der Studiengang zur Verfügung. Diese Daten können verwendet werden, um ein personalisiertes System zu erstellen. Nachfolgend werden dem Studierenden die verfügbaren Inhalte angezeigt. Innerhalb eines „Content-Shop“ des IDM-Systems, welches an einen Onlineshop angelehnt ist, kann ausgewählt werden, zu welchen Inhalten ein Zugang gewünscht ist. Neben den zwei Kategorien Daten und Software unterteilt sich der Content-Shop in zwei große Bereiche. Während der eine Bereich alle zur Verfügung stehenden Inhalte, sortiert nach Studiengängen, auflistet, liefert der zweite Bereich eine speziell auf den Studierenden zugeschnittene Auswahl an Inhalten. Diese Vorauswahl dient dazu, die Übersicht zu verbessern und kann vom Studierenden nach eigenen Wünschen angepasst werden. Die Auswahl wird dabei von einem Empfehlungssystem generiert, welches vorhandene Daten des Studierenden verwendet, um eine repräsentative Vorauswahl der Inhalte zusammenzustellen. Vorerst werden dabei nur die besuchten Studiengänge sowie der jeweiligen Fachsemester berücksichtigt. Das System unterstützt aber bereits das Heranziehen aller im IDM verwalteten Informationen zur Generierung einer Empfehlung. Die Verwaltung modelunabhängiger Metadaten ist bereits in Planung.

3.1 Das Live-System

Das OS-Image soll am Ende der Provisionierung automatisch erstellt werden. Dies wird durch einen Appliance-Buildserver realisiert, welcher über eine Web-Service Schnittstelle angestoßen wird. Aktuell wird als Basisbetriebssystem ein modifiziertes Ubuntu-Derivat verwendet. Über die mitgelieferten Systemwerkzeuge wie yum kann dieses unabhängig vom Content-Shop erweitert werden. Ein im erzeugten System integrierter Konfigurator ist für die personenbezogene Einrichtung der installierten Dienste wie E-Mailclient, Webbrowser oder den Zugang zum AFS oder zum Cloud-Speicher zuständig. Dazu verwendet der Konfigurator die übermittelten Personendaten aus der Provisionierung.

Das Image wird in einem Format zur Verfügung gestellt, welches es dem Studierenden ermöglicht, es entweder direkt von einem USB-Stick aus zu starten, oder als virtuelle Maschine innerhalb einer Virtualisierungssoftware zu betreiben. Nach der Erstellung steht das Image dem Studierenden drei Tage lang in verschlüsselter Form zum Download zur Verfügung und wird anschließend von den Servern der TU-Berlin entfernt. Wird vom Studierenden z.B. das Passwort geändert, so wird das System neu erstellt (unter Berücksichtigung des neuen Passwortes) und steht erneut für eine bestimmte Zeit zum Download bereit. Auf diese Weise sind die konfigurierten Dienste

weiterhin nutzbar. Dieser Prozess kann auch ohne Passwortänderung manuell vom Studierenden angestoßen werden. Alternativ kann das fertige Image auch direkt im Cloud-Speicher abgelegt werden und von dort auf das gewünschte Zielgerät heruntergeladen werden. Die Zugriffrechte werden dabei durch das IDM gesteuert.

Nutzer, die manuelle Anpassungen am System vorgenommen haben und ihr Passwort ändern sind nicht gezwungen das neu erzeugte Image zu nutzen. Alternativ kann der Konfigurator im System erneut aufgerufen werden um das neue Passwort zu registrieren.

3.2 Zugriff zu den Inhalten

Daten die während des Arbeitens mit dem persönlichen System entstehen oder verändert werden, müssen auch über die Neuerstellung des Systems hinaus Bestand haben. Um dies zu erreichen wird auf dem System bereits der Zugang zu einem Cloudspeicher-Dienst eingerichtet.

Jedes Mitglied der TU-Berlin erhält mit der Provisionierung auch einen Zugang im Cloud-Speicher mit einer persönlichen Quota abhängig davon, ob es sich um einen Mitarbeiter oder einen Studierenden handelt. Neben den persönlichen Daten werden hier auch die studienrelevanten Inhalte abgelegt. Um die Quota der Studierenden nicht mit den ausgewählten Inhalten zu belasten, werden keine Kopien der Daten angelegt, sondern lediglich Zugriffe auf verteilte Ordner verwaltet.

Das IDM-System steuert dabei, wer Zugriff auf welchen Bereich erhält und unterscheidet zwischen zwei Benutzergruppen.

Die Nutzer der Inhalte, also in erster Linie die Studierenden, erhalten lesenden Zugang zu all den Ordnern, die sie im Content-Shop des IDM ausgewählt haben. Diese Auswahl kann jederzeit über das persönliche Portal angepasst werden.

Die Bereitsteller der Inhalte erhalten vom IDM schreibenden Zugriff auf alle Ordner, für die sie eine entsprechende Verwalterrolle besitzen. Über eine Selbstbedienungsfunktion im persönlichen Portal können diese Nutzer auch weitere verteilte Ordner im Cloud-Speicher anlegen und mit entsprechenden Meta-Daten versehen.

Beide Benutzergruppen haben den Vorteil, dass sie von jedem System aus, für das ein Cloud-Speicher-Client zur Verfügung gestellt wird, Zugriff auf die Daten haben.

4 Ausblick

Das entwickelte Framework ist ein Grundgerüst, welches in unterschiedlicher Weise weiterentwickelt werden kann. Die einzelnen vorgestellten Bereiche decken bereits die Grundfunktionalitäten ab, welche erweitert werden können, um den Benutzern so einen größeren Komfort zu bieten.

So kann die Benutzung des Content-Shops als zwingender Bestandteil des Provisioning-Prozesses etabliert werden, was dafür sorgen würde, dass jeder Benutzer (da jeder Benutzer provisioniert sein muss) ein entsprechendes Live-System besitzt.

Ausgehend vom beschriebenen Grundgerüst, kann die Integration von Software in das OS-Image weiter untersucht werden. Diese Software kann direkt bei Erstellung des Images integriert werden. Dabei ist darauf zu achten, dass die (im Content-Shop ausgewählte) Software mit anderen ausgewählten Softwarepaketen kompatibel ist. Wie auch bereits beim Content, sollte die inkrementelle Erweiterung und Aktualisierung der Software innerhalb des personalisierten Systems realisiert werden. Dadurch wird ein ständiges Neuerstellen des Systems verhindert.

Mit wachsender Anzahl der Nutzer und der damit verbundenen Meta-Daten können auch die Funktionsweise der Content-Shops und des Empfehlungssystems angepasst werden.

Sowohl die zur Auswahl herangezogenen Algorithmen selbst als auch die Art des Systems können angepasst und überarbeitet werden. Hierfür kann es ggf. nötig sein, das Datenmodel zur Haltung der Metadaten anzupassen.

Durch Erweiterung der verwertbaren Daten um z.B. Prüfungsergebnisse oder die Wahl der Veranstaltungen, kann auch die Vielfalt der angebotenen Inhalte erhöht werden.

Die stetig wachsende Zahl an mobilen Endgeräten macht ebenfalls die Betrachtung einer möglichen Nutzung des bereitgestellten Systems auf unterschiedlichen mobilen Plattformen notwendig.

Nicht alle mobile Endgeräte bieten die Möglichkeit, OS-Images zu verwenden. Eine Möglichkeit, trotz dieser Einschränkung das erstellte OS-Image zu verwenden, ergibt sich dann, wenn die Images direkt von Rechenzentrum gehostet werden, und die Studierenden z.B über eine Web-Desktop Lösung oder eine View-Umgebung auf Ihre personalisierten Systeme zugreifen können. Dies setzt zwar eine Internetanbindung voraus – spätestens seit der flächendeckenden W-LAN Anbindung auf dem Campus stellt dies jedoch kaum ein Problem dar.

Literaturverzeichnis

[HKR08b] T. Hildmann, O. Kao, and C. Ritter. Rollenbasierte Identitäts- und Autorisierungsverwaltung an der TU Berlin. 1. DFN-Forum Kommunikationstechnologien Verteilte Systeme im Wissenschaftsbereich, 2008.

[HR07] T. Hildmann and C. Ritter. TUBIS-Integration von Campusdiensten an der Technischen Universitat Berlin. *PIK-Praxis der Informationsverarbeitung und Kommunikation*, 30(3):145–151, 2007.

[RHK10] C. Ritter, T. Hildmann, O. Kao. Erfahrungen und Perspektiven eines rollenbasierten IdM , 3. DFN-Forum Kommunikationstechnologie, 26. Mai 2010