IdM made in Chemnitz

Identity Management im URZ der TU Chemnitz

Daniel Klaffenbach

Universitätsrechenzentrum

27. Mai 2014

Gliederung

1. Aktueller Stand
   - Ausgangssituation
   - Ein Neuanfang
   - MoUSe2
2. Strategie
3. Dienste- und Ressourcenverwaltung
   - Begriffe
   - Integration ins IdM

Rückblick

- Identity Management → lange Tradition an der TU Chemnitz
- Seit 1998: **M**anagement **o**f **U**sers and **Se**rvices (kurz *MoUSe*)
  - PHP-Anwendung (Eigenentwicklung) zur Nutzerverwaltung
  - Zuordnung aller Personen zu Einrichtungen, Struktureinheiten und Personentypen
  - Verwaltung der Nutzungsberechtigung
  - Ein Account pro Person (keine getrennten Studenten- und Mitarbeiteraccounts)
  - Täglicher Datenabgleich von Studenten- und Mitarbeiterdaten
  - Verwaltung von Ressourcen wie z.B. Mailadressen oder Zugangskarten
- Im Laufe der Jahre: Grundlage für immer weitere Dienste
  → Zunehmende Verschmelzung von Identity-Management mit der Diensteverwaltung
- Nachfolgesystem seit 2013 im Produktivbetrieb

IdM und Service-Management – wie passt das zusammen?

- Normalerweise keine Verwaltung von Diensten durch IdM-System
- Anbindung verschiedener Zielsysteme an IdM
- Aber: Neben klassischen Identitäts-Attributen sind u.U. auch Rollen & Berechtigungen für Zielsysteme relevant
- Außerdem: Status verschiedener Zielsysteme auch für IdM von Relevanz (z.B. für Reporting-Funktionen für Benutzer)
- Unsere Philosophie:
  - Integration der Zielsystemanbindung direkt im IdM
    $\rightarrow$ hoher Komfort für Nutzer, da IdM somit zentrale Anlaufstelle
    $\rightarrow$ technisch ebenfalls sinnvoll (Berechtigungsprüfung für versch. Zielsysteme direkt im IdM)
  - Integration weiterer Dienste, um vorhandene Architektur mitzunutzen

Ablösen des alten Systems

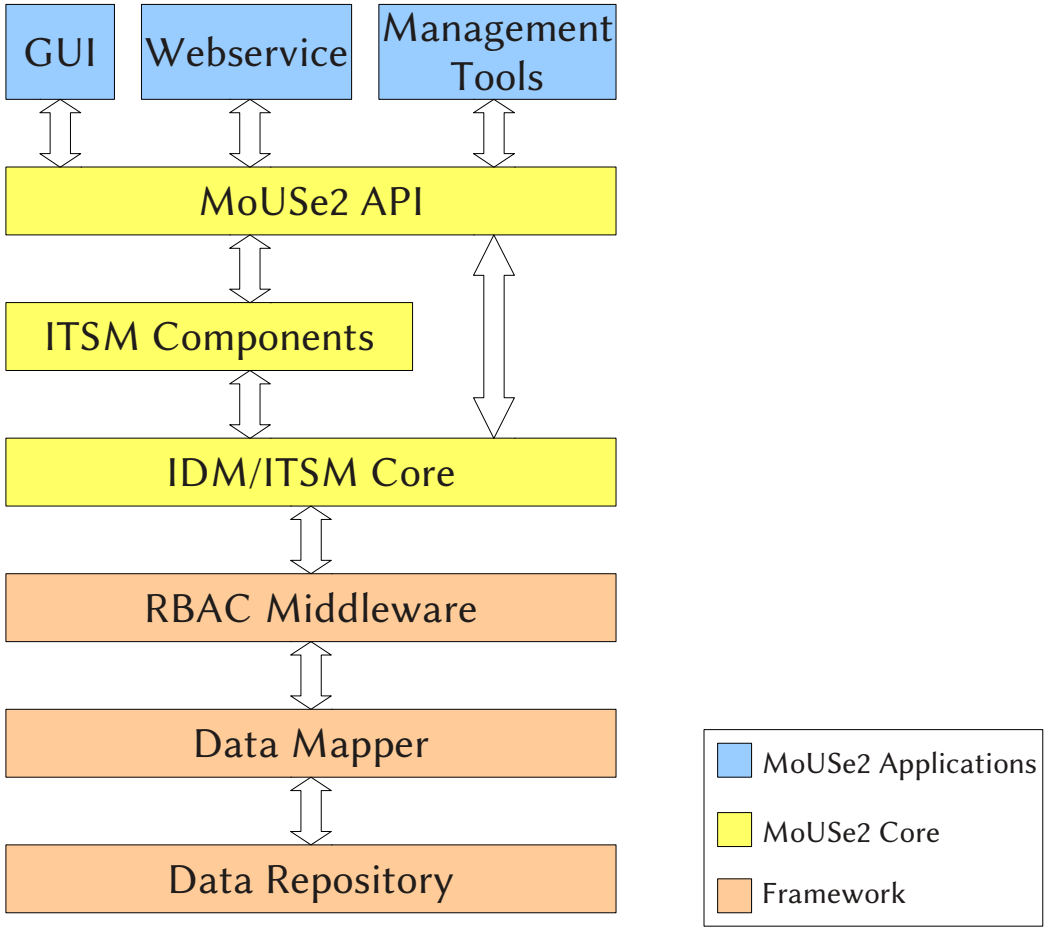
- Konzeption & Entwicklung einer neuen Lösung seit 2010
- Ziele:
  - Vereinfachung und Vereinheitlichung vieler Prozesse
  - Integration eines rollenbasierten Autorisierungskonzeptes
  - Einheitliche Abbildung von Diensten und Ressourcen
  - Konsequentes Lifecycle-Management
  - Moderne Architektur
  - Verbesserte Reporting-Funktionen
- Produktivbetrieb seit Oktober 2013
  - Schrittweise Migration verschiedener Dienste nach **MoUSe2** läuft, Kerndienste bereits migriert
  - Parallelbetrieb des Legacy-Systems noch bis 2015 geplant

MoUSe2

- Vollständige Neuentwicklung → keine Abhängigkeiten zu altem System
- Basis-Daten:
  - Python mit Django-Framework
  - RDBMS (MySQL, Oracle oder PostgreSQL)
  - RBAC[1] über Django Middleware
  - RESTful Webservice & Python API
  - WSGI-konformer Webserver
- Event-Trigger für Lifecycle-Events
- Einheitliches Provisionierungsverfahren
  - Deploy-Manager
  - Anbindung der Zielsysteme über native Python-APIs
- Umfassendes Ressourcenkonzept

[1] RBAC nach ANSI/INCITS 359-2004

Architektur



IdM-Strategie

- IdM weiterhin im eigenen Haus
- Kontinuierliche Verbesserung und Weiterentwicklung von *MoUSe2*
- Kombination von IdM mit Service-Management
- Kurzfristige Agenda:
  - Aufnahme weiterer Dienste in *MoUSe2*-Framework
  - Abbildung von kostenpflichtigen Ressourcen → Interaktion mit Accounting-Werkzeugen/Haushalt
  - Überarbeitung der Schnittstellen zu HIS
  - Verbesserung des Scorings der Matching-Verfahren zur Dublettenbestimmung

IdM-Strategie

- IdM weiterhin im eigenen Haus
- Kontinuierliche Verbesserung und Weiterentwicklung von *MoUSe2*
- Kombination von IdM mit Service-Management
- Kurzfristige Agenda:
  - Aufnahme weiterer Dienste in *MoUSe2*-Framework
  - Abbildung von kostenpflichtigen Ressourcen → Interaktion mit Accounting-Werkzeugen/Haushalt
  - Überarbeitung der Schnittstellen zu HIS
  - Verbesserung des Scorings der Matching-Verfahren zur Dublettenbestimmung

Begriffe

Ressource

- Eine Funktionalität oder ein Merkmal
- Kann von Benutzern in Anspruch genommen werden
- Menge von Attributen und Operationen
- Referenziert i.d.R ein Objekt in der realen Welt
  $\rightarrow$ Kann provisioniert werden (Deployment)

Dienst

- Eine Gruppierung von Ressourcen
- Enthält Meta-Definitionen für seine Ressourcen

Integration des Dienste- und Ressourcen-Konzeptes ins IdM

- Modellierung jedes Zielsystems als *Ressource* → Instanz einer Ressource entspricht dem Datensatz des Nutzers im jeweiligen Zielsystem
- Zustandsänderung einer Ressource → Auslösen eines Deployvorgangs
- Behandlung von Lifecycle-Events direkt durch Ressourcen (*Publish-Subscribe*)
- Generische Behandlung von Standard-Abläufen
  - Ressource läuft ab/wird gesperrt/Nutzer verliert Berechtigung/...
  - Verlängerung von Ressourcen
  - Definition von Ressourcenverantwortung
  - Erinnerung für Benutzer über ablaufende Ressourcen
- Übersicht über Art und Zustand aller Ressourcen

Ressourcenliste

TU Chemnitz → URZ → IdM-Portal → Benutzermenü → Dienste

Benutzermenü
- Benutzerübersicht
- Benutzerdaten bearbeiten
- Passwort ändern

Dienste
- Account
- E-Mail
- Speicherdienste
- Netz
- Gruppen

Weitere Dienste
- MoUSe1 (Türzugang, VoIP, Projekt-Ordner, Gapps)
- PC-Admin
- Software
- VPSH

Verschiedenes
- Ressourcenliste
- Ausstehende Anfragen
- Finanzen
- Gastaccounts

Ressourcenliste

Diese Seite bietet einen Überblick über alle IT-Ressourcen, die Sie im URZ in Anspruch nehmen. Sie können den untenstehenden Filter verwenden, um die anzuzeigenden Ressourcen und Dienste einzuschränken.

Filter

Dienst	Ressource	Rolle	Status	Deploy Status	Ablaufdatum	Aktionen
Account	Resource 'Active Directory' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'LDAP' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'Kerberos' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'PasswordRecovery' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'Login' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'Passwd-Entry' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'Public LDAP' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'ZUV Active Directory' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Account	Resource 'AFS Account' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Default	Meta resource for deploy management for user Daniel Klaffenbach	Resource Owner	aktiv	ok	31. Dezember 2099	
Legacy	Resource 'MoUSe1 Legacy' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
Groups	Gruppe 'tuc:zuv_users'	Resource Owner	aktiv	ok	31. Dezember 2099	
Groups	Gruppe 'urz_testnutzer'	Resource Owner	aktiv	ok	31. Dezember 2099	
E-Mail	daniel.klaffenbach@s2007.tu-chemnitz.de	Resource Owner	aktiv	ok	31. März 2055	
E-Mail	klada@hrz.tu-chemnitz.de	Resource Owner	aktiv	ok	31. März 2055	
E-Mail	klada@informatik.tu-chemnitz.de	Resource Owner	aktiv	ok	31. März 2055	
E-Mail	daniel.klaffenbach@informatik.tu-chemnitz.de	Resource Owner	aktiv	ok	31. März 2055	
E-Mail	daniel.klaffenbach@hrz.tu-chemnitz.de	Resource Owner	aktiv	ok	31. März 2055	
E-Mail	klada@tu-chemnitz.eu	Resource Owner	aktiv	ok	31. März 2055	
E-Mail	Resource 'URZ Mailbox' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	
E-Mail	Resource 'Group Mailbox' for Daniel Klaffenbach	Resource Owner	gelöscht	ok	31. Dezember 2099	
Storage	Resource 'ZUV Windows Home Verzeichnis' for Daniel Klaffenbach	Resource Owner	aktiv	ok	31. März 2055	

Beispiel

- Benutzer besitzt verschiedene Basis-Ressourcen (Mailadressen, Kerberos, AD, LDAP, Home, ...)
  - Event „Namensänderung“ nur relevant für AD, LDAP und evtl. Mail → Abonemment
  - Event „Berechtigungsdatum geändert“ für alle Relevant → wird ohne Abonnement behandelt
- Benutzer besitzt verschiedene beauftragte Ressourcen (Projektverzeichnisse, IP-Adressen, ...)
  - Kann Verantwortung delegieren
  - Kann Ressourcen nicht über sein Berechtigungsdatum hinaus verlängern
  - Erhält *eine* Erinnerung über *alle* ablaufenden Ressourcen

Beispiel

- Benutzer besitzt verschiedene Basis-Ressourcen (Mailadressen, Kerberos, AD, LDAP, Home, ...)
  - Event „Namensänderung“ nur relevant für AD, LDAP und evtl. Mail → Abonemment
  - Event „Berechtigungsdatum geändert“ für alle Relevant → wird ohne Abonnement behandelt
- Benutzer besitzt verschiedene beauftragte Ressourcen (Projektverzeichnisse, IP-Adressen, ...)
  - Kann Verantwortung delegieren
  - Kann Ressourcen nicht über sein Berechtigungsdatum hinaus verlängern
  - Erhält *eine* Erinnerung über *alle* ablaufenden Ressourcen

Fragen
???