Identity und Access Management in der Cloud – Fallbeispiel

Roland Seidelt
virtual7 GmbH
Karlsruhe

Schlüsselworte
Oracle Identity Manager, Oracle Enterprise Single Sign-on, Cloud, Berechtigungsverwaltung, Benutzerverwaltung, Single Sign-on, Identity Management, Access Management

Einleitung

Die KIVFB bietet als kommunal organisierter Gesamtlösungsanbieter seinen Kunden eine Cloud, in der alle Lösungen und Dienste der KIVBF gebündelt über einen zentralen Zugang zur Verfügung stehen.
Den 40.000 Usern der Cloud wird für alle Lösungen und Dienste ein Single Sign-on zur Verfügung gestellt, das mit dem Produkt Oracle ESSO realisiert wird.

Die User sollen dezentral durch bis zu 5000 Administratoren auf Kundenseite verwaltet werden. Diesen Administratoren wird mit dem Oracle Identity Manager (OIM) eine web-basierte Oberfläche zur Verwaltung ihrer Benutzer und deren Berechtigungen angeboten.

Mit diesen zwei Lösungen werden wichtige Anforderungen an die KIVBF-Cloud unterstützt:

- Datensicherheit
- Benutzerfreundlichkeit durch Single Sign-on
- Automatisierte Bereitstellung von Lösungen durch ein Zusammenspiel von OIM mit der Cloud-Verwaltungssoftware
- Dezentrale Benutzerverwaltung in einem Self-Service-Portal

Der Vortrag gibt einen Überblick über die KIVBF-Cloud und zeigt die Lösungen auf, die durch den Einsatz von ESSO und OIM realisiert wurden.

Die zentralen Fragen, die beantwortet werden, sind:

- Wie kann den Usern der Cloud ein Single Sign-on bereitgestellt werden?
- Wie kann die User- und Berechtigungs-Verwaltung effizient, das heißt konkret dezentral, gestaltet werden?

Was macht die KIVBF?

Die Kommunale Informationsverarbeitung Baden-Franken (KIVBF) ist ein IT-Systemhaus und Gesamtlösungsanbieter für Städte, Gemeinden und Landkreise.

Von der Form her ist die KIVBF ein kommunaler Zweckverband, der auf einer Fusion von regionalen Rechenzentren in Karlsruhe, Freiburg, Heidelberg und Heilbronn im Jahr 2003 basiert. Die KIVFB besitzt die zwei Tochtergesellschaften Kommunales Rechenzentrum Baden-Franken GmbH (KRBF GmbH) und endica GmbH.

Dem Zweckverband gehören über 500 baden-württembergische Gemeinden oder Städte, sowie etwa 25 Kreise und 5 sonstige Körperschaften des öffentlichen Rechts (unter ihnen auch das Land Baden-Württemberg) als Mitglied an (Stand 1. Januar 2014). Über die Gremien des Zweckverbandes wirken die Mitglieder an der Strategie der KIVBF-Gruppe mit.

Die KIVBF stellt ihren Mitgliedern, die gleichzeitig Kunden der KIVBF sind, rund 60 Lösungen aus den folgenden Bereichen zur Verfügung:

- Finanzverfahren
- ordnungsrechtlichen Verfahren (z. B. Einwohnerwesen und Ordnungswidrigkeiten)
- Lösungen für die Personalabrechnung und für das Personalmanagement
- Versorgungs- und Entsorgungslösungen

Die KIVBF-Cloud

Die von der KIVBF bereitgestellten Anwendungen unterscheiden sich in Art und Weise. Hier ein paar Beispiele für verschieden Anwendungstypen:

- Web-Anwendungen (typische Client-Server, zum Beispiel Oracle BI)
- unabhängige Desktop-Anwendungen (z.B. Office Lösungen)
- Desktop-Anwendungen mit Zugriff auf zentrale DB (z.B. .NET-Anwendungen mit zentraler DB)
- SAP

Die einzelnen Lösungen sind zum Teil mehrmandantenfähig, zum Teil aber auch nicht. Weiter unterscheidet sich die Bereitstellung dadurch, dass Lösungen mal von der KIVBF gehostet werden, mal beim Kunden direkt installiert und betrieben werden.

Aufgrund dieser Diversität wurde der Ansatz der KIVBV-Cloud geboren, konzipiert und umgesetzt. Hauptantrieb dafür war die Kostenersparnis auf Seiten der KIVBF und deren Kunden. Insbesondere durch die Reduktion von Installations- und Betriebskosten soll es möglich werden, attraktive Preise auch für Kunden, sprich Kommunen, von kleinerer Größe anzubieten.

Weiter soll die Cloud einen höheren Standardisierungsgrad einführen, Flexibilität und Skalierbarkeit sichern, sowie durch Device-unabhängige Zugänge komfortabler für den Benutzer werden und insbesondere mit mobilen Zugang zukunftsorientiert sein. Im Konzept finden sich zudem auch die Anforderungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) berücksichtigt.

Die KIVBF-Cloud versteht sich als Community-Cloud für Einrichtungen der kommunalen öffentlichen Verwaltung mit Schwerpunkt im Verbandsgebiet der KIVBF. Dabei besteht für die Kunden, bzw. Mitglieder der KIVBF die Möglichkeit sich „Private Clouds“ innerhalb dieser Plattform zu buchen und Dienste in hybrider Verschränkung mit ihren eigenen Services zu nutzen.

Technisch basiert die KIVBF-Cloud maßgeblich auf Citrix Technologien und dem Open Virtualization Format (OVF). Der Zugriff auf die Cloud erfolgt dabei über Citrix Netscaler und Citrix Storefront, das dem Anwender die ihm verfügbaren Lösungen listet. Diese Lösungen werden dann als Citrix XenApps oder Citrix XenDesktops bereitgestellt, wofür der Anwender einen Client benötigt, der für verschiedene Hardware und Betriebssysteme verfügbar ist, insbesondere auch für mobile Endgeräte. Die Lösung selbst kann dabei aus einem komplexeren Set von Servern bestehen, die als sogenannte virtuelle Landschaft in einem virtuellen LAN bereitgestellt wird. Dabei sorgt eine Cloud-Management Lösung der Firma fluid Operations dafür, dass solche virtuellen Landschaften auf Basis

von Templates beliebig und voll-automatisiert bereitgestellt und somit vom Kunden im Self-Service gebucht werden können.

Welche Anforderungen ergeben sich an das Access- und Identity Management?

Aus der Architektur und den allgemeinen Anforderungen an die KIVBF-Cloud ergeben sich für das Access- und Identity Management verschiedene Anforderungen. Maßgeblich zu nennen sind die Folgenden:

- Einfacher, komfortabler Zugang für Endbenutzer
- Sicherheitsaspekte / Anforderungen BSI
- Automatische Bereitstellung von Lösungen
- Effiziente Administration der Benutzer durch die Kunden selbst

Daraus leitet sich dann zunächst die Forderung eines Single Sign-on ab. Desweitern wird eine Software zur Verwaltung von Benutzern und Berechtigungen benötigt, die sich in die automatisierten Prozesse rund um die Bereitstellung von Lösungen einpasst. Die Lösungen müssen dabei BSI-konform gestaltet sein.

Zwei Oracle Produkte boten die notwendigen Funktionen und Voraussetzungen diesen Anforderungen gerecht zu werden. Details zu den Lösungen finden sich in den nächsten beiden Abschnitten.

Single Sign-on – Einmal Passwort und dann los!

Um die KIVBF-Cloud nutzen zu können, muss sich der Benutzer zunächst über Netscaler sozusagen in der Cloud selbst anmelden. Durch diese Anmeldung steht im dann zunächst Citrix Storefront zur Verfügung, das, als quasi Portal, Links auf die für den User verfügbaren Lösung-Landschaften bereithält. Der Benutzer kann nun zwar direkt die Landschaft aufrufen und eine XenApp oder XenDesktop Session öffnen, aber innerhalb dieser Session benötigt gegebenenfalls die Lösung selbst eine weitere Autorisierung.

Zum Beispiel könnte die Landschaft eine web-basierte Server-Client Landschaft bereithalten. Das heißt in der Landschaft würde ein Applikations-Server eine Anwendung hosten, auf die der Benutzer über ebenfalls bereitgestellten Browser zugreift. Die Anwendung erfordert eine Anmeldung und authentifiziert den Benutzer mit Hilfe eines in der Landschaft verfügbaren LDAP-Verzeichnisses (zum Beispiel ein Windows Active Directory). Jede Lösung hat damit ein unabhängiges LDAP-Verzeichnis. Diese sind dabei dezentralisiert innerhalb der Lösungs-Landschaften installiert.

Der Benutzer hat damit zum einen eine Kennung mit einem bestimmten Passwort für die Cloud selbst und zusätzlich je Lösung eine weitere Kennung mit einem weiteren Passwort.
Zum einen möchte man dem Benutzer nicht zumuten, dass er sich beliebig viele unterschiedliche Kennungen-Passwort-Paare merken muss, zum anderen sollte der Benutzer nicht unnötigerweise mehrmals zur Authentifizierung aufgefordert werden.

Erstere Anforderung ließe sich noch über eine Vereinheitlichung der Kennung und eine Synchronisation aller Passwörter abdecken. Allerdings leiten sich daraus komplexe technische Prozesse ab. Da dies zudem nicht die mehrmalige Anmeldung durch den Benutzer vermeiden würde, wurde mit dem Oracle Logon Manager, einem Bestandteil des Oracle Enterprise Single Sign-on Produktes, eine Lösung gewählt, die einerseits dem Benutzer den Zugang zu den bereitgestellten Lösungen vereinfacht, andererseits den Anforderungen an die Sicherheit gerecht wird.

Der Logon Manager greift für alle Anwendungen, die in sogenannten Templates konfiguriert sind. Diese Templates werden ebenfalls im Repository abgelegt.

In der KIVBF-Cloud Architektur ist der Logon Manager samt Repository dezentral innerhalb jeder einzelnen Lösung installiert. Als Repository wird ein AD-LDS verwendet. Die einzelnen Komponenten sind damit Bestandteil der Lösungs-Landschaften und werden damit mit den Landschaften selbst vollständig automatisiert bereit gestellt.

Das folgende Schaubild zeigt abstrahiert die Architektur, wie sie in jeder Landschaft verfügbar ist:

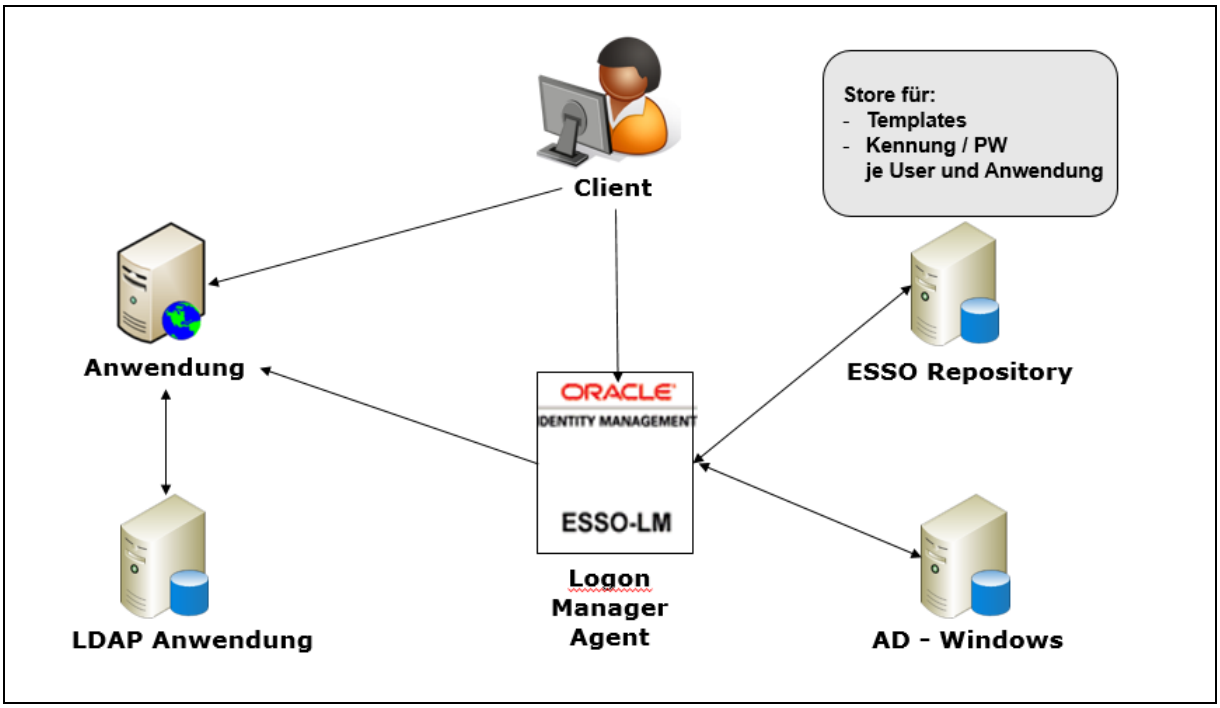

Abb. 1: Architektur Oracle Enterprise Single Sign-on – Logon Manager (innerhalb einer Landschaft)

Der Oracle Logon Manager ist, vereinfacht gesagt, ein Passwort Manager. Die Benutzer können je Anwendung Kennung und Passwort ablegen. Diese werden in einem Repository abgelegt. Der Logon Manager fängt Anmelde- und Passwort-Änderungs-Dialoge von Anwendungen ab und meldet den Benutzer bei der Anwendung an.

Hier eine Übersicht zu den wesentlichen Funktionen des Logon Managers:

- **Abfragen von Kennung und Passwort beim initialen Aufruf einer Anwendung**

  Wenn ein Benutzer das erste Mal eine Anwendung aufruft, fängt der Logon Manager den Anmelde-Dialog ab und fordert den Benutzer auf, seine Kennung und sein Passwort für diese Anwendung im Repository des Logon Managers zu speichern.

- **Verwaltung von mehreren Kennungen je Anwendung**

  Hat ein Benutzer für eine Anwendung mehrere Kennungen, weil er in der Anwendung beispielsweise als Administrator aber auch als normaler Benutzer fungiert, ist dies möglich. Der Logon Manager lässt den Benutzer dann bei jedem Aufruf der Anwendung wählen, mit welcher Kennung er die Anwendung nutzen möchte.

- **Automatische Anmeldung des Benutzers**

  Ruft ein Benutzer eine Anwendung auf, fängt der Logon Manager den Anmelde-Dialog auf und meldet den Benutzer im Hintergrund automatisch bei der Anwendung an, sofern der Benutzer bereits gültige Anmeldedaten im Repository hinterlegt hat.

- **Windows Authentifizierung am Logon Manager**

  Der Benutzer muss sich am Logon Manager anmelden, damit dieser selbst geschützt ist. Im KIVBF-Cloud Szenario verfügt der Benutzer innerhalb der Lösungs-Landschaft über eine Windows-Session, die dazu genutzt werden kann, den Benutzer am Logon Manager ohne weiteres Zutun anzumelden.

- **Unterstützung alle Passwort-relevanten Dialoge**

  Der Logon Manager kann prinzipiell alle Dialoge einer Anwendung, die im Zusammenhang mit Passwörtern stehen, handhaben. Beispielsweise greift der Logon Manager auch wenn die Anwendung den Benutzer zum Zurücksetzen des Passwortes aufruft, wenn dieses möglicherweise am Ablaufen ist.

Oracle Identity Manager als Lösung für eine effiziente Benutzer- und Rechte-Verwaltung

Die KIVBF-Cloud wird von etwa 1.000 Kunden und bis zu 40.000 Benutzern genutzt. Eine effiziente Benutzer- und Rechteverwaltung muss daher zum einen zumindest bis zu einem gewissen Grade automatisiert werden, zum anderen dezentralisiert eingerichtet werden. In der KIVBF-Cloud werden deshalb bestimmte Daten in verschiedenen Prozessen über definierte Schnittstellen automatisiert im Oracle Identity Manager (OIM) bereitgestellt. Sowohl die Benutzer als auch die Berechtigungen sind dabei in einer Kunden-Struktur abgelegt, so dass jeder Kunde sich Administratoren-Accounts erstellen kann, über die er dann seine Mitarbeiter verwalten und berechtigen kann.

Innerhalb des OIMs werden im Wesentlichen folgende Objekte verwaltet:

- Kunden
- Benutzer (Endanwender und Kunden-Administratoren)
- Passwörter
- Accounts (entsprechen Zugangsberechtigungen in die Cloud)
- Berechtigungen (entsprechen dem Zugriff auf einzelne Lösungen)

Die Verwaltung der Objekte beinhaltet das Anlegen, Ändern und Löschen der Objekte.

Dies geschieht entweder durch manuelle Aktion der Kunden-Administratoren oder durch automatisierte Prozesse.

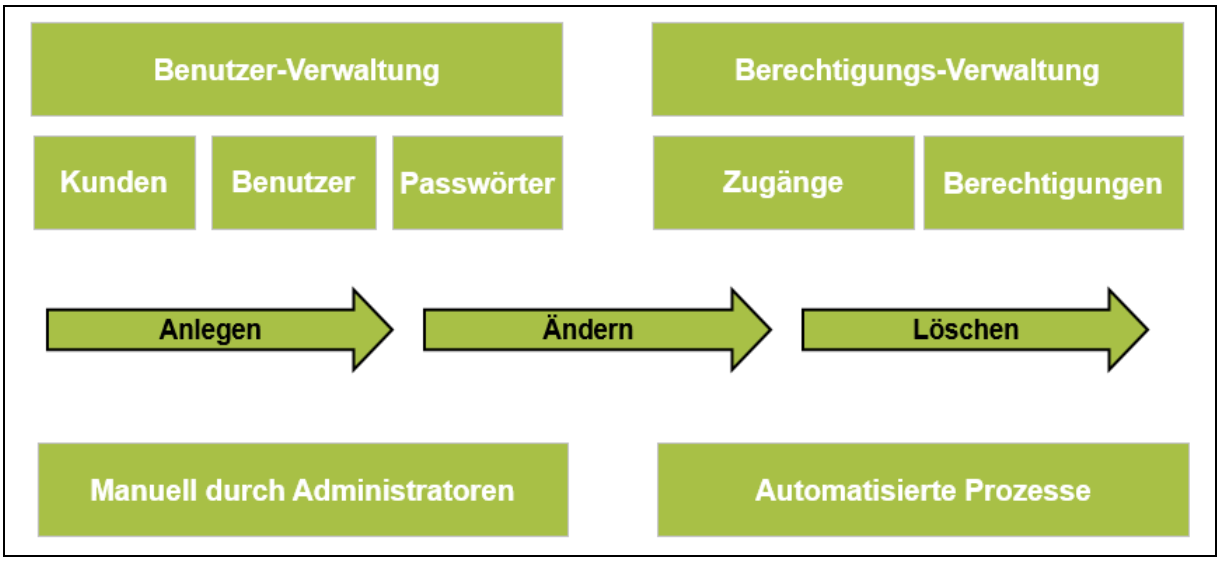

Abb. 2: Übersicht Aufgaben des OIMs

Der OIM bietet eine Fülle von konfigurierbaren und anpassbaren Funktionen. So gibt es zum Beispiel Schnittstellen zu LDAP-Verzeichnissen (z.B. Windows Active Directory) oder Datei-Formaten (z.B. CSV). Weiter bringt der OIM eine Workflow-Engine mit, einen Prozess-Scheduler, eine Reporting-Engine und Auditing Funktionen mit sich.

In der KIVBF-Cloud Architektur nutzt der OIM verschiedene Schnittstellen. Im folgenden Diagramm sind die wesentlichen Schnittstellen dargestellt und werden im Anschluss auch kurz erläutert.

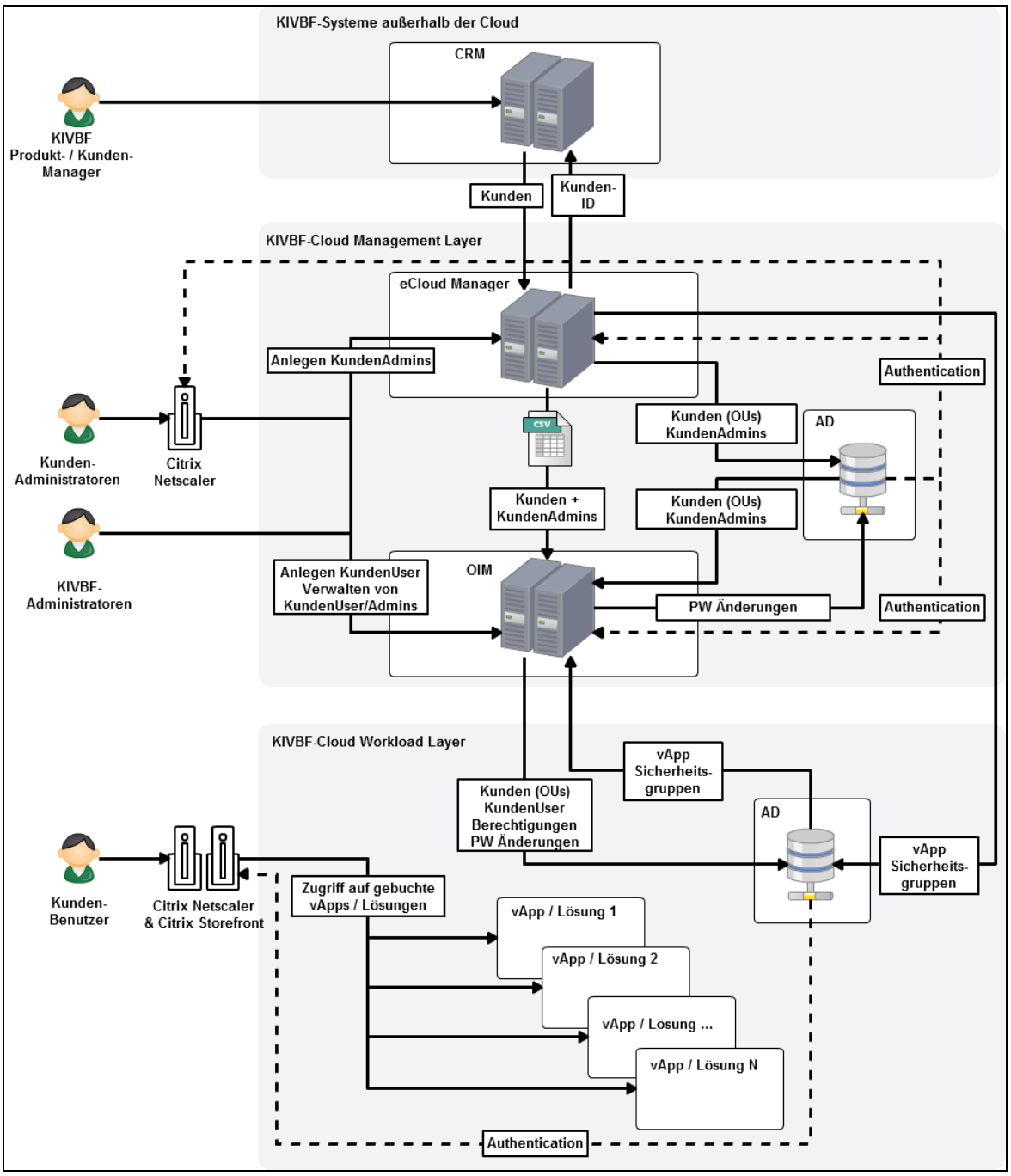

Abb. 3: Architektur der Oracle Identity Manager Lösung

Im Schaubild oben sind zum einen zwei Schichten der Cloud abgebildet:

- Cloud Management Schicht
- Cloud Workload Schicht

Die Cloud hat eine weitere dritte Schicht, die Administrations-Schicht, die aber für das Identity und Access-Management ohne Bedeutung ist und deshalb hier außer Acht gelassen wird. Im Schaubild ist neben den zwei genannten Schichten noch ein Bereich gezeigt, in dem eine Anwendung aufgeführt ist, die außerhalb der Cloud betrieben wird, aber Daten in die Cloud Management Schicht liefert.

Im Folgenden eine Liste der einzelnen Komponenten mit kurzer Funktions-Beschreibung:

- **CRM-System**

  Das CRM-System hat eine Schnittstelle zum eCloud Manager und überträgt an diesen Kundendaten. Im Gegenzug wird eine im eCloud Manager erzeugte eindeutige Kunden-ID in das CRM-System geschrieben.

- **eCloud Manager**

  Im eCloud Manager können Kunden Lösungen buchen und damit die automatisierte Bereitstellung von Landschaften anstoßen. Im eCloud Manager können zudem Kunden-Administratoren manuell angelegt werden.

  Der eCloud Manager hat die oben erwähnte Schnittstelle zum CRM-System, eine Schnittstelle zum OIM und Schnittstellen zu den ADs. Über diese Schnittstellen werden die Daten der Kunden, der Kunden-Administratoren und der von Kunden gebuchten Lösungen übertragen.

- **OIM**

  Der OIM wird vom eCloud Manager mit den Daten der Kunden und Kunden-Administratoren versorgt. Zudem gleicht der OIM Daten mit den ADs ab und zieht sich die Berechtigungen, die Kunden zugeordnet sind, weil sie bestimmte Lösungen gebucht haben.

  Über den OIM können Kunden-Administratoren Benutzer anlegen und pflegen, Berechtigungen vergeben und entziehen, sowie Passwörter zurücksetzen. Diese Aktionen lösen direkte Schreibvorgänge in die ADs aus.

- **AD der Cloud Management Schicht**

  Um Zugriff auf Ressourcen (z.B. eCloud Manager oder OIM) in der Cloud Management Schicht zu haben, muss ein Benutzer gegen das dort vorhandene AD authentifiziert werden. Das AD muss deswegen die Kundenstruktur und die Accounts der Kunden-Administratoren vorhalten, die aus dem eCloud Manager initial kommen und dann mit dem OIM ausgetauscht werden.

- **AD der Cloud Workload Schicht**

  Damit ein Benutzer eine Lösung aufrufen kann, muss er sich gegen das AD der Workload Schicht authentifizieren. Im AD sind demzufolge die Accounts der Benutzer abgelegt, aber auch die Berechtigungen, die ein Benutzer innerhalb der Cloud hat, sprich welche Lösungen der Benutzer sehen und aufrufen kann.

Fazit und Ausblick

Die auf den Oracle Produkten basierenden Lösungen erfüllen die Anforderungen, die sich im Kontext der KIVBF-Cloud ergeben und leisten damit einen wichtigen Beitrag zum Erfolg der KIVBF-Cloud. Die auf der Oracle Enterprise Single Sign-on basierende Lösung bietet den Benutzern einen Komfort, dem für die Akzeptanz der Cloud höchste Bedeutung beigemessen wird.
Der Oracle Identity Manager unterstützt die Anforderungen hinsichtlich der Automatisierung und ermöglicht die Delegierung der Benutzer- und Berechtigungsverwaltung, die nötig ist, um einen effizienten Betrieb der Cloud zu ermöglichen.

Für die Zukunft ist der Ausbau der Lösung innerhalb der KIVBF-Cloud angedacht. Die bisherige Lösung der KIVBF-Cloud greift im aktuellen Status Quo für alle Zugänge auf die Cloud und alle Berechtigungen innerhalb der Landschaften. In einer Ausbaustufe können auch die Berechtigungen innerhalb der Lösungen berücksichtigt werden.

Zudem ist bei der KIVBF bereits ein weiteres Cloud Projekt in der Planung und Umsetzung, nämlich die sogenannte Bildungs-Cloud. Über diese sollen allen Schulen im Land Baden-Württemberg Dienste zur Schulverwaltung, aber auch zu Kollaborationsmöglichkeiten, wie zum Beispiel virtuellen Klassenräumen, bereitgestellt werden. In diesem Szenario werden ca. 4.000 Schulen als Kunden ca. 1,2 Millionen Schüler und Lehrer als Benutzer mit sich bringen. Dies bringt neue Herausforderungen mit sich, für die es auch Lösungsansätze gibt, die den Einsatz des Oracle Identity Managers und weiterer Produkte aus dem Portfolio des Oracle Identity und Accessmanagement Stacks beinhalten.

Kontaktadresse:

Roland Seidelt

virtual7 GmbH

Zeppelinstraße, 2

D-76185 Karlsruhe

Telefon:	+49 (0) 721-619 017 26
Fax:	+49 (0) 721-619 017 29
E-Mail	Roland.Seidelt@virtual7.de
Internet:	www.virtual7.de