

Integrationsplattform Autorisierungsmodul

Studiengang: MAS Information Technology

Betreuer: Igor Lastric

Experte: Prof. Dr. Gerhard Hassenstein (Berner Fachhochschule)

Industriepartner: Galaxis AG, Niederbipp

Der elektronische Datenaustausch mit allen Partnern aus der Gesundheitsbranche hat sich in den letzten Jahren intensiviert. Die Sicherheitsvorschriften für den Umgang mit Daten entwickeln sich laufend weiter und die Informationssysteme sind im Umbau, was eine grosse Flexibilität der Integrationsschicht verlangt. Die Authentifizierung und Autorisierung der Partner spielt dabei eine entscheidende Rolle und muss in die verschiedenen Applikationen integriert werden können.

Ausgangslage

Mehrere Applikationen der Integrationsplattform beziehen Informationen auf unterschiedliche Arten und von verschiedenen Quellen, um Benutzer zu authentifizieren und zu autorisieren. Dabei sind die verwendeten Systeme zur Authentifizierung nur reduziert verfügbar. Mit einer Entkopplung der Systeme soll die Integrationsplattform flexibel auf Veränderungen reagieren können. Dazu muss eine einheitliche Lösung für die Benutzerverwaltung gesucht werden. Die Einführung einer eigenen Benutzerverwaltung erfordert eine eigene Datenhaltung und die REST Service Anbindung.

Analyse

Die bestehenden Prozesse und Benutzerverwaltungen wurden mit einer umfangreichen Anforderungsanalyse erörtert. Daraus entstand ein Dokument mit Anforderungen an die Funktionen und Prozesse. Die wichtigsten Anforderungen bieten die Grundlage für die Produktevaluierung unter einer Vielzahl von verfügbaren Produkten aus dem OpenSource Bereich.

OpenAM, Keycloak und dem Apache Directory Projekt mit dem MyVD Server sind drei Produkte, welche als Lösungsvarianten in Frage kommen. Mit der Methode der Nutzwertanalyse konnten die Lösungen mit den detaillierten Anforderungen überprüft werden. Architektonische Durchstiche wurden als Prototypen mit allen Varianten realisiert und lieferten die notwendigen Informationen für die Beurteilung und später für die Konzeption der gewählten Lösung.

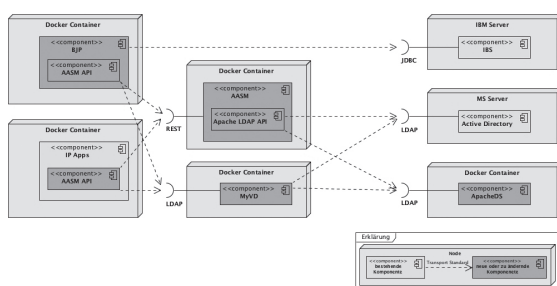
Lösungskonzept

Die gewählte Lösung beinhaltet einen eigenen Directory Server (ApacheDS), eine REST Applikation, den MyVD Server und ein API für die Integration in den Applikationen. Die API beinhaltet alle notwendigen Technologien wie shiro, REST Kommunikation und nachfolgend auch ein Session Management mit MongoDB. Die technischen Konzepte des erstellten Softwarearchitekturdokument beinhalten weitere Ansätze wie z.B. die Verwendung des Post/Redirect/Get Pattern. Die Lösung mit REST und LDAP kann auch für nicht Java-Applikationen verwendet werden.



Daniel Hunziker

danhu@bluewin.ch



Zentrale AASM Applikation für die Authentifizierung und Autorisierung

Ergebnis

Mit dieser Lösung können die angestrebten Ziele wie die Entkopplung, eigene Datenhaltung und die zentrale Verwaltung erreicht werden.

Das Softwarearchitekturdokument mit den verschiedenen Sichten, den detaillierten Konzepten und der Dokumentation aller Entwurfsentscheidungen für die gewählte Lösung bildet den Abschluss dieser Arbeit. Die ausgearbeitete Lösung, wird in naher Zukunft in der Integrationsplattform umgesetzt. Die definierten Massnahmen aus den Erkenntnissen werden in den Entwicklungsprozess einfließen.