Samuel Jost

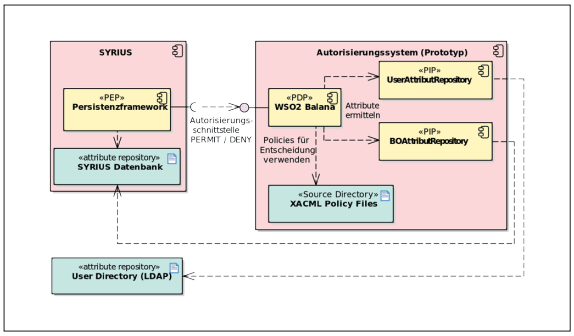
Stefan Kapferer

Diplomanden	Samuel Jost, Stefan Kapferer
Examinator	Prof. Dr. Olaf Zimmermann
Experte	Dr. Gerald Reif, Innovation Process Technology AG, Zug, ZG
Themengebiet	Application Design
Projektpartner	Adcubum AG, St. Gallen, SG

Attributbasierte Autorisierung in einer Branchenlösung für das Versicherungswesen

Analyse, Konzept und prototypische Umsetzung

Beispiel einer funktionalen Anforderung als User Story



Prototyp basierend auf der ABAC-Referenzarchitektur

```
/*
 * VIP-Schutz-Policy-Set
 */
policyset vipPolicySet {
  apply permitOverrides

policy vipPolicy = "http://adcubum.com/vipPolicy" {
  target
   clause bo.metaBoId == -3  or  bo.metaBoId == -7
   clause operation.operationId=="READ" or operation.operationId=="WRITE"
   clause bo.partner.isVIP == true
  apply permitOverrides

  rule allowAccessVIPservice {
   condition syruser.abteilung == "VIPService"
   permit
  }

  rule denyForOthers {
   deny
  }
}
```

Policy in vereinfachter, XACML-basierter Syntax (ALFA)

Ausgangslage: In adcubum SYRIUS®, einer geschichteten ERP-Lösung für Versicherungen, werden Berechtigungen direkt in der Datenbank verwaltet. Zugriffe auf die Daten aus SYRIUS werden in der Persistenzschicht autorisiert. Diese Lösung bringt Probleme mit sich, sobald Datenteilbestände in externen Komponenten, wie zum Beispiel einer Such- und Indexierungslösung, gehalten werden. Um diese Daten zu autorisieren, muss heute zusätzlich SYRIUS aufgerufen werden. Damit zukünftig Daten in einer externen Komponente autorisiert werden können, wurde in der Studienarbeit von Stefan Kapferer ein «Redesign» der Persistenzschicht vorgeschlagen und eine RESTful-HTTP-Schnittstelle für die neue Komponente entworfen. Die vorliegende Arbeit prüft, ob eine auf dem «Attribute-based Access Control»(ABAC)-Paradigma basierende Komponente die jetzige Berechtigungslösung ersetzen kann.

Vorgehen/Technologien: In dieser Bachelorarbeit wurden die fachlichen Schutzanforderungen an die Autorisierungskomponente in Zusammenarbeit mit Kunden von Adcubum aufgenommen und in Form von User Stories erfasst. Anhand der Anforderungen wurde analysiert, welche Informationen das System für die Autorisierungsentscheidungen benötigt und aus welchen Datenquellen diese bezogen werden. Weiter wurde ein Performancekostendach für die Autorisierungsanfragen festgelegt und untersucht, an welchen Stellen der vorgeschlagenen Architektur Performanceoptimierungen möglich sind. Policies zu den wichtigsten funktionalen Anforderungen zeigen auf, dass die technische Umsetzung mit dem ABAC-Paradigma möglich ist. Für die Erstellung der Policies wurden verschiedene Policy-Syntaxen evaluiert, wobei die Entscheidung auf die verbreitete XML-Sprache XACML fiel. Der entwickelte Prototyp verwendet die in der vorangegangenen Studienarbeit definierte Schnittstelle, um Autorisierungsanfragen auf Basis der verfassten XACML-Policies zu verarbeiten. Weiter wurden Vorschläge für das Migrationsvorgehen und dessen Herausforderungen erarbeitet.

Ergebnis: Diese Arbeit liefert die konzeptionellen Grundlagen für die Entwicklung eines ABAC-basierten Autorisierungssystems. Die in dieser Arbeit erfassten funktionalen und nicht funktionalen Anforderungen ermöglichen eine fundierte Evaluation eines Autorisierungsproduktes. Der Prototyp mit den verfassten XACML-Policies zeigt, dass sich die an SYRIUS gestellten Schutzanforderungen mit ABAC umsetzen lassen. Technische Risiken, die der Architekturdesignwechsel hin zu ABAC mit sich bringt, konnten durch diese Arbeit minimiert werden.