

# Policy Authoring Tool

**IT Security / Betreuer: Prof. Gerhard Hassenstein**

**Experte: Prof. Dr. Andreas Spichiger**

**Projektpartner: IBM Research – Zurich, Rüschlikon**

Die Sicherheit von IT-Systemen ist heute ein zentrales Thema für jedes Unternehmen. Eines der wichtigsten Werkzeuge ist die Zugriffskontrolle, welche genau definiert und durchsetzt, wer auf welche Daten oder Anwendungen zugreifen darf. Früher war die Systemvielfalt gut überschaubar und meistens reichten dafür bereits die Funktionen, welche in Betriebssystemen integriert waren. In Zeiten von dedizierten Serverfarmen und serviceorientierter Architektur wird die Kontrolle jedoch komplexer. Diese Arbeit beschäftigt sich mit der kollaborativen Administration moderner Zugriffsrichtlinien.

## Motivation

Mit dem XACML-Standard der OASIS (Organization for the Advancement of Structured Information Standards) wurde eine xml-Notation zum Festlegen von Zugriffsrichtlinien definiert. Dieser Standard ermöglicht Zugriffskontrollsysteme systemübergreifend zu implementieren und Richtlinien zentral zu verwalten. Bereits seit einiger Zeit sind Administrationswerkzeuge für die Verwaltung solcher XACML-Strukturen erhältlich und werden auch produktiv eingesetzt. Diese Lösungen bieten jedoch kaum Möglichkeiten für die kollaborative Arbeit. In der Praxis ist es oft so, dass Mitarbeitende Zugriffsrechte benötigen und diese bei vorgesetzten Stellen beantragen müssen. Diese geben die Anfrage wiederum an andere Stellen zur Umsetzung im System weiter.

## Ziel

Es soll eine Webapplikation entwickelt werden, welche zeigt, wie kollaborative Ansätze im Definieren von Richtlinien angewendet werden können. Die beteiligten Akteure sollen in dieser Applikation neue Zugriffsregeln beantragen können, welche dann in derselben Applikation von anderen Akteuren genehmigt oder abgelehnt werden können. Es gilt sich einen Ansatz zu überlegen, welcher diesen Prozess festlegt und den korrekten Ablauf sicherstellt.

## Umsetzung

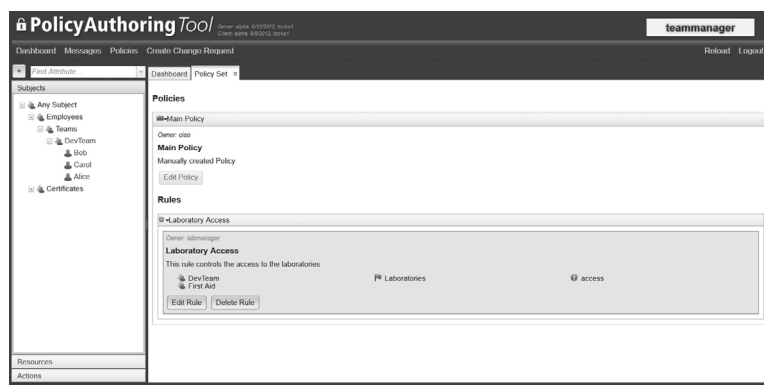
Die Implementation wurde in eine Server- und eine Client-Applikation unterteilt. Der Server basiert auf den Komponenten der Java Plattform (Enterprise Edition). Für die Kommunikation mit dem Client wird ein RESTful Web Service (JAX-RS) verwendet. Dies ermöglicht den datensparsamen und asymmetrischen Austausch von Informationen über das HTTP(S)-Protokoll. Der Client basiert auf dem JavaScript Toolkit Dojo und ist völlig von der Serverseite losgelöst. Der Client bezieht die nötigen Daten über den erwähnten Web Service und stellt dem Benutzer eine angenehme, grafische Darstellung zur Verfügung. Die Applikation ist mit allen bekannten Webbrowsern kompatibel und bietet so einen plattformunabhängigen Zugang. Durch den Einsatz

des Web Services wäre es ausserdem möglich, weitere Clientapplikationen für spezifische Plattformen wie iOS oder Android zu entwickeln.

Mit der Umsetzung des Policy Authoring Tools konnte ein Ansatz veranschaulicht werden, welcher die kollaborative Definition und Administration von Zugriffsrichtlinien ermöglicht. Die Webapplikation kann nun zur Demonstration zukünftiger Administrationskonzepte verwendet werden.



Stefan Tock



Policy Authoring Tool Web-Client