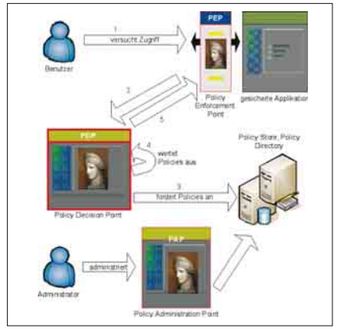
René Eggenschwiler

HERAS^{AF}

Holistic Enterprise-Ready Application Security$^{Architecture\ Framework}$

Manageable policy-based Access Control for J2EE

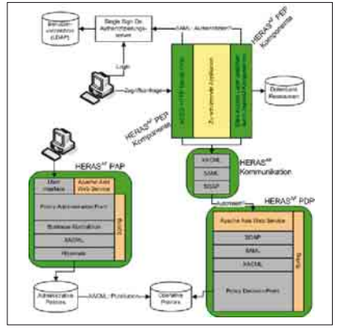
Diplomand	René Eggenschwiler
Examinator	Prof. Dr. Josef M. Joller
Experte	Wolfgang Giersche, Zühlke Engineering AG, Schlieren
Themengebiet	Internet-Technologien und -Anwendungen



Policy-basierte Zugriffskontrolle

Aufgabenstellung: Organisationen betreiben ein komplexes System von IT-Anwendungen. Daher besteht für sie die Notwendigkeit, eine zuverlässige, kundenspezifische Autorisierungslösung zur Verfügung zu stellen. Dies ist eine echte Herausforderung. Wenn es um die Entscheidung geht, wer auf welche Art und Weise zu welchen Ressourcen Zugriff hat oder nicht, können Richtlinien und Policies kompliziert werden und schwierig zu handhaben sein. Die meisten kommerziellen und nicht gewerblichen Anwendungen kommen mit ihrem eigenen Benutzerspeicher und ihren eigenen Zugriffssteuerungsmechanismen daher. Quelloffene, standardisierte Lösungen gibt es noch keine.

Mit HERAS^{AF} wird ein quelloffenes Projekt gestartet, das sich zum Ziel setzt, eine zentral verwaltbare, unternehmenstaugliche Autorisierungslösung zu realisieren. HERAS^{AF} baut auf frei verfügbaren, etablierten und zukunftsträchtigen Technologien und Standards auf. Dabei stehen Interoperabilität, Erweiterbarkeit und Austauschbarkeit der integrierten Komponenten im Vordergrund. Diese Diplomarbeit realisiert den Kern von HERAS^{AF} und legt somit die Basis für das Projekt und dessen Prototyp.



HERAS^{AF} Komponentenschema

Weitere Infos: Die komplette Diplomarbeit sowie auch detailliertere Informationen zu HERAS^{AF} und dessen Weiterführung finden sich unter: http://isys.hsr.ch –> Education –> Completed –> HERAS-AF

Ziel der Arbeit: Design, Realisierung und Dokumentation

- des logischen Struktur-Modells von HERAS^{AF} (XACML 2.0 konform)
- der Integration von Sun's XACML-Implementation
- der Persistenz des Modells mit Hibernate 3
- einer API für die Benutzung des Modells und der Logik des Policy Administration Points

Lösung: In der ersten Phase der Arbeit wurde das Struktur-Modell von HERAS^{AF} entwickelt. Dieses unterstützt alle Definitionen und Funktionen der Richtlinienbeschreibungssprache XACML. Die Aspekte von Persistenz und XACML-Integration wurden dabei komplett voneinander getrennt. In der zweiten Phase des Projektes wurden die Anforderungen und Funktionen realisiert, die den Anspruch der Unternehmenstauglichkeit erfüllen. Dazu gehört die Abstraktion der technischen XACML-Sprache zu einer frei definierbaren Geschäftssprache. Diese Funktionen wurden durch ein konfigurierbares Vorlagensystem realisiert. Entstanden ist eine Multi-Projekt-Lösung mit verschieden verteilbaren Komponenten in Java und J2EE. Somit wurde ein Framework realisiert, das in einer Multi-Server-Umgebung bzw. Multi-Anwendungs-Umgebung eingesetzt und gewartet werden kann. Der HERAS^{AF}-Prototyp hat gezeigt, dass nahezu alle erdenklichen Anwendungsfälle einer ganzheitlichen Autorisierungslösung abgedeckt werden können und eine unternehmenstaugliche Business-Abstraktion realisierbar ist.

Die verschiedenen Standards und Technologien konnten zu einer durchgehenden Lösung vereinigt werden. Mittels «Dependency Inversion» wurden dabei Abhängigkeiten minimal gehalten. Dies führt zu hoher Wartbarkeit, Flexibilität, Erweiterbarkeit, und Skalierbarkeit des Frameworks.