Berechtigungsverwaltung

Studiengang: MAS Information Technology

Die Softwareentwicklung der Bedag Informatik AG hat einen neuen Technologie-Stack ausgearbeitet bei dem mittels OpenID Connect und Keycloak als IAM-System die Authentifizierung gewährleistet werden soll. Wie kann nun die Autorisierung am besten in ein solches System integriert werden?

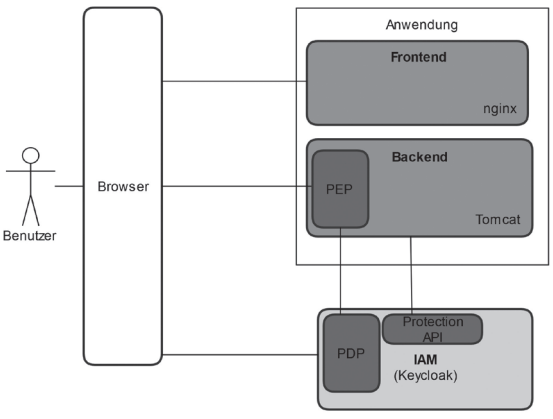
Silvan Strüby

Umfeld

Das Kerngeschäft der Bedag ist die Entwicklung, die Wartung und der Betrieb von geschäftskritischen Informatiklösungen. Um die Vielfalt eingesetzter Technologien über die Applikationen hinweg im Griff zu haben, setzten wir auf die Schaffung von Basiskomponenten. Damit wollen wir die Wiederverwendbarkeit erhöhen. Eine dieser Komponente ist das IAM-System Keycloak.

Ausgangslage

Ziel dieser Arbeit ist, die beste Lösung zur Implementierung von Berechtigungsaspekten in unseren Applikationen aufzuzeigen. Dazu gehört die Prüfung ob unsere Anforderungen an die Berechtigungsverwaltung damit erfüllt werden können. Zukünftig soll so erreicht werden, dass die Berechtigungsverwaltung harmonisiert wird. Als Rahmenbedingung ist gegeben, dass die Lösung auf dem Technologie Stack aufbaut.



Systemübersicht

Umsetzung

In einem ersten Schritt habe ich die Anforderungen der heutigen Applikationen an die bestehenden Berechtigungsverwaltungssysteme erhoben. Darauf aufbauend erarbeitete ich verschiedene Varianten wie die Berechtigungsverwaltung in einer neuen Applikation integriert werden kann. In meinen Varianten legte ich den Fokus insbesondere auf die optimale Platzierung des Policy Decision Point (PDP).
Ich habe die Varianten hinsichtlich der Anforderungen bewertet. Die siegreiche Variante habe ich dann im Rahmen eines Proof of Concept (PoC) prototypisch in einer bestehenden Anwendung umgesetzt, um deren Eignung aufzuzeigen.

Ergebnis

Die Studie hat gezeigt, dass sich der PDP (eine Komponente der Berechtigungsverwaltung) unter unseren Rahmenbedingungen idealerweise ausserhalb der Applikation befindet. Zum einen ergibt dies eine klare Aufteilung der Aufgaben. Zum anderen haben Anpassungen an den Berechtigungen keinen Einfluss auf den Betrieb der Applikation, da dort keine Änderungen vorgenommen werden müssen.
Im PoC habe ich die Applikation dahingehend abgeändert, dass ich im Backend die Berechtigungsprüfungen ausgebaut und durch die Konfiguration eines Policy Enforcement Point (PEP) ersetzt habe. Der PEP nutzt den PDP von Keycloak um die Entscheidung über die Berechtigungsanfrage zu klären. Durch die Protection API von Keycloak kann die Applikation zudem weitere Entscheidungsgrundlagen im PDP erstellen.