# Externe und applikationsinterne Autorisierung in OAuth2 Systemen

Mit OAuth2 ist eine Sicherung von http-Schnittstellen möglich. Hierbei erhält ein Client von einem Autorisationserver einen Token, mit dem er Zugriff auf Schnittstellen eines Resourceservers erhält. Ein valider Token ist mit einer Authentifizierung gleichzusetzen. Die Autorisierung hingegen, also die Entscheidung, ob der Token die benötige Berechtigungen besitzt, lässt sich in dem Resourceserver selbst implementieren oder aber auch auslagern. Bei komplexen Zugriffsrichtlinien und einer heterogenen Applikationslandschaft ist es sinnvoll, die Autorisierung zu entkoppeln.

Eine Entkopplung der Autorisierung ist mittels Open Policy Agent (OPA) möglich. Das hat allerdings zur Folge, dass der Resourceserver jedes Mal bei eingehenden http-Anfragen den OPA-Service um eine Entscheidung fragen muss, d.h. es besteht das Risiko von gravierenden Performanceeinbußen. Da bei einer hohen Last auf Schnittstellen diese i.d.R. durch horizontale Skalierung entlastet werden, können Performanceeinbußen äußerst kostspielig sein.

Es wurden beide Systeme evaluiert unter den Kriterien der Round-Trip-Time (RTT), Datendurchsatz, RAM-Belegung, CPU-Auslastung sowie Ausfallsicherheit. Dazu wurden zwei Testsysteme geschaffen und Performance-und-Lasttests mit dem Tool Apache JMeter durchgeführt und mit JMeter sowie dem Windows Ressourcemonitor die Messwerte protokolliert.

Dabei ist man zu dem Ergebnis gekommen, dass …