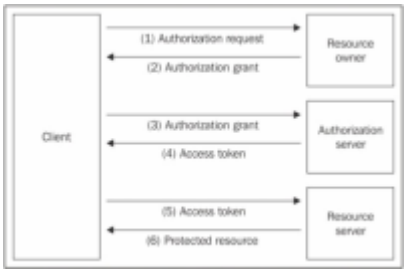
Keycloak

Bei Keycloak handelt es sich um ein open-source Identitäts- und Zugriffsverwaltungssystem, dass es vereinfachen soll Applikationen und Dienste zu sichern. Dabei implementiert es wichtige Standards wie OpenID Connect und SAML. Im Rahmen dieser Arbeit ist lediglich OpenID Connect relevant. Auch ermöglicht Keycloak es Logins von anderen Plattformen wie GitHub oder Twitter zu implementieren. Außerdem kann Keycloak sich auch mit beispielsweise einem Active Directory verbinden, welches oftmals in Firmen eingesetzt wird, um die Nutzer-Daten mit diesem zu teilen. Ein weiteres wichtiges Feature ist die Bedienoberfläche. (Keycloak.org, o.J.)

OAuth und OpenID Connect

Die Unterstützung von OAuth 2.0 in Keycloak stellt eines der wichtigsten Features da. Spasovski beschreibt OAuth 2.0 wie eine schützende Schicht für einen Dienst, sodass die Nutzer-Applikation eine Methode hat, um an geschütze Daten zu gelangen. OAuth 2.0 (voller Titel: “The OAuth 2.0 Authorization Framework”) ist eine Spezifikation eines Protokolls zur Sicherung von Diensten, wobei die Spezifikation Freiraum für verschiedene Implementierung offen hält. Der häufigste Anwendungsfall für OAuth 2.0 sind der Schutz von RESTful APIs und webbasierten Applikationen. (Spasovski, 2013)

Grundfunktionalität

Die Grundfunktionalität lässt sich kurz zusammenfassen: Möchte eine Applikation auf geschützte Daten zugreifen, macht diese sogenannte HTTP Anfragen an einen Server. Dabei wird ein Zugriffstoken mitgeliefert. Dieser Token enthält Informationen, welcher Nutzer der Applikation gestattet auf die Daten zuzugreifen. 

In Abbildung SPASOVSKI_OAUTH wird ein Beispiel einer Authentifizierung gezeigt. Zunächst fragt die Nutzerapplikation den Zugriff auf die geschütze Ressource an. Wird dies gestattet erhält der Nutzer ein “Authorization grant”. Dies enthält dann Informationen über die Authentifizierung. Folgend gibt die Nutzerapplikation den “Authorization grant” weiter an den Authentifizierungsserver. Dieser überprüft den “Authorization grant” und gibt bei Bestätigung einen “Access Token” aus.

Weitere Features

Unterschied zu anderen Authentifizierungsmethoden

Implementierung in Keycloak

From:
https://wiki.eolab.de/ - **HSRW EOLab Wiki**

Permanent link:
https://wiki.eolab.de/doku.php?id=user:jan001:ba:keycloak&rev=1612971982

Last update: **2021/08/24 17:34**