Authentifizierung und Autorisierung in der IT

Grundlagen und Konzepte

2 Anwendungsfälle

As we've come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided.

Art Wittmann

Warum Authentifizierung und Autorisierung in der IT heute ein entscheidender Faktor sind, lässt sich kurz und knapp mit dem hohen Geschäftswert von Daten beantworten. Außerdem mit dem Umstand, dass IT-Systeme im täglichen Geschäftsbetrieb unverzichtbar sind.

Offen ist die Frage: Wann sind Authentifizierung und Autorisierung relevant?

Die kurze und knappe Antwort: Jedes Mal, wenn der Zugriff auf Daten und Systeme erfolgen soll. Diese Situationen lassen sich in acht verschiedene Anwendungsfälle unterscheiden. Bei einigen Anwendungsfällen scheinen die Unterschiede eher geringfügig zu sein und fallen im ersten Moment nicht auf. Bei anderen ist der Unterschied sofort ersichtlich.

Die nachfolgenden Anwendungsfälle beschreiben daher stets eine eindeutige Ausgangssituation. Dazu gehört etwa, ob ein Anwender mit einem vertrauenswürdigen Client oder einem nicht-vertrauenswürdigen Client zugreifen möchte, ob der Anwender Informationen teilen oder auf Ressourcen zugreifen möchte, ob sich der Anwender mit einem allgemeinen Profil oder einem speziellen Profil authentifizieren möchte und Ähnliches.

2.1 Vertrauenswürdiger Client

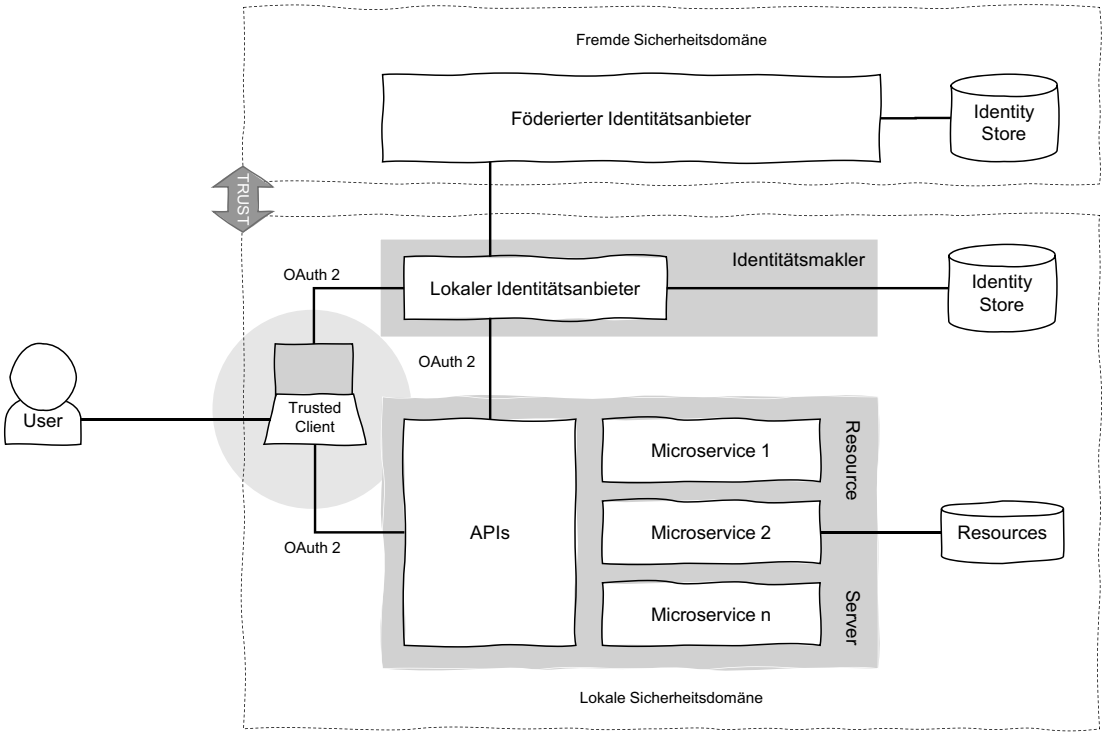

Bild 2.1 Vertrauenswürdiger Client: Der Anwender greift mit einem vertrauenswürdigen Client zu.

Einer der am häufigsten anzutreffenden Anwendungsfälle ist der Zugriff eines Anwenders mit einem vertrauenswürdigen Client. Dieser ist im Unternehmenskontext alltäglich. Bild 2.1 stellt diesen Anwendungsfall in der Übersicht dar.

Der Ausgangspunkt ist, dass der Anwender auf ihm gehörende oder ihm zugeordnete Ressourcen zugreifen möchte und dafür einen vertrauenswürdigen Client nutzt. Dieser Client gehört zur lokalen Sicherheitsdomäne, etwa eines Unternehmens.

Die Ressource selbst wird durch einen Microservice bereitgestellt, der wiederum durch eine API abgesichert ist. Auch die API ist geschützt respektive der Zugriff auf die API. Hierfür kommt ein lokaler Identitätsanbieter zum Einsatz. Der Zugriff auf die Ressource erfolgt also nicht direkt, sondern über mehrere Zwischenschritte, die die Sicherheitsrichtlinien umsetzen. Der Resource Server, der den Zugriff auf die Ressource schützt, prüft dann per OAuth Introspection das Token beim Identitätsanbieter auf Gültigkeit.

Mit OAuth, siehe Abschnitt 4.5, lässt sich dieser Anwendungsfall hervorragend absichern. Dabei bieten sich gleich drei verschiedene Grant Types an:

- *Authorization Code Grant Type*, beschrieben in Abschnitt 4.5
- *Resource Owner Credentials Grant Type*, beschrieben in Abschnitt 4.5
- *Client Credentials Grant Type*, beschrieben in Abschnitt 4.5

Das Bild 2.1 zeigt auch eine fremde Sicherheitsdomäne, die aber nicht in jedem Anwendungsfall vorkommen muss. Der Identitätsmakler dient in diesem Fall dazu, zwischen Identitätsanbietern einer lokalen und einer fremden Sicherheitsdomäne zu vermitteln. Wichtig ist dabei, dass zwischen der lokalen und der fremden Sicherheitsdomäne eine Vertrauensbeziehung bestehen muss.

2.2 Single Page Application

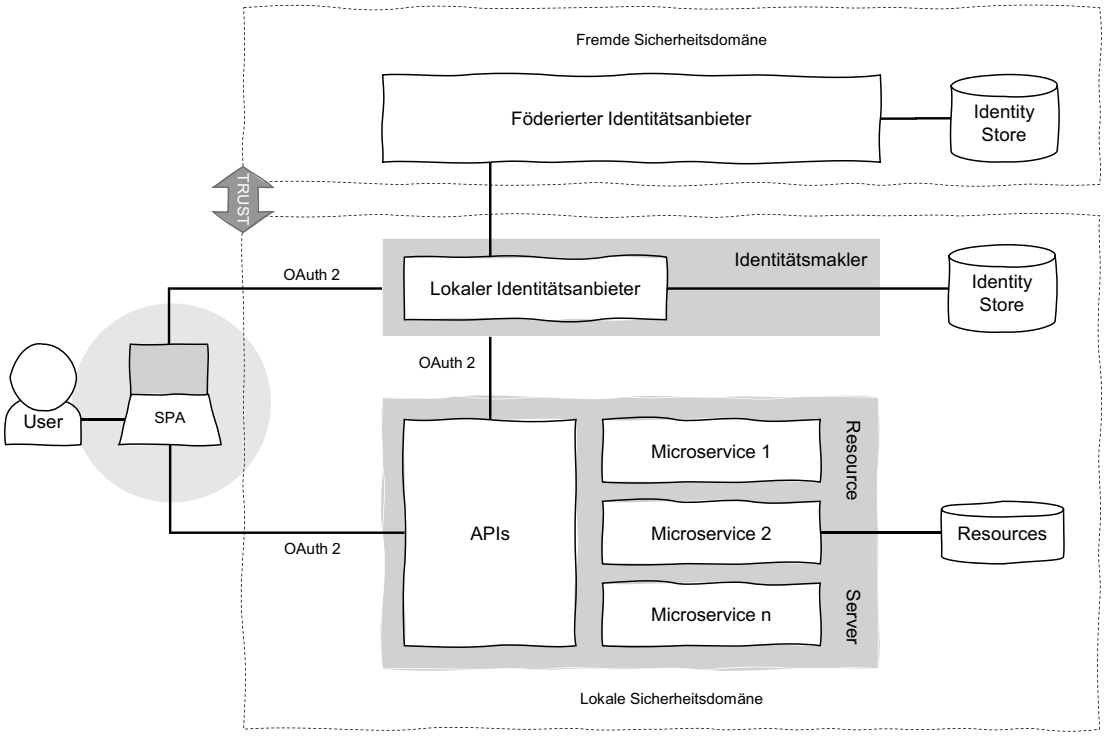

Bild 2.2 Single Page Applications: SPAs gelten generell als nichtvertrauenswürdige Clients. Grund ist, dass sich Code und Speicherbereich meist problemlos einsehen lassen.