**DIPLOMARBEIT**

**Gesamtprojekt**

**Gewinnspielapp / Veranstaltungskarten**

Ausgeführt im Schuljahr 2023/24 von: Betreuer:

Berke AKIN 5cWI Eduard Hallinger

Marc MADLENER 5cWI Eduard Hallinger

Dornbirn, am …………..

Abgabevermerk

Diplomarbeit, am …………… Eduard Hallinger

**EIDESSTAATLICHE ERKLÄRUNG**

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegeben Quellen und Hilfsmittel nicht benutzt und die den benutzten Quellen wortwörtlich und inhaltlich entnommenen Stellen als solche erkenntlich gemacht habe.

Dornbirn, am ……………

………………………………

Berke Akin

………………………………

Marc Madlener

**DIPLOMARBEIT**

**DOKUMENTATION**

Name der Verfasser: Berke Akin, Marc Madlener

Jahrgang | Schuljahr: 5cWI | 2023/24

Thema der Diplomarbeit: Gewinnspielapp / Veranstaltungskarten

Kooperationspartner: Bernhard Lang

Vorwort

Table of Contents

[**1.** **ZIELSETZUNG** 5](#_Toc155285220)

[**2.** **AUFGABENSTELLUNG** 5](#_Toc155285221)

[2.1 Aufgabenstellung 5](#_Toc155285222)

[**3.** **OpenID Connect** 5](#_Toc155285223)

[3.1 OpenID Connect - Allgemein 5](#_Toc155285224)

[3.2 OpenID Connect – Funktionsweise 6](#_Toc155285225)

[3.3 OpenID Connect – Anwendung in der Arbeit 7](#_Toc155285226)

# **ZIELSETZUNG**

# **AUFGABENSTELLUNG**

## 2.1 Aufgabenstellung

Die Firma Rauch bekommt Karten zugeschickt, die sie unter den MitarbeiterInnen verteilen können. Es bleiben immer Karten übrig und diese werden unter den MitarbeiterInnen verlost. Die Karten werden als PDF mithilfe einer RestAPI in das Gewinnspiel integriert. Das Gewinnspiel basiert auf dem First Come / First Serve Prinzip. Man kann ein Gewinnspiel erstellen, wo die Mitarbeiter teilnehmen können. Der Gewinner wird nach Ende des Gewinnspiels informiert und kann sich die Karte anschauen und abholen.

Die Firma Rauch stellt uns dabei einen Server und eine Datenbank zur Verfügung. Die Anwendung wird webbasiert sein, weshalb wir bei diesem Projekt das JavaScript Framework VueJS verwenden werden.

# **Single Sign on**

## OpenID Connect - Allgemein

OpenID Connect ist ein offenes Authentifizierungsprotokoll, das Oauth 2.0 profitiert und um eine zusätzliche Identitätsebene erweitert. Über OIDC können Clients die Identität eines Endnutzers mit Hilfe der Authentifizierung durch einen Autorisierungsserver bestätigen. Das Einbinden von OIDC in Ergänzung von OAuth 2.0 schafft ein einzelnes Framework, das die Sicherung von APIs, mobilen nativen Anwendungen wie auch Browser-Anwendungen in einer einzigen kohärenten Architektur verspricht.

## OpenID Connect – Funktionsweise

Die Anwendung beginnt mit einem OAuth-Fluss, der den Nutzer zur Autorisierung einer Anfrage auffordert. Im Zuge dieses Flusses schließt der Client den OpenID Connect-Bereich gemeinsam mit Bereichen für jede zusätzliche Benutzerinformation ein, die er benötigt.

Nach der Verarbeitung der Anfrage erhält der Client ein Zugriffs-Token und ein ID-Token, die von dem Autorisierungsserver ausgestellt werden, der Anfragen mit Daten dieses Nutzers enthält. Die SSO-Erfahrung des Nutzers basiert auf der Übermittlung des ID-Tokens vom Autorisierungsserver an den Client. Der Client kann anschließend einen speziellen Endpunkt auf dem Autorisierungsserver ansprechen, der auch als UserInfo-Endpunkt bezeichnet wird, um dort die übrigen Anfragen über den Nutzer abzurufen.

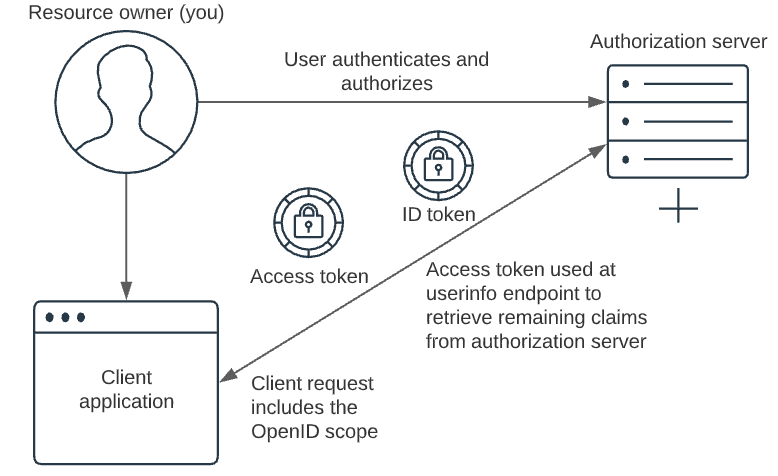


Abbildung 1: OpenID Connect Funktionsweise

## OpenID Connect – Anwendung in der Arbeit

Im Rahmen unserer Diplomarbeit wird OpenID Connect als essenzielles Protokoll für den Single Sign-On (SSO) des Benutzers implementiert. Die primäre Zielsetzung besteht darin, dem Benutzer eine nahtlose und effiziente Authentifizierung zu ermöglichen, indem er sich lediglich einmal anmelden muss und anschließend uneingeschränkten Zugang zu den Ressourcen erhält, ohne wiederholt Zugangsdaten eingeben zu müssen.

Durch die Nutzung von OpenID Connect wird ein benutzerzentrierter Ansatz verfolgt, der es dem Nutzer gestattet, nach erfolgreicher Anmeldung sämtliche Funktionalitäten der Seite vollständig zu nutzen. Dieser Prozess garantiert eine reibungslose Benutzererfahrung, indem der Benutzer nach dem Authentifizierungsvorgang unmittelbar auf die benötigten Ressourcen zugreifen kann.

Des Weiteren ermöglicht OpenID Connect die Zuweisung von Rollen im Rahmen des SSO. Dies bedeutet, dass dem angemeldeten Benutzer spezifische Berechtigungen und Zugriffsrechte zugewiesen werden, um seine Interaktion mit der Plattform zu regeln. Dadurch wird ein individualisierter und sicherer Zugang zu den unterschiedlichen Funktionalitäten gewährleistet, während gleichzeitig die Integrität der Daten und des Systems gewahrt bleibt.

Die Integration von OpenID Connect in unsere Diplomarbeit dient dem Zweck, eine hochgradig benutzerfreundliche, sichere und effiziente Authentifizierungsmethode zu implementieren, die die Grundlage für ein optimales Nutzungserlebnis bildet.

* 1. Microsoft Authentication Library

Die Microsoft Authentication Library (MSAL) ermöglicht es Entwicklern, Tokens von der Microsoft-Identitätsplattform zu erwerben, um Benutzer zu authentifizieren und auf gesicherte Web-APIs zuzugreifen. Sie kann verwendet werden, um sicheren Zugriff auf Microsoft Graph, andere Microsoft-APIs, Web-APIs von Drittanbietern oder Ihre eigene Web-API zu ermöglichen. MSAL unterstützt viele verschiedene Anwendungsarchitekturen und Plattformen, darunter .NET, JavaScript, Java, Python, Android und iOS. MSAL kann wie bei unserer Diplomarbeit für Webanwendungen benutzt werden, wo man Benutzer angemeldet werden müssen.

* 1. Azure Portal

Das „Azure Portal“ ist eine webbasierte Plattform, die von Microsoft für die Verwaltung und Überwachung von Azure-Ressourcen bereitgestellt wird. Azure ist Microsofts Cloud-Computing-Plattform, die eine Vielzahl von Diensten und Ressourcen für Unternehmen und Entwickler bietet. Das Azure Portal fungiert als zentrale Anlaufstelle, über die Benutzer auf ihre Azure-Ressourcen zugreifen, sie konfigurieren und überwachen können. Ein großer Vorteil ist die Rollenverwaltung, um sicherzustellen, dass nur autorisierte Personen auf bestimmte Ressourcen zugreifen können.

3.6 Verwaltung von Berechtigungen

Berechtigungen sind ein wesentlicher Bestandteil unserer Diplomarbeit. Die Definition und Zuteilung von Rollen erfolgt dabei über das Azure Portal, wo sämtliche Mitarbeiter ihre entsprechenden Rollen zugeteilt bekommen. Eine dieser Rollen ist die des "EventCreators". Diese spezifische Berechtigung ermöglicht es den autorisierten Personen, Events zu erstellen, wobei sie wichtige Informationen wie Anfangs- und Enddatum, eine detaillierte Beschreibung sowie die Option zum Hochladen von PDF-Dateien eingeben können.

Um diese Berechtigungsstruktur zu realisieren, greifen wir auf MSAL (Microsoft Authentication Library) zurück, welches eine nahtlose Integration in das Azure Portal ermöglicht. Dort erfolgt die Überprüfung, ob die betreffenden Personen die Rolle des "EventCreators" innehaben. Nur wenn dies der Fall ist, erhalten sie die notwendigen Zugriffsrechte, um Events zu erstellen.