White-Paper: Single Sign-On mit Microsoft Entra ID (ehem. Azure Active Directory)

Inhalt

Über dieses White-Paper....3
Zusammenfassung....3
Gilt für....3
Status....3

Theorie....4
Einführung....4
Hintergrund....4

Umsetzung....5
Voraussetzungen....5
Konfiguration....5
Anwendung....6

Weitere Informationen....7

Rechtliche Hinweise....8

Über dieses White-Paper

Änderungsstand: 2024.2.1-SNAPSHOT

Autor: Markus KARG (karg@quipsy.de)

Zusammenfassung

Die Einrichtung von **Microsoft Entra ID** (ME-ID), ehem. Azure Active Directory, als OpenID Connect Identity Provider (OIDC IdP) ermöglicht die Anmeldung an QUIPSY® mit Microsoft Entra ID-Benutzerkonten.

Gilt für

- QUIPSY® 2024.2.1-SNAPSHOT

Status

Dies ist ein offizielles Whitepaper für QUIPSY® 2024.2.1-SNAPSHOT.

Theorie

Einführung

Unternehmen bieten ihren Mitarbeitern eine Vielzahl an Anwendungen, um die betrieblichen Aufgaben zu erfüllen. Bestimmte Anwendungen, beispielsweise QUIPSY®, müssen die *Identität* des Anwenders kennen, beispielsweise um den Zugang zu Anwendungen oder bestimmten Funktionen zu beschränken. In der Folge müssen sich Nutzer an *mehreren* Anwendungen anmelden, d. h. ihre Identität *immer wieder* belegen, beispielsweise mittels der Kenntnis eines Passwortes.

Um diese vielen Anmeldevorgänge zu reduzieren, aber auch um modernere bzw. sicherere Identitätsnachweise nutzen zu können, setzen Unternehmen *SSO* (Single Sign-On) ein. Hierbei erfolgt eine Trennung in ein zentrales, *identifizierendes* System, den sogenannten *Identitätsprovider* (IdP), und die Anwendungen, welche keine eigenständige Identitätsfeststellung mehr vornehmen, sondern eine vom IdP geprüfte und bestätigte Identität *nutzen*.

Viele Unternehmen setzen zur zentralen Identitätsverwaltung *Microsoft Entra ID* (ehem. *Azure Active Directory*) ein, einen Teil der *Microsoft Azure* Cloud.

Dieses White-Paper beschreibt, wie sich *Microsoft Entra ID* als SSO-Lösung mit QUIPSY® einrichten und nutzen lässt.

Hintergrund

- **SSO** (Single Sign-On) bezeichnet Verfahren und Technologien zur einmaligen, zentralen Anmeldung eines Benutzers mit dem Ziel, *alle* Anwendungen zu verwenden, ohne sich an *jeder* Anwendung getrennt anmelden zu müssen.
- **OIDC** (OpenID Connect) ist ein internationaler Industriestandard für Single Sign-On, der eine weltweit einheitliche Schnittstelle zu Identitätsprovidern (IdP) normiert. Dieser wird von vielen IdP, wie beispielsweise ME-ID, implementiert und von vielen Anwendungen, wie beispielsweise QUIPSY®, unterstützt.
- **ME-ID** (Microsoft Entra ID, ehem. Azure Active Directory) ist ein OIDC-konformer IdP der Fa. Microsoft, der als Teil von *Microsoft Azure* seine Benutzerkonten im Cloud-Angebot der Fa. Microsoft verwaltet. ME-ID ist integraler Bestandteil der Azure-Cloud, muss jedoch zur Verwendung mit QUIPSY® konfiguriert werden.

Umsetzung

Voraussetzungen

- QUIPSY® ist installiert und betriebsbereit konfiguriert und Sie verfügen über die notwendigen Kenntnisse und Berechtigungen, um Änderungen an QUIPSY® vorzunehmen.
- Anwender sind in QUIPSY® angelegt und diese können sich erfolgreich an QUIPSY® anmelden.
- Microsoft Entra ID ist betriebsbereit eingerichtet und Sie verfügen über die notwendigen Kenntnisse und Berechtigungen, um Änderungen an diesem ME-ID-Mandaten vorzunehmen.
- Anwender sind in Microsoft Entra ID angelegt und diese können sich erfolgreich an Microsoft Entra ID anmelden.
- Der Betriebsablauf darf unterbrochen werden. **Während der Abarbeitung dieses White-Papers ist QUIPSY® nicht nutzbar.**

Konfiguration

Die grundsätzliche Einrichtung von OIDC ist im QUIPSY®-Handbuch beschrieben. Dieses White-Paper beschreibt darüber hinausgehend die speziellen Belange von ME-ID, die hierbei zu berücksichtigen sind.

Hinsichtlich der im Folgenden gezeigten Befehle wird auf die jeweiligen Produkthandbücher verwiesen.

Grundsätzliches

Die gesamte ME-ID-Administration, incl. der Anmeldung von OIDC-Clients (somit also von QUIPSY®), erfolgt über die Entra-Webseite. Die OIDC Client ID wird durch ME-ID *automatisch* zugeteilt.

QUIPSY® als OIDC-Client in Microsoft Entra ID konfigurieren

Die Konfiguration von OIDC auf ME-ID ist grundsätzlich unter https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-protocols-oidc beschrieben.

Die in ME-ID vorzunehmende App-Registrierung benötigt eine Plattform-Konfiguration vom Typ "Single-Page-Web-Anwendung". In dieser sind die folgenden Umleitungs-URIs zu hinterlegen:

- `https://quipsy:8080/oidc/callback`
- `http://quipsy:8080/oidc/callback`

Die folgende Option muss aktiviert sein:

- `Der Umleitungs-URI ist für den Autorisierungscodeflow mit PKCE berechtigt.`

Darüber hinaus ist im Bereich `Implizite Genehmigung und Hybridflows` die folgende Option einzuschalten:

- `ID-Token`

Microsoft Entra ID in QUIPSY® als IdP konfigurieren

Die in QUIPSY® zu hinterlegende Kennung (`iss`) hat den folgenden Aufbau: `https://login.microsoftonline.com/<Mandanten-ID>/v2.0` und wird über diesen Befehl in QUIPSY® hinterlegt:

```
quipsy admin oidc add-client --iss <iss> --client-id
 <client-id>
```

Microsoft-Entra-ID-Konten zu QUIPSY®-Konten zuordnen

Jedes QUIPSY®-Konto, das sich per ME-ID anmelden können soll, benötigt die Zuordnung des betreffenden ME-ID-Kontos.

Dies kann *durch die betroffene Person selbst* erfolgen, sofern diese über einen alternativen Anbieter (z. B. die interne QUIPSY®-Anmeldung) angemeldet ist. Hierzu ist der Menüpunkt "Verbinde OIDC-Konto" zu wählen. In der Folge erscheint eine Auswahl der administrativ konfigurierten OIDC-IdPs, sofern mehr als ein einziger IdP konfiguriert ist. Nach Auswahl des IdPs (bzw. automatisch, wenn nur ein einziger IdP konfiguriert ist), erscheint die Anmeldemaske des IdP. Sobald an dieser eine erfolgreiche Anmeldung durchgeführt wurde, ist die Zuordnung des betreffenden Kontos abgeschlossen.

Alternativ kann die Hinterlegung *durch eine Person mit Administrationsbefugnis* per CLI erfolgen. ME-ID besitzt keinen Befehl und auch keine Benutzeroberfläche, um die benötigte Kennung (`sub`) zu ermitteln, diese kann jedoch über den Umweg einer OIDC-API-Anfrage im Browser herausgefunden werden. Hierzu ist der folgende URL-Aufbau anzuwenden:

```
https://login.microsoftonline.com/<Mandaten-
ID>/oauth2/v2.0/authorize?client_id=<client-
id>&response_type=id_token&redirect_uri=https://quipsy:8080/
oidc/callback&scope=openid&nonce=12345
```

Der Befehl zur Hinterlegung der Kennung (`sub`) in QUIPSY® ist:

```
quipsy admin oidc add-account --user-id <user-id> --iss
 <iss> --sub <sub>
```

Anwendung

ME-ID zeigt beim QUIPSY®-Login eine Anmeldeseite.

Auf der Anmeldeseite sind der AD-Kontoname und das zugehörige Passwort einzutragen.

Je nach Konfiguration erlaubt ME-ID die Speicherung der Anmeldung im Sinne von SSO.

Flackert statt der Anmeldeseite nur kurz ein Popup-Fenster auf und verschwindet dann sofort wieder, hat ME-ID im Sinne von SSO eine zuvor gespeicherte Anmeldung wiederverwendet.

Weitere Informationen

- Weitere Informationen zu **OpenID Connect** sind auf der Webseite der OpenID Foundation (OIDF) zu finden.
- Weitere Informationen zu **Microsoft Entra ID** (ehem. Azure Active Directory) sind auf der Webseite der Microsoft Corporation zu finden.
- Weitere Informationen zu **QUIPSY®** finden Sie im Handbuch.

Rechtliche Hinweise

Alle genannten Markennamen sind durch die jeweiligen Markeninhaber geschützt und dürfen nicht ohne entsprechenden Hinweis verwendet werden.