White-Paper: Single Sign-On mit Auth0

Inhalt

Über dieses White-Paper

Änderungsstand: 2023.0.1-SNAPSHOT

Autor: Markus KARG (karg@quipsy.de)

Zusammenfassung

Die Einrichtung von **Auth0** als OpenID Connect Identity Provider (OIDC IdP) ermöglicht die Anmeldung an QUIPSY® mit Auth0-Benutzerkonten.

Gilt für

- QUIPSY® 2023.0.1-SNAPSHOT

Status

Dies ist ein offizielles Whitepaper für QUIPSY® 2023.0.1-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 *Auth0* ein, einen Onlinedienst der Fa. Okta.

Dieses White-Paper beschreibt, wie sich *Auth0* 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 Auth0, implementiert und von vielen Anwendungen, wie beispielsweise QUIPSY®, unterstützt.
- **Auth0** ist ein OIDC-konformer IdP der Fa. Okta, der seine Benutzerkonten im Cloud-Angebot dieses Unternehmens verwaltet. Auth0 muss 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.
- Ein Auth0 Tenant ist betriebsbereit eingerichtet und Sie verfügen über die notwendigen Kenntnisse und Berechtigungen, um Änderungen an diesem Auth0-Tenant vorzunehmen.
- Anwender sind in diesem Tenant angelegt und diese können sich erfolgreich an diesem Tenant 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 Auth0, die hierbei zu berücksichtigen sind.

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

Grundsätzliches

Die gesamte Auth0-Administration, incl. der Anmeldung von OIDC-Clients (somit also von QUIPSY®), erfolgt über die Auth0-Webseite. Die OIDC Client ID wird durch Auth0 *automatisch* zugeteilt.

QUIPSY® als OIDC-Client in Auth0 konfigurieren

Die Konfiguration von OIDC auf Auth0 ist grundsätzlich unter https://auth0.com/docs beschrieben.

Auf Auth0 ist über die Schaltfläche `+ Create Application` eine Anwendung mit dem Application Type `Single Page Web Application` anzulegen. In dieser sind die folgenden Umleitungs-URIs unter `Allowed Callback URIs` zu hinterlegen:

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

Im Abschnitt `Advanced Settings` müssen die folgenden Optionen aktiviert sein:

- `OIDC Conformant` auf dem Reiter `OAuth`
- `Password` auf dem Reiter `Grant Types`, wenn die Anmeldung des Anwenders *über ein Passwort* erfolgen soll

Auth0 in QUIPSY® als IdP konfigurieren

Die in QUIPSY® zu hinterlegende Kennung (`iss`) hat den folgenden Aufbau: `https://<tenant-domain>/`, wobei die Tenant Domain auf Auth0 in der Application-Konfiguration auf dem Reiter `Settings` unter dem Stichwort `Domain` genannt wird. Dort ist ebenso die Client-ID zu finden. Diese wird über diesen Befehl in QUIPSY® hinterlegt:

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

Auth0-Konten zu QUIPSY®-Konten zuordnen

Jedes QUIPSY®-Konto, das sich per Auth0 anmelden können soll, benötigt die Zuordnung des betreffenden Auth0-Kontos.

Auth0 zeigt die benötigte Kennung (`sub`) auf der Detailseite eines Auth0-Users in der Titelzeile unter dem Stichwort `user_id` an.

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

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

Anwendung

Auth0 zeigt beim QUIPSY®-Login eine Anmeldeseite.

Auf der Anmeldeseite sind der Auth0-Kontoname und das zugehörige Passwort einzutragen.

Je nach Konfiguration erlaubt Auth0 die Speicherung der Anmeldung im Sinne von SSO.

Flackert statt der Anmeldeseite nur kurz ein Popup-Fenster auf und verschwindet dann sofort wieder, hat Auth0 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 **Auth0** sind auf der Webseite der Okta, Inc. 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.