Möglicher Single Sign On-Workflow für ein System mit einer Adressse / Instanz, aber ohne nachfolgenden Datenaustausch.

Anwendungsgebiet: Viele Steuerberater / viele Mandanten greifen von einer (Buchhaltungs-)System-Adresse auf kontool zu. Dieses jene (Buchhaltungs-)System ist für alle Steuerberater mit der gleichen (Web-)Adresse erreichbar.

Basis: OAuth 2.0 Protokoll.

Benötigt wird mindestens ein Endpunkt, mit dem kontool Kontakt für die Autorisierung aufnehmen kann – idealerweise sind es zwei.

Beispielhaft:

1. https://www.buchhaltungs-instanz.de/oauth2/auth.php
2. https://www.buchhaltungs-instanz.de/oauth2/token.php

Im Folgenden wird von folgender Adresse der Buchhaltungs-Instanz ausgegangen: https://buchhaltungs-instanz.de

1.) Mandant / Nutzer klickt auf einen Button/Link um sich in kontool anzumelden:

https://www.mykontool.de/auth?system=[ID von kontool vergeben]

2.) Daraufhin baut kontool einen Link zusammen, der den Nutzer zur folgenden Seite auf der Buchhaltungs-Instanz weiterleitet:

(beispielhaft:)

https://buchhaltungs-instanz.de/oauth2/auth.php?client_id=f11233fc-da7b-4b77-a05d-1e65b2f08cbe&redirect_uri=https://www.mykontool.de/auth/in&state=vesPfawcxQnvB6voG9tf59rHslstbn

Erklärung der Parameter, die kontool liefert:

- client_id => ist eine eindeutige, öffentliche ID, die kontool bezeichnet und die wir mit Ihnen vereinbart haben und auf Ihrer Seite gegengeprüft werden muss.
- redirect_uri => ist eine eindeutige URL, zu der User später weitergeleitet wird -> muss ebenfalls auf Ihrer Seite gegengeprüft werden, darf nicht irgendeine Adresse sein.

  Dies sollte als Liste ausgeführt sein, also mit mehreren gültigen URLs – denn es wird mehrere URLs geben, z.B. auf den Testserver).

  - https://www.mykontool.de/auth/in
  - https://thunder.mykontool.de/auth/in
  - https://localhost:50019/auth/in
- state => verhindert CSRF Attacken und ermöglicht uns eine Zuordnung zur Buchhaltungs-Instanz.

[Es gibt noch andere Parameter im OAuth 2.0 Protokoll, aber diese werden hier erstmal nicht beachtet]

3.) Auf der oben genannten Seite (Buchhaltungs-Instanz) muss sich der Nutzer nun anmelden, sollte er nicht schon angemeldet sein.

4.) Nach der Anmeldung oder wenn der Nutzer schon angemeldet ist, wird er wieder zu der angegebenen kontool Adresse weitergeleitet (siehe „redirect_uri“ in Schritt zwei):

https://www.mykontool.de/auth/in?code=MP84YXJfvf8lNsOtLlgLDsMdW9ZBSdjB6Q&state=vesPfawcxQnvB6voG9tf59rHslstbn

Erklärung der Parameter:

- code => ist ein zufällig von der Buchhaltungs-Instanz generierter, eindeutiger Code, der dem Nutzer zugeordnet und nur für 60s gültig ist.
- state => ist eins zu eins der ursprünglich von kontool im Schritt zwei mitgeschickte „state“.

5.) kontool schickt daraufhin im Hintergrund per POST eine Anfrage mit dem „code“ aus Schritt 4 an die Steuerberater-Instanz, ergänzt um Sicherheitsinformationen, die klarstellen, dass kontool Zugriff haben will:

```
POST /oauth2/token.php HTTP/1.1
Host: buchhaltungs-instanz.de

client_id=f11233fc-da7b-4b77-a05d-1e65b2f08cbe&client_secret=iNumzT
49a77d3ca0f9afewWGFERdfrehgtrh342VHstrqWesH8tm9&code=
MP84YXJfvf8lNsOtLlgLDsMdW9ZBSdjB6Q&redirect_uri=https://www.mykontool.de/auth/in
```

Erklärung der Parameter:

- client_id => die eindeutige, öffentliche ID aus Schritt zwei.
- client_secret => ist ein privater, nicht öffentlich bekannter Schlüssel, der kontool identifiziert und den wir mit Ihnen vereinbart haben und auf Ihrer Seite gegengeprüft werden muss.
- code => ist der „code“ der Buchhaltungs-Instanz aus Schritt vier.
- redirect_uri => mit welcher (kontool-)Adresse wurden ursprünglich die Abfragen gestartet.

6.) Bei erfolgreicher Überprüfung der mitgeschickten Parameter liefert die Buchhaltungs-Instanz Benutzerinformationen als Antwort an die POST-Anfrage in Schritt fünf an kontool zurück:

z.B. als JSON:

```
{
  "user_guid": "cULSIjwefxfexx32xxIhbgbjX0R6MkKO",
  "user_email": "testuser@test.de",
  "user_companyname": "Testfirma",
  "user_type": "0",
  "user_accountant_guid": "9035ca6c-543e-4740-8229-1cc1bd30c08b ",
  "user_active": "1",
  "system_url": "https://stb-mueller.de",
  …
}
```

Erklärung der Parameter:

- user_guid => eine eindeutige ID aus der Buchhaltungs-Instanz - nicht die E-Mail-Adresse, da sich diese ja im Laufe der Zeit ändern könnte.
- user_email => E-Mail-Adresse des Nutzers.
- user_companyname => Unternehmensname.
- user_type => bezeichnet, ob es sich um einen Steuerberater (1) oder Mandanten (0) handelt
- user_accountant_guid => wenn Nutzer Typ „Mandant“ dann gibt dies die eindeutige ID des Steuerberaters wieder.

  [Optional, nur in Mehrbenutzersystemen]
- user_active => ist der Nutzer noch aktiv (1) oder nicht mehr (0).
- … weitere Parameter, z.B. Berater/Mandantennummer…