DARC-SSO

Die Anbindung an den DARC-Single-Sign-On erfolgt über die Klasse SsoDARC.class.php.

Beim Aufruf der Factory-methode "CreateForClient" wird die URL ./well-known/openid-configuration vom DARC-SSO / Test-SSO geladen und bei weiteren Aufrufen werden die dort hinterlegten Endpunkte verwendet. Parameter für diese Methode sind ClientId und ClientSecret, die Rücksprungadresse sowie ein Flag ob PROD- oder Test-Umgebung

Die Methode "GetLoginUrl" erzeugt die URL, welche für die Authentifizierung angesprungen, d.h. an den Browser des Benutzers als "redirect to" gesendet werden muss.
Über den $State Parameter wird ein Json-Objekt mitgegeben, in welchem der Raum-Link, Displayname und Videoconsent hinterlegt werden, damit nach erfolgter Anmeldung gleich in den Raum weitergeleitet wird.
Die weiteren an den SSO übergebenen Parameter sind die Client_id, die Rücksprung adresse "redirect_uri" und der response-type "code", welcher ein Token zurückliefert.

> ⚠ ClientId und erlaubte Rücksprungadresse/n sind auf SSO-Seite statisch hinterlegt. Wird der SSO woanders eingesetzt, ist Rücksprache mit DARC-IT notwendig.

Nach erfolgter Authentifizierung beim SSO erzeugt dieser ein Einmal-Token, mit dem die Stammdaten abgefragt werden können. Der Browser des Benutzers wird an die Rücksprungadresse weitergeleitet und das Token als Parameter "?code=" angehängt.
Die Funktion "ProcessAuthorizationCode" bekommt diesen Code als Parameter und fragt damit beim Token-Endpunkt die Stammdaten des Benutzers in Form eines signierten JWT ab.

Ebenso kann die Funktion ProcessAuthorizationCode mit einem Refresh-Token aufgerufen werden (bool $Refresh = true) , um die Session eines bereits bekannten, autorisierten Benutzers zu verlängern. Zurück kommt ebenfalls das JWT.

Das JWT enthält die Stammdaten des Benutzers, Gültigkeitsdaten und das (nächste) gültige Refresh-Token und in einem Json-Array namens "aemter" die DARC-Ämter. Der Datentyp ist leider kein Objekt, sondern ein Array, deswegen findet man das DARC-Amtskürzel in $Amt[0] und den Zuständigkeitsbereich in $Amt[1].

Weitere Hilfsfunktionen in der SSO-Klasse prüfen auf die Ämter VO, DV, OVV bzw ermitteln das höchste Amt. Diese Hilfsfunktionen arbeiten dabei immer auf dem JWT-Stammdatensatz, d.h. ohne einen vorherigen Aufruf von ProcessAuthorizationCode funktioniert das nicht.