Flows:
1. Login.php script would be invoked when a login button from oauth2 services clicked

2. If the service is an OIDC provider like google, then script will send request to discovery endpoint, response should contains jwks_uri

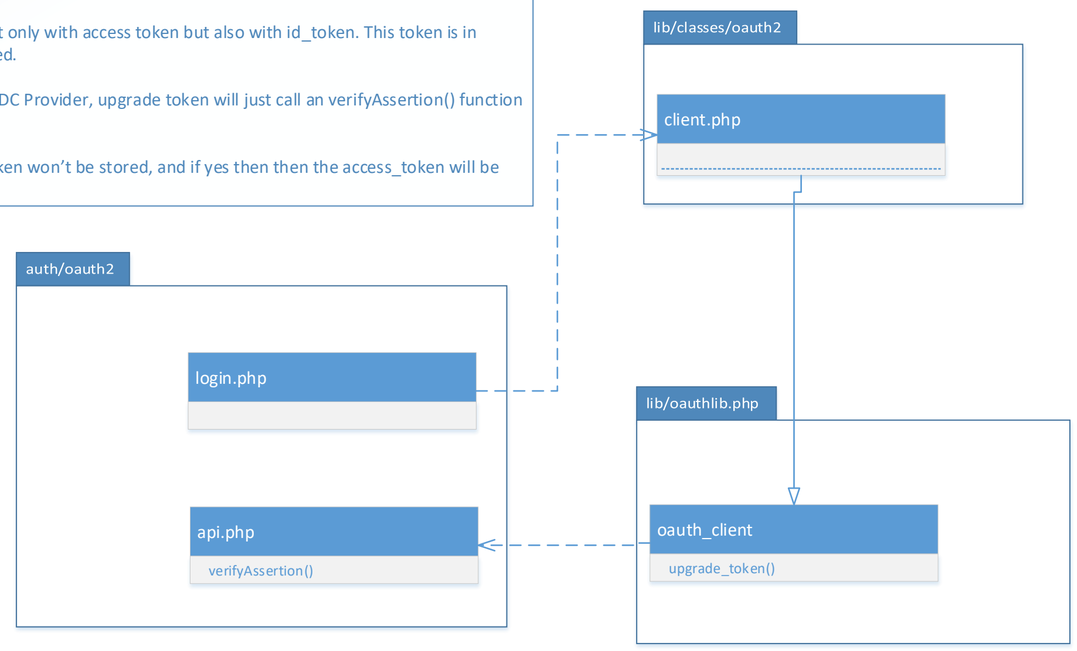
3. Send the request jwks_uri, as response OIDC provider will send the actual JWKS that could be used to verify the signature of JWT from this provider.

4. Save this JWKS

5. continue the script as usual

6. At some point upgrade_token() will be invoked, and send the request for access_token to the service....

7. OIDC Provider return this request not only with access token but also with id_token. This token is in format of JWT and it needs to be verified.

8. To verify the token(JWT) from the OIDC Provider, upgrade token will just call an verifyAssertion() function from oauth2/api

9. If the token is invalid then access_token won't be stored, and if yes then then the access_token will be stored.