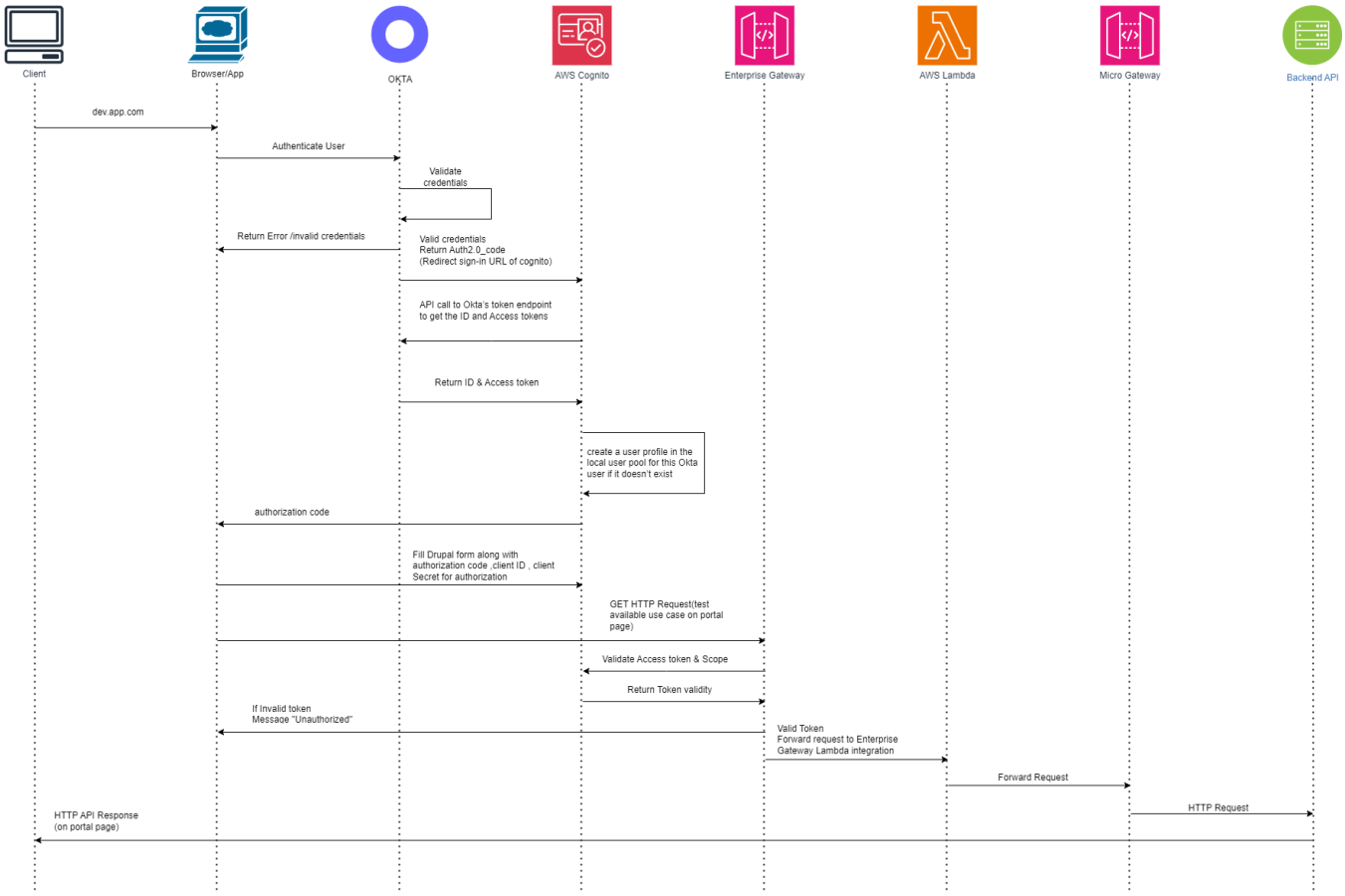
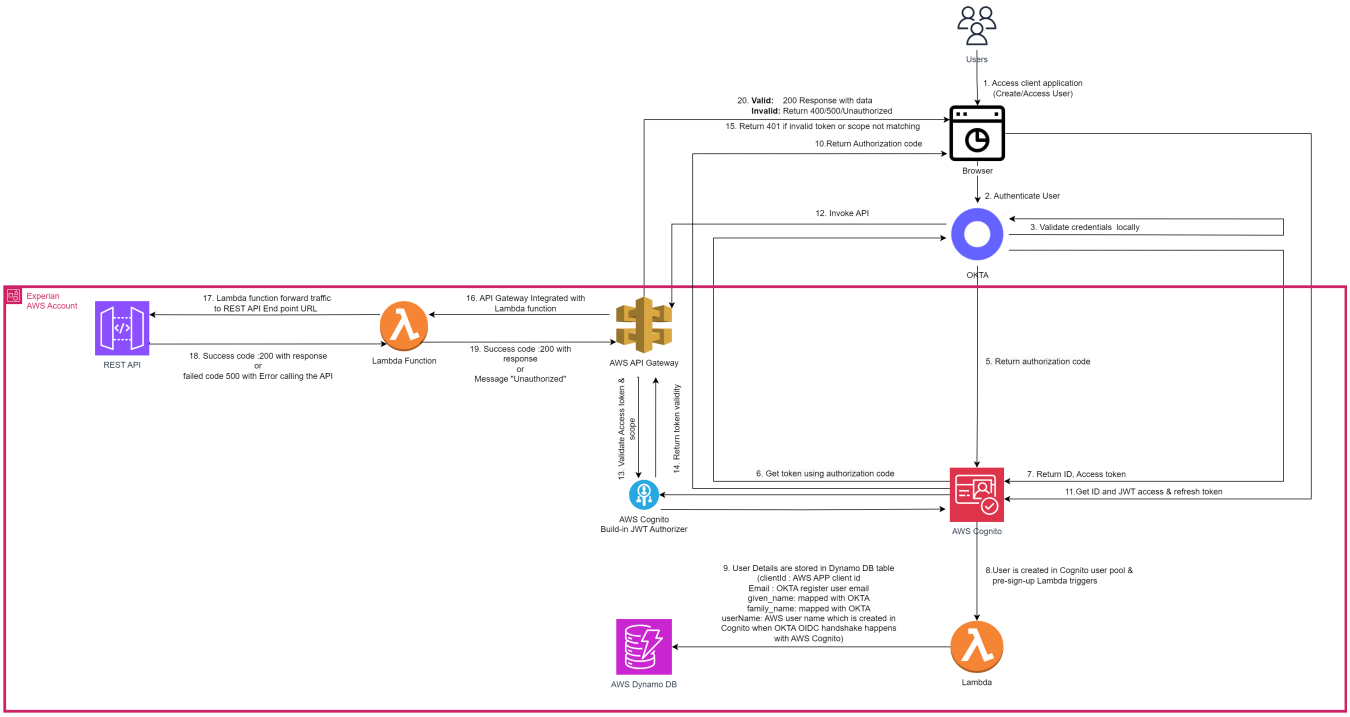
WF-05: B2C (Business to Consumer) - Okta integration with AWS Cognito and AWS Dynamo DB

Component Diagram



Flow Diagram



FLow Steps

Pre-requisites

- OIDC is used for token base authentication
- Create OKTA Identity provider in AWS and map it with the respective AWS Cognito user pool
- Add OKTA as identity provider in AWS Cognito user pool
    1. OKTA Application Client ID and Secrets required in AWS Cognito for OpenID connect
    2. Required Issuer URL from OKTA
- Map attributes between OKTA OpenID connect (OIDC) and AWS Cognito user pool. OIDC is used for token base authentication
- Configure a AWS Cognito pre-sign-up trigger
- Create a Dynamo DB table which can store the user details.
- Create a lambda function that have dynamo DB table as target for storing the user details
- Integrate AWS Cognito user pool with AWS API gateway as a authorizer

Steps

a. User opens a browser and types the client app URL eg. “experian.buname.sb.com”
b. Automatically initiate an Authentication/OIDC flow with AWS Cognito to authorize url. OR Allow user to enter login details for Authentication. AWS Cognito receives the request from client app and either displays the login page with a button to initiate the OIDC federation or automatically initiate the OIDC federation with Okta by redirecting to /authorize URL.
c. Okta will return an authorization code back to AWS Cognito.
d. AWS Cognito will make a backend API call to Okta’s token endpoint to get the ID and Access tokens. Okta will return an ID and Access tokens
e. AWS Cognito will create a user profile in the local user pool for this Okta user if it doesn’t exist and redirect back to Client app with an authorization code.
f. AWS Cognito will return and ID and Access tokens
g. Client app will validate the ID token, check if it is a valid user and return the web page to the browser
h. Client app will invoke API with Access token
i. AWS API gateway will validate Access Token and scope with AWS Cognito
j. AWS Cognito will return the token validity
k. For valid token return 200 Response with Data or return 403 for invalid token on the browser
l. When OKTA return ID and Access token to Cognito. The Cognito create a user profile in the Cognito User pool .
m. As pre configure AWS lambda is attached with user pool that will send the user details in AWS Dynamo DB.
n. As the user creation happens, lambda triggers and can store below fields in Dynamo DB tables

ClientId : AWS APP client id
Email : OKTA register user email
given_name: mapped with OKTA
family_name: mapped with OKTA
userName: AWS user name which is created in Cognito when OKTA OIDC handshake happens with AWS Cognito