

B2C Customer Portal



US based company required to develop a centralized portal for internal users (Corp, Sales and Ops), External clients (Salesforce existing clients, Subcontractor partners (Salesforce existing vendors), public/anonymous client prospects, public/anonymous subcontractor prospects) providing varying/appropriate authentication & access and presenting them with a list of services as per their roles & permissions.

Below are the main features implemented in this portal:

- Authentication of Internal users via Active Directory
- Authentication of External (known clients and partner-vendors) users via B2C-MFA-Azure Tenant methods
- Facility for new client prospects to request an order of magnitude non-qualified quote by providing specific N/Q Quote form inputs.
- Facility for new subcontractor prospects to request con by providing specific N/Q Quote form inputs.
- User's post authentication, as per their role defined, they will be able to access the services in the portal – presents the features access.
- It supports following user types:
 - Internal Users
 - External Clients
- It provides following services such as:
 - o Login authentication via B2C MFA Azure service
 - o Submit Order for the list of client's services.
 - o Data Exchange –using DropBox storage provider.
 - o Direct access request-response to Salesforce for specific client data
 - o Pass data to a queue or directly to MS Azure DataLake Gen2

Azure Active Directory B2C tenant method:

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs. Azure Active Directory B2C (Azure AD B2C) is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring and automatically handling threats like denial-of-service, password spray, or brute force attacks.

