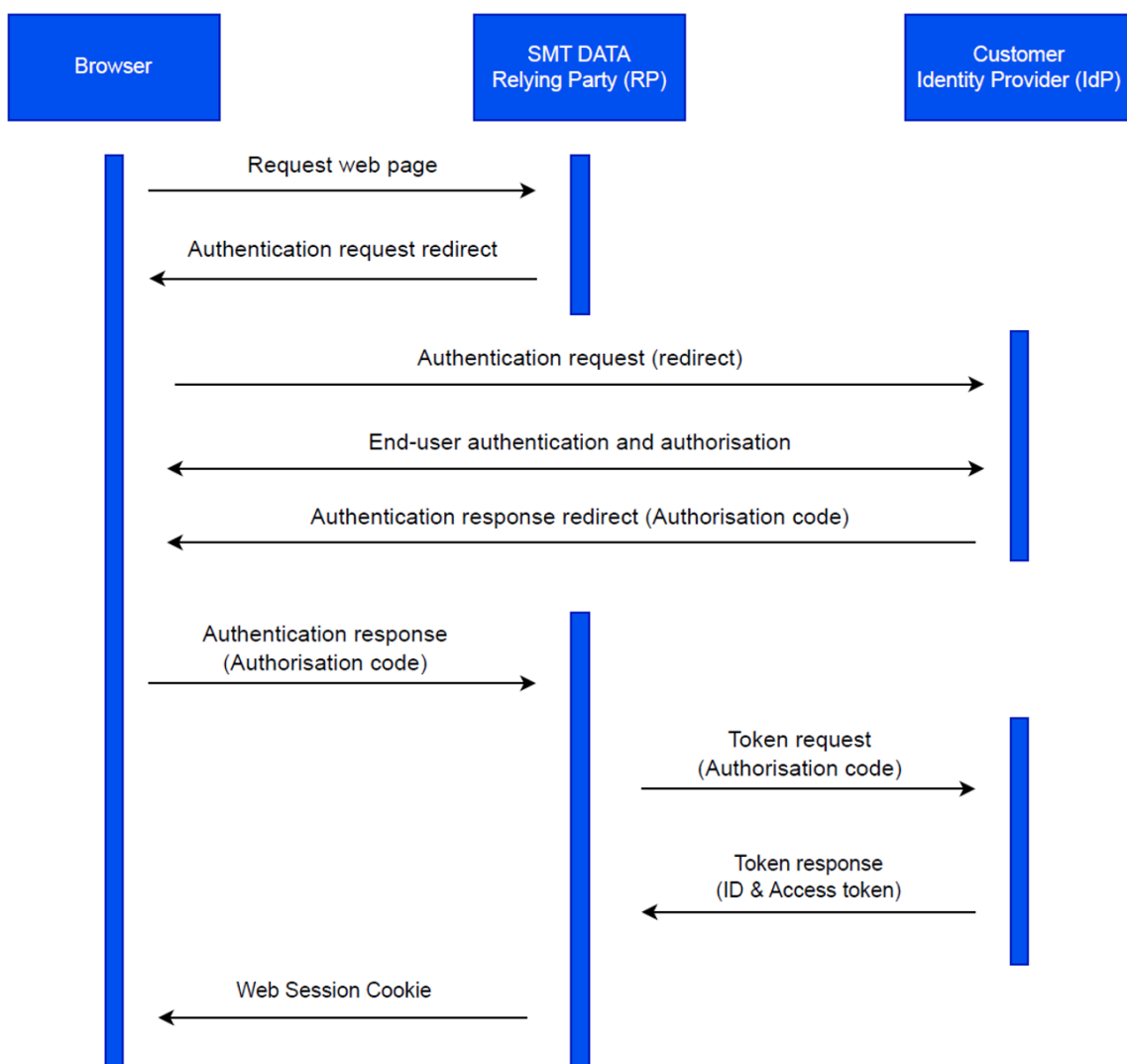


**Guide:**

# SSO & AD integration.

In this guide you will get an overview on how the AD Integration & SSO with ITBlaaS is set up including the openID connect authorization code flow and the IdP requirements.

## OpenID Connect Authorization Code Flow



## IdP Requirements

### IdP Discovery Document (Well-Known Configuration)

- Discovery URL (Usually '/.well-known/openid-configuration') (provided by IdP)

### Client Registration Details

- Client ID: Unique identifier for the Relying Party (provided by IdP)
- Client Secret: Secret known only by the Relying Party and IdP (provided by IdP)
- Redirect URIs: Allow Relying Party Callback URL (Allow by IdP)

### Supported Scopes

- 'openid', 'profile', 'email'

### Claim/Attribute Mapping

- What claims will be included from the IdP in the ID token (e.g., 'sub', 'name', 'email')

### Token Audience Restriction

- IdP can optionally provide a 'aud' claim to be used by RP

## User Administration in Customer AD

When User Administration is controlled in Customer AD the following conditions apply:

- SSO must be activated between Customer AD and ITBlaaS.
- Standard User Administration is disabled for the client in the ITBI Portal, as shown in below table.
- When a client user, without a valid AD-Group assigned, accesses the ITBI Portal, he/she will meet an error message telling: 'You do not have a valid license, please contact your AD-Administrator.'
- Client must provide <AD-Group Object ID> to SMT Data for each ITBI License as shown in below table.

#ID	ITBI License	Description	Customer AD Mapping
01	Consumer	Portal Access	<AD-Group Object ID>
02	BI Advanced	Portal Access Thick Client to build BI reports	<AD-Group Object ID>
03	BI Developer	Portal Access Thick Client to build BI reports Access to publish BI reports to all users	<AD-Group Object ID>
04	AI Developer	Portal Access Data Lake Access	<AD-Group Object ID>
05	Tech Admin	Access to configure data transfers <del>User Administrator Access</del>	<AD-Group Object ID>

## Next step

Please contact [support@smtdata.com](mailto:support@smtdata.com) for callback URL and further instructions on how to test the flow.