Frequently Asked Questions

Interoperability Developer Portal

Horizon Blue Cross Blue Shield of New Jersey

Contents

Subscription Keys, Client IDs and Client Secrets

What are Subscription Keys, Client IDs and Client Secrets?

The Subscription Keys, along with the Client ID and associated Client Secret, enable your App to access the appropriate data.

Subscription Keys

Subscription Keys are codes required to control access to API products. There are two Subscription Keys, Primary and Secondary, for each API you subscribe to. These keys are unique to you and are generated when the service is created and can be individually regenerated on demand.

When the Primary Subscription Key expires, you can use the Secondary Subscription Key and request a new Primary Subscription Key to keep at least one Subscription Key active for continued access to the service.

Subscription Keys must be rotated every six months before they expire. You must rotate the Subscription Keys to re-subscribe to each API product.

The Subscription Key is passed as a header element while calling the appropriate Interop API. Below is a sample of a header element:

Client ID and Client Secret

The Client ID is a set of alphanumeric characters issued upon approval of your App registration. It is associated with your app and organization.

The Client Secret is a set of alphanumeric characters (similar to a password) and is also issued upon approval of your App registration.

The Client Secret is associated with the Client ID for a particular app.

The Client Secret must be rotated every 12 months before it expires. Failure to rotate the Client Secret will disable the App's integration.

How do I get Subscription Keys?

After you register and get access to the portal, sign in, select the API product you want, and select Subscribe. The keys are displayed. Copy and save both keys for building your application.

Can I get Subscription Keys without a Client ID and Client Secret?

While you can get Subscription Keys without a Client ID and Client Secret, you cannot call any APIs with Subscription Keys only. For your App to work, you need a Subscription Key, Client ID, and Client Secret.

How do I get a Client ID and Client Secret?

Follow these steps:

1. Register as a developer and get access to the portal.
2. Register App and receive approval.

   You will then receive the Client ID and Client Secret via email within five business days.

Note: You must use the same email address when you register your App that you used to register as a developer on the portal.

Note: You must register each App separately. You will receive a Client ID and Client Secret for each App that is approved.

What do I do if I don't receive the Client ID or Client Secret?

Open this site: https://developer.interop.horizonblue.com and select **Contact Support** at the bottom of the page. The Issue Submission Form page is displayed.

Note: The Contact Support link is available on all pages, including the Help page.

Fill out the fields and select the appropriate options (all fields are required).

For Category, select **3rd Party Application**.

For Issue Type, select **3rd Party App developer OAUTH (i.e. client credentials, failed tokens, etc.)**.

For User Impact, indicate that you didn't receive your Client ID or Client Secret.

After you submit the form, you will receive separate emails from Horizon BCBSNJ Developer Services with your Client ID and/or Client Secret.

How can I get a Subscription Key, Client ID and Client Secret for a registered App?

Subscription Keys are unique to the developer who selected the API product. You must request your own Subscription Keys.

Register on the portal, sign in, select the API product you want, and select Subscribe. The keys are displayed. Copy and save both keys for building your application.

The Client ID and Client Secret are associated with your organization and a registered App. You must re-register the App to receive a new Client ID and Client Secret for the App.

How can I get new Subscription Keys and a new Client ID and Client Secret for a registered App?

Subscription Keys are unique to the developer who selected the API product. You must request your own Subscription Keys.

To get new Subscription Keys, register on the portal, sign in, select the API product you want, and select Subscribe. The keys are displayed. Copy and save both keys for building your application.

The Client ID and Client Secret are associated with your organization and a registered App. You can request via Support to receive a new Client ID and Client Secret for the registered App.

Can the same Subscription Keys be issued to more than one developer?

No. Each developer is issued a unique set of Subscription Keys for each API product.

Note: Each developer is also issued a unique set of Subscription Keys for the same API product.

Can I get a Client ID and Client Secret without registering as a developer on the portal?

No. You must register as a developer on the portal before you can get the Client ID and Client Secret.

What do I do if I forget my Client ID or Client Secret?

Open this site: https://developer.interop.horizonblue.com and select **Contact Support** at the bottom of the page. The Issue Submission Form page is displayed.

Note: The Contact Support link is available on all pages, including the Help page.

Fill out the fields and select the appropriate options (all fields are required).

For Category, select **3rd Party Application**.

For Issue Type, select **3rd Party App developer OAUTH (i.e. client credentials, failed tokens, etc.)**.

For User Impact, indicate that you forgot your Client ID or Client Secret.

After you submit the form, you will receive separate emails from Horizon BCBSNJ Developer Services with your existing Client ID and/or Client Secret.

When do Subscription Keys expire?

Subscription Keys expire every six months. You will receive a notification prior to expiration. You must regenerate both Subscription Keys to get new keys. If the keys expire before you get the new keys, your App will lose access to Horizon BCBSNJ data.

When Do the Client ID and Client Secret expire?

The Client ID does not change and never expires. The Client Secret expires every 12 months. You will receive a notification prior to expiration. You must rotate the Client Secret before it expires or your App will lose access to Horizon BCBSNJ data.

How do I manage Subscription Keys, Client IDs and Client Secrets?

Subscription Keys

You receive two Subscription Keys after you register on the portal and select an API product: a Primary Key and a Secondary Key.

These keys expire every six months. You will receive a notification prior to expiration. You must rotate both Subscription Keys to get new keys. If the keys expire before you get the new keys, your App will lose access to Horizon BCBSNJ data.

Client-ID and Client Secret

You receive the Client ID and Client Secret after you register your App and it is approved.

The Client ID does not change and never expires. The Client Secret expires every 12 months. You will receive a notification prior to expiration. You must change the Client Secret before it expires or your App will lose access to Horizon BCBSNJ data.

Send an email from your registered email address to HZNInteropAppRegistration@horizonblue.com. When the request is approved, you will receive an email with the Client Secret.

Access

How can I access the portal if my account has been locked?

Open this site: https://developer.interop.horizonblue.com and select **Contact Support** at the bottom of the page. The Issue Submission Form page is displayed.

Note: The Contact Support link is available on all pages, including the Help page.

Fill out the fields and select the appropriate options (all fields are required).

For Category, select **Developer Portal Account**

For Issue Type, select **Account lockout**.

After you submit the form, you will receive an email from Horizon BCBSNJ Developer Services indicating your account has been unlocked.

Who do I contact if I am unable to access the portal?

If the web site is down for maintenance, the following message is displayed with instructions:

> Please follow the Instructions in the window.

Who do I contact if I am unable to access the APIs on the portal?

Open this site: https://developer.interop.horizonblue.com and select **Contact Support** at the bottom of the page. The Issue Submission Form page is displayed.

Note: The Contact Support link is available on all pages, including the Help page.

Fill out the fields and select the appropriate options (all fields are required).

> For Category, select **Other**.
>
> For Issue Type, select **Non Categorized Issue**s.
>
> For User Impact, indicate what you are unable to access.

After you submit the form, Horizon BCBSNJ Developer Services will contact you.

How do I get a new Password if I've forgotten mine?

Select Forgot Password on the Sign in page of the portal and follow the instructions.

How do I get access to API product data for my App?

Follow these steps:

1. Register as a developer and get access to the portal.
2. Register your App and receive approval.
3. Use your Client ID and Client Secret to get an access token.
4. Use the Subscription Keys and access token to access API product data.

Note: You must use the same email address when you register your App that you used to register as a developer on the portal.

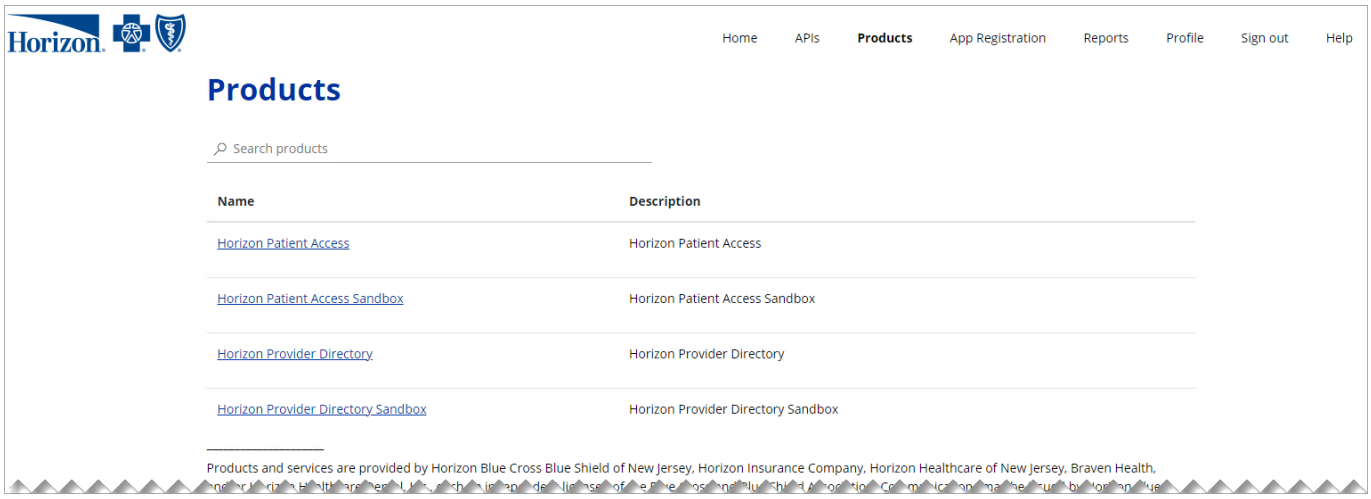
Note: You must register each App separately. You will receive a Client ID and Client Secret for each App that is approved.

APIs

Where will I find API products in the portal?

After you have registered for the portal, you will be able to view the API products. They are listed under the Products menu at the top right of the page.

Here is a sample of API products.



What APIs are currently available on the Portal?

As API products are made available, they will be listed under Products at the top right of the page.

Misc.

How many apps can I register?

You can register as many Apps as you would like.

Can multiple developer accounts share one App?

Each App registered by a developer belongs to that developer only and cannot be shared with other developer accounts.

How and when are refresh tokens used?

Refresh tokens are issued along with identity and access tokens and have longer expiration periods compared to access tokens. They can be used to get new access tokens when existing access tokens expire.

Refresh tokens are typically used to acquire access tokens as long as the refresh token is valid.

For more details on the Refresh token, see "What does the OAuth token response look like?" and "When Do the Refresh Token and Access Token expire?"

What browsers are supported by the portal?

Here are the browsers that we support:

- Apple Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

What is a Test App ID?

The Test App ID is the corresponding Application ID that was previously registered to connect to the sandbox. If a test App was not previously registered, you need to an App to connect to the sandbox APIs. Use the sandbox to test your App prior to registering the production App and connecting to the production APIs.

Security

What is the difference between Patient Access API authentication and Provider Directory API authentication?

Provider Directory APIs do not need member details—they are public in nature. However, all Patient Access APIs need member details.

The difference is in the token structure of the two API types.

What are the validation rules for your App's Test App ID

As an App developer you must be aware of the following validation rules related to the field, **TEST APP ID FOR YOUR APP**, in the application registration web form.

- The **TEST APP ID FOR YOUR APP** field is displayed when you register a production App (when you select **Production** for **ENVIRONMENT FOR YOUR APP**). You should enter your Test App ID.
- The Test App ID belongs to the account provided during the registration of the production App.
- The Test App ID must NOT be for an App that is already linked to another production App that you have registered. Every production App has a 1:1 mapping with a Test App. There must be a Test App for every production App.
- The Test App ID character must be 36 characters.
- The App ID must be associated with the developer.
- The App ID must be unique.
- The App must support PKCE flow to work.

How does multi-factor authentication work when I register at the Horizon Interoperability Developer Portal?

You will receive an OTP (one-time password) in an email that will be sent to you when you register as a developer at the developer portal. You will use your user name, password, and OTP to log into the portal.

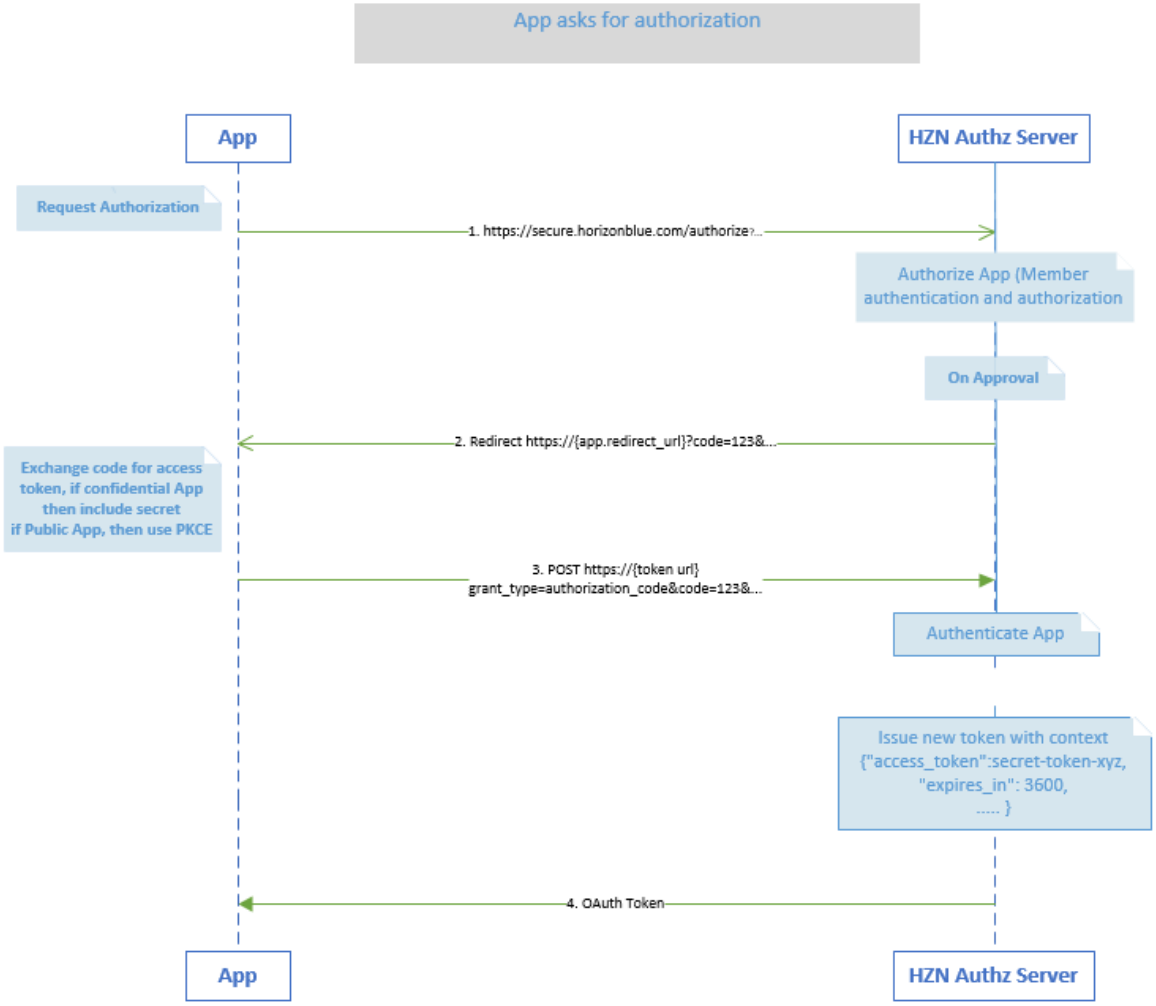
Each time you log into the portal thereafter, you will enter your user name and password and select **OTP**. You will receive an email with another OTP, which you will use to complete your login.

How do I get my App authorization and resource retrieval?

Horizon BCBSNJ follows the SMART FHIR Standard.

SMART Authorization Sequence

Here is the sequence diagram that depicts how Apps are connected to Horizon APIs for App authentication and member data access.



Here are the steps your App must follow to adhere to the SMART FHIR Standard.

1. App Authorization Flow.

   At launch, the app constructs a request for authorization by adding the following parameters to the query component of the "authorize" endpoint URL.

Parameters Table		
Parameters	**Required Field**	**Description**
response_type	Yes	Fixed Value: "Code"
client_id	Yes	Client ID is used to identify the Developer App. This value will be provided to the developer during registration of the application, and will be same as App ID.
redirect_uri	Yes	This is the redirect_uri supplied by 3rd Party App during registration.
scope	Yes	Only supports patient/*.read. This will be defaulted to patient/*.read, if present or not. Using the openid fhiruser scope will return an identity token
state	Yes	An opaque value used by the client to maintain state between the request and callback. The authorization server includes this value when redirecting the user-agent back to the client. The parameter will be used for preventing cross-site request forgery or session fixation attacks.
aud	Yes	The "aud" (audience) claim identifies the FHIR Gateway URL that the JWT is intended for. The Identify Provider will check the Client ID, and insert the respective URL of Sandbox or Prod Gateway. Example: Client ID C001 being registered for Sandbox will have: https://sandbox.api.interop.horizonblue.com.
acr_values	Yes	Qualifier that 3rd party app will pass to identify the member affiliation to the Horizon or Braven brand. Only one of the following valid values is passed: • HORIZON, or • BRAVEN

Authorization Request Example

https://secure.horizonblue.com/authorize?response_type=code&client_id=app-client-id&redirect_uri=https://3rdPartyapp.com/after-auth&scope=patient/*.read&acr_values=HORIZON&state=98wrghuwuogerg97&aud=https://sandbox.api.interop.horizonblue.com.

2. Horizon IDP evaluates the authorization request by asking for the end-user input (user identification and consent).

   A successful response to this is the **Auth Code**.

   Authorization Response Example

   A successful response will look like this:

   https://<3rdPartyRedirectURL>?code=O25sdOCYee2N4E9GO97V4x5JvkAcgu5HE_8AAAAB&state=*xyz* where *xyz* = value sent by third-party app.

3. App exchanges the authorization code for the Access Token.

   After obtaining an authorization code, the app trades the code for an access token via HTTP POST to the authorization server's token endpoint URL, using content-type application/x-www-form-urlencoded, as described in section 4.1.3 of RFC6749.

   For public apps, authentication is not possible (and thus not required), since a client with no secret cannot prove its identity when it issues a call. (The end-to-end system can still be secure because the client comes from a known, https protected endpoint specified and enforced by the redirect URI.) For confidential apps, an Authorization header using HTTP Basic authentication is required, where the username is the app's client_id and the password is the app's client_secret.

   Request:

Parameters Table		
Parameters	**Required Field**	**Description**
grant_type	Yes	Fixed Value: authorization_code
Code	Yes	The Code that the app received from the authorization server.
redirect_uri	Yes	This is the same redirect_uri supplied in the initial authorization request.
client_id	Conditional	Required for public apps. Omit for confidential apps.

Token Request Example

POST https://securetest.horizonblue.com/Fed4Sp/as/token.oauth2
Include the request fields in the post body


```
{
  "scope": "openid fhirUser patient/*.read",
  "client_id": "dcb6e113-5913-56ca-997c-e0b774875562",
  "iss": "https://securetest.horizonblue.com/Fed4Sp",
  "aud": "https://preptz.api.interop.horizonblue.com",
  "sub": "28ca7b7c-317f-5be5-bef7-f3996a562451",
  "loginid": "JSKIDMOREXUAT1",
  "requestorid": "28ca7b7c-317f-5be5-bef7-f3996a562451",
  "roles": "PATIENT",
  "tenantid": "fc4de0e3-d41f-46b2-9d10-00bcf2fb4978",
  "pi.sri": "aG_HAeK4y81Ob2IELrO-itArvE8",
  "usertype": "Braven",
  "memberId": "4893627",
  "exp": 1623685357
}
```


Response:

The authorization server will return a JSON object that includes an access token or a message indicating that the authorization request has been denied. The JSON structure includes the following parameters:

Parameters Table	
Parameters	**Description**
access_token	The access token issued by the authorization server
token_type	Fixed Value: Bearer
expires_in	Lifetime in seconds of the access token, after which the token will not be accepted by the resource server.
Scope	Scope of access authorized. Note that this can be different. The scope is defaulted to Patient/*.read.
Id_token	Authenticated patient identity and user details.
refresh_token	Token that can be used to obtain a new access token, using the same or a subset of the original authorization grants.

Note: If there is a requirement for the Provider directory API, it follows client_credential.

Note: If there is a requirement for the Patient Access API, it follows authorization_code.

Token Response Example:

{
"access_token":"eyJhbGciOiJSUzI1NiIsImtpZCI6IjEiLCJwaS5hdG0iOiI3ZzF6In0.eyJzY29wZSI6Im9wZW5pZCBmaGlyVXNlciBwYXRpZW50Lyoucm...",

"refresh_token": "pJOW5qazAkEBR9NV23lkQQrEgU25JsFCEsfbcsXqVC",

"id_token":"eyJhbGciOiJSUzI1NiIsImtpZCI6IlBGcDRUMmV6NnNxSmh4bXhNaUVnOFY1WXhwUSJ9.eyJzdWIiOiJaTklDS0VMWFVBVDEy...",

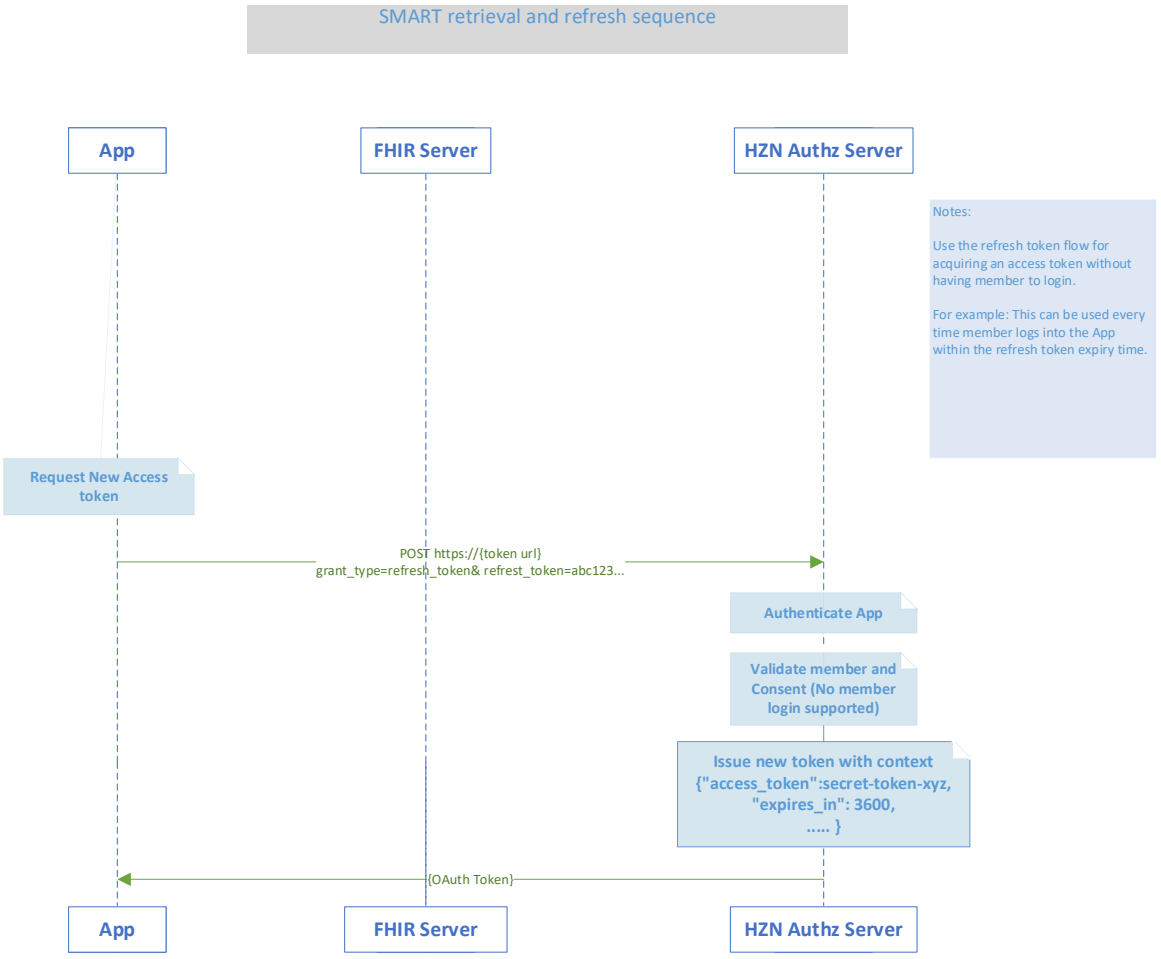
"token_type": "Bearer",

"expires_in": 7199
}

At this point, the authorization flow is complete.

SMART retrieval and refresh sequence

Here is the sequence diagram that depicts how to work with data and the Refresh and Access Tokens.



4. App accesses member data via FHIR API.

5. App uses a Refresh Token to obtain a new Access Token.

Note: Refer to www.hl7.org/fhir/smart-app-launch for more details.

What is the Identity Token Structure?

The Identity token structure is provided in the table.

Note that the term "claim" is used in standard FHIR terminology.

Parameters Table	
Parameters	**Description**
Sub	The Sub is the external member id. This ID uniquely defines the user.
Aud	The "aud" (audience) claim identifies the FHIR Gateway URL that the JWT is intended for. The Identify Provider will check the Client ID, and insert the respective URL of Sandbox or Prod Gateway. Example: Client ID C001 being registered for Sandbox will have: https://sandbox.api.interop.horizonblue.com.
jti	The "jti" (JWT ID) claim provides a unique identifier for the JWT. The identifier value MUST be assigned in a manner that ensures that there is a negligible probability that the same value will be accidentally assigned to a different data object. If the application uses multiple issuers, collisions MUST be prevented among values produced by different issuers as well. The "jti" claim can be used to prevent the JWT from being replayed. The "jti" value is a case-sensitive string. Use of this claim is OPTIONAL.
Iss	The "iss" (issuer) claim identifies the principal that issued the JWT. The "iss" value is a case-sensitive string containing a URI value. In this case the iss value will be: https://secure.horizonblue.com/Fed4Sp.
iat	The "iat" (issued at) claim identifies the time at which the JWT was issued. This claim can be used to determine the age of the JWT. Its value MUST be a number containing a NumericDate value. Use of this claim is OPTIONAL.
exp	This is a timestamp with the below format 1970-01-01T0:0:0Z, and is used for internal use by Horizon.

Where can I get the configuration details for the authorization server?

The link below shows the "well-known endpoints," which identify the configuration details. You can use the relevant information for authorization server endpoints, such as authorization URL, token end points, and other details:

https://secure.horizonblue.com/Fed4Sp/.well-known/openid-configuration.

How will an App get a new access token if the current access token expires?

If the access token expires or there is no valid access token, the App will request a new access token by sending the refresh token to the authorization server. The authorization server will then send a new access token and a new refresh token to the App.

Where should I manage the refresh token?

It is strongly recommended that you manage the refresh token on the server side. This will allow you to switch your devices with your current valid token without having to request a new refresh token.

What does the OAuth token response look like?

This is a sample of the response from the authorization server when a request from the Third-Party App is authorized:

{
"access_token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6IjEiLCJwaS5hdG0iOiI3ZzF6In0.eyJzY29wZSI6Im9wZW5pZCBmaGlyVXNlciBwYXRpZW50LyoucmVhZCIsImNsaWVudF9pZCI6ImludGVyb3BhcHBhY2Nlc3MiLCJ0ZW5hbnRpZCI6ImZjNGRlMGUzLWQ0MWYtNDZiMi05ZDEwLTAwYmNmMmZiNDk3OCIsInBpLnNyaSI6InNKVkdRVmVTSVd6aldJYlBleV8zNm.....",

"refresh_token": "pJOW5qazAkEBR9NV23lkQQrEgU25JsFCEsfbcsXqVC",

"id_token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6IlBGcDRUMmV6NnNxSmh4bXhNaUVnOFY1WXhwUSJ9.eyJzdWIiOiJaTklDS0VMWFVBVDEyM0BHTUFJTC5DT00iLCJhdWQiOiJpbnRlcm9wYXBwYWNjZXNzIiwianRpIjoiaUtkSmdNNDdmTzgyZ0txdVJGR3Z2ViIsImlzcyI6Imh0dHBzOi8vc2VjdXJldGVzdC5ob3Jpem9uYmx1ZS5jb20vRmVkNFNwIiwiaWF0IjoxNjE3MjEwMjU3LCJleHAiOjE2MTcyMTA1NTd9.n5pJZbl7l2btNvHsfUbuaz608mal3h4l.....",

"token_type": "Bearer",

"expires_in": 7199
}

This is a sample of the access components after the access token has been decoded:


```
{
  "scope": "openid fhirUser patient/*.read",
  "client_id": "interopappaccess",
  "iss": "https://securetest.horizonblue.com/Fed4Sp",
  "aud": "https://preptz.api.interop.horizonblue.com",
  "tenantid": "fc4de0e3-d41f-46b2-9d10-00bcf2fb4978",
  "pi.sri": "sJVGQVeSIWzjWIbPey_36c7ZA-I",
  "Sub": "ZNICKELXUAT123@GMAIL.COM",
  "requestorid": "12312321",
  "roles": "MEMBER",
  "exp": 1617218315
}
```


This is a sample of the ID components after the ID token has been decoded:


```
{
  "sub": "ZNICKELXUAT123@GMAIL.COM",
  "aud": "interopappaccess",
  "jti": "iKdJgM47fO82gKquRFGvvV",
  "iss": "https://securetest.horizonblue.com/Fed4Sp",
  "iat": 1617210257,
  "exp": 1617210557
}
```


What authorization flows are supported for your Apps?

Horizon supports these flows:

- OAuth
- PKCE

If your App is a public App, you should support PKCE. However, PKCE must be followed on both the Client and Server side.

If your app is confidential, you must support OAuth, which uses ClientID and Client Secret.

Note: As a best practice, you should not store the Client ID and Client Secret in your app on the client side.

When Do the Refresh Token and Access Token expire?

The Refresh Token expires after 90 days.

The Access Token expires after thirty minutes.

What tokens are in the OAuth Token?

Horizon BCBSNJ shares the following tokens as part of the OAuth Token:

- ID Token
- Refresh Token
- Authorization Token