BC Services Card – Open ID Connect Integration Guide

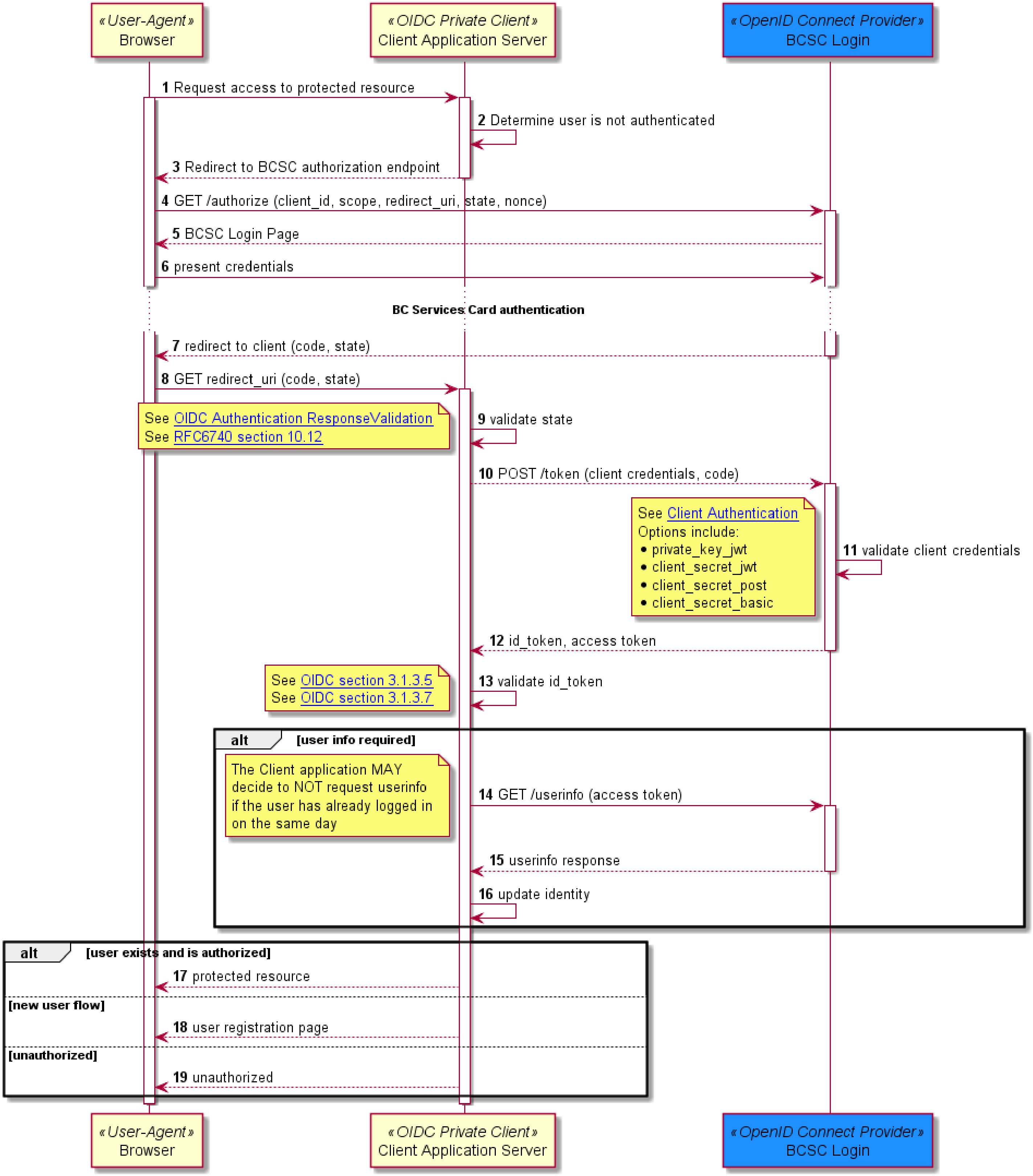
This document is an initial high-level description of how relying parties can integrate their solutions with the BC Services Card Identity Assurance Service (IAS) utilizing the OpenID Connect authentication protocol. In this document the terms client and relying party are used interchangeably and both refer to the same entity.

Version	Date	Author	Comments
0.0.1	Nov. 22, 2018	Jordan Armstrong, Technical Integration Specialist, IDIM Program Marcos Carretero, BC Services Card Solution Architect, IDIM Program	Compile draft for review.
0.0.2	Nov. 26, 2018	Marcos Carretero, BC Services Card Solution Architect, IDIM Program	Review and edit.
1.0.0	Nov. 27, 2018	Jordan Armstrong, Technical Integration Specialist, IDIM Program	Edits and publish first draft.
1.0.1	Jan. 18, 2019	Jordan Armstrong, Technical Integration Specialist, IDIM Program	Included updated issuer and authorization endpoints. Added discovery endpoint and demo application information.
1.0.2	May 8, 2019	Jordan Armstrong, Technical Integration Specialist, IDIM Program	Update UserInfo call in sequence diagram. Add PROD Discovery Endpoint.
1.0.3	Aug. 28, 2019	Jordan Armstrong, Technical Integration Specialist, IDIM Program	Removal of amr from list of claims and ID token sample. Update list of claims to include given_names and provide example of difference between given_name and given_names.

Table of Contents

BCSC OIDC Login Sequence

The following diagram depicts the general sequence of BC Services Card Login for OpenID Connect.


«User-Agent» Browser
«OIDC Private Client» Client Application Server
«OpenID Connect Provider» BCSC Login
1 Request access to protected resource
2 Determine user is not authenticated
3 Redirect to BCSC authorization endpoint
4 GET /authorize (client_id, scope, redirect_uri, state, nonce)
5 BCSC Login Page
6 present credentials
BC Services Card authentication
7 redirect to client (code, state)
8 GET redirect_uri (code, state)
See OIDC Authentication ResponseValidation
See RFC6740 section 10.12
9 validate state
10 POST /token (client credentials, code)
See Client Authentication
Options include:
• private_key_jwt
• client_secret_jwt
• client_secret_post
• client_secret_basic
11 validate client credentials
12 id_token, access token
See OIDC section 3.1.3.5
See OIDC section 3.1.3.7
13 validate id_token
alt
[user info required]
The Client application MAY decide to NOT request userinfo if the user has already logged in on the same day
14 GET /userinfo (access token)
15 userinfo response
16 update identity
alt
[user exists and is authorized]
17 protected resource
[new user flow]
18 user registration page
[unauthorized]
19 unauthorized
«User-Agent» Browser
«OIDC Private Client» Client Application Server
«OpenID Connect Provider» BCSC Login

Narrative:

1. A User with a browser attempts to access a protected resource at the Client.
2. The Client determines that the browser is not authenticated.
3. The Client responds with a redirect to the browser. The redirect is an OIDC Authentication Request directed to BCSC Login (the OpenID Provider). The request contains the client_id, the client's registered redirect_uri, a state parameter, and an optional nonce parameter (recommended).
4. The browser sends the Authentication Request to BCSC Login.
5. BCSC Login returns the Login page.
6. The User chooses their Login flow and presents credentials to send to BCSC Login.
7. Once the User has been authenticated, Login sends an OIDC Successful Authentication Response to the redirect_uri from the original request.
8. The browser sends the response to the Client/Relying Party.
9. The Client validates the response.
10. The Client sends a Token request using the Client's registered authentication mechanism.
11. BCSC Login authenticates the Client request
12. BCSC Login sends an access token and id_token to the Client.
13. The Client validates the id_token and determines whether the user exists in the Client system and may make access control decisions at this point. The Client may consider the browser session to be authenticated at this point.
14. The Client may send a UserInfo request to Login for claims about the authenticated User.
15. BCSC Login sends the UserInfo response.
16. The Client updates its local user registry with the identity information from the BCSC User Response.
17. If the User exists and is authorized, the Client sends the protected resource that was requested at step 1.
18. Alternatively, if the User does not exist, the Client may send a new user registration page.
19. Or, an unauthorized response.

Authentication Request

This section describes the Authentication Request parameters supported by BCSC Login.

Parameter	OIDC Optionality	BCSC Optionality	Description
scope	Required	Required	The scope parameter is a space delimited list of scopes and must contain the value *openid*. Scopes currently supported by IAS include: • openid • profile • email • address Other scope values may be supported in the future.
response_type	Required	Required	The type of response requested. This parameter must always be set to *code*.
client_id	Required	Required	This is the client_id that is registered with IAS and is provided to the client by the IDIM Client Relationship Management Team. The value is often the URL of the client system.

Parameter	OIDC Optionality	BCSC Optionality	Description
redirect_uri	Required	Required	This is the URI to which the authentication response will be sent, and must be a value that is registered in IAS. Clients MAY have multiple redirection URIs registered to support different areas of their application.
state	Optional	Required	Opaque value used to maintain state between the request and the callback. This value is used to mitigate cross-site request forgery attacks.
nonce	Optional	Recommended	String value used to associate a Client session with an ID Token, and to mitigate replay attacks. The value is passed through unmodified from the Authentication Request to the ID Token. Sufficient entropy MUST be present in the nonce values used to prevent attackers from guessing values.

ID Token Claims

Claim	Description	Example
iss	Issuer Identifier for the Issuer of the response.	https://idtest.gov.bc.ca/oauth2/
sub	Subject identifier for the authenticated user that is locally unique to the client and never reassigned. This is also known as the Directed Identifier (DID), and may be up to 255 characters. The length depends on the configuration options for the client. The subject identifier can be configured to be fully qualified or not.	Not Qualified: MPX2WF45KT4FD3LWERR2YGPRKTNEMA25 Fully Qualifed: urn:did:MPX2WF45KT4FD3LWERR2YGPRKTNEMA25|urn:idcheck:demo:sit1
aud	The audience that this id_token is intended for and will contain the client_id of the client application.	https://ministry.gov.bc.ca/service/ or urn:ca:bc:gov:ministry:service
exp	Expiration time after which the token will not be accepted. This value is a JSON number representing the number of seconds from 1970-01-01T0:0:0Z as measured in UTC until the date/time. IAS will generally set this to 10 minutes from the issued time, but is configurable for the client.	1499612280970
iat	The time that this token was issued as a JSON number representing the number of seconds from 1970-01-01T0:0:0Z as measured in UTC.	1499612281970

Claim	Description	Example
auth_time	Time when the End-User authentication occurred. Its value is a JSON number representing the number of seconds from 1970-01-01T0:0:0Z as measured in UTC until the date/time. The value will generally be within seconds of the issued time if the token request was made immediately by the client after receiving the authentication response.	1499612280969
nonce	String value used to associate a Client session with an ID Token, and to mitigate replay attacks. The value is passed through unmodified from the Authentication Request to the ID Token. If present in the ID Token, Clients MUST verify that the nonce Claim Value is equal to the value of the nonce parameter sent in the Authentication Request. If present in the Authentication Request, Authorization Servers MUST include a nonce Claim in the ID Token with the Claim Value being the nonce value sent in the Authentication Request.	n-0S6_WzA2Mj
acr	Authentication Context Class Reference. String specifying an Authentication Context Class Reference value that identifies the Authentication Context Class that the authentication performed satisfied.	IAS will set this value to be the Identity Assurance Level of 2 or 3 depending on the identification level of the IIS Identity and the credential used for authentication.

Identity Claims

Identity information can be retrieved by the client application and this BCSC IAS returns the identity claims in a JSON message. Note that a client will not necessarily receive all claims. The claims that a client receives is defined in the information sharing agreement that is developed during the onboarding process. The following claims may be received by the client.

IDIM Identity Attribute	OIDC Claim Name	Type	OIDC Standard Claim Name	Identity Attribute Description
AuthenticationIdentifier	sub	string	Yes	An identifier issued by IAS. Format may be an Identity Reference, Qualified Directed Identifier or Directed Identifier.

IDIM Identity Attribute	OIDC Claim Name	Type	OIDC Standard Claim Name	Identity Attribute Description
UserDisplayName	display_name	string	No	The Individuals name which is their preferred name if available or composed of their documented name. First name + Surname.
EmailAddress	email	string	Yes	The email address provided by the individual.
AuthoritativePartyName	authoritative_party_name	string	No	This is set to IAS.
PrimaryDocumentedSurname	family_name	string	Yes	The individual's documented surname recorded from valid identification.
PrimaryDocumentedGivenName	given_name	string	Yes	The individual's documented given name (first) recorded from valid identification. *(Note: This returns first name only and may not include all portions of the first name. For example: if the name included a space such as "Betty Jo" and Jo was included in a middle name field then only Betty would be returned.)*
PrimaryDocumentedGivenNames	given_names	string	Yes	The individual's documented given names (first and middle) recorded from valid identification. *(Note: This returns all of the names an individual has other than their surname.)*
BirthDate	birthdate	date	Yes	The individual's documented birth date recorded from valid identification.
Age	age	integer	Yes	The individual's age in years based on the documented birth date recorded from valid identification.
Age19OrOver	age_19_or_over	boolean	No	An indicator of whether the individual's age is 19 years or greater based on the documented birth date recorded from valid identification.
Sex	gender	string	Yes	The individual's documented sex recorded from valid identification.
Locality	locality	string	Yes	The city, municipality or district of an individual's provided residential address.
StateOrProvince	region	string	Yes	The province or state code of an individual's provided residential address.
PostalCode	postal_code	string	Yes	The postal code of the individual's provided residential address.

IDIM Identity Attribute	OIDC Claim Name	Type	OIDC Standard Claim Name	Identity Attribute Description
Country	country	string	Yes	The country code of an individual's provided residential address.
AddressBlock	address	string	Yes	All address lines of the individual's provided residential address.
IdentityAssuranceLevel	identity_assurance_level	integer	No	The level of confidence in the certainty of the identity claims of the individual according to the OCIO Identity
IdentityAssuranceLevel1	identity_assurance_level1	boolean	No	An indicator that there is low confidence in the identity claims of the individual according to the OCIO Identity
IdentityAssuranceLevel2	identity_assurance_level2	boolean	No	An indicator that there is medium confidence in the identity claims of the individual according to the OCIO Identity
IdentityAssuranceLevel3	identity_assurance_level3	boolean	No	An indicator that there is high confidence in the identity claims of the individual according to the OCIO Identity
StreetAddress	street_address	string	Yes	Full street address component, which MAY include house number, street name, Post Office Box, and multi-line extended street address information. This field MAY contain multiple lines, separated by newlines. Newlines can be represented either as a carriage return/line feed pair ("\r\n") or as a single line feed character ("\n").
AuthoritativePartyIdentifier	authoritative_party_identifier	string	No	One value for each BC Services Card (IAS) environment: urn:ca:bc:gov:ias:idtest urn:ca:bc:gov:ias:prd
AuthenticationTransactionIdentifier	transaction_identifier	string	No	d165ff0e8897144ec487566c9e174ef2
UserIdentifierType	user_identifier_type	string	No	did
UserType	user_type	string	No	VerifiedIndividual (This is always the returned value for BCSC).
QualifiedDirectedIdentifier	sub	string	No	urn:did:a12666b6-bf36-4848-a1b9-c5e15c280f45|urn:ca:bc:gov:fin *(fully qualified – contains Privacy Zone/Sector identifier)*
DirectedIdentifier	sub	string	No	a12666b6-bf36-4848-a1b9-c5e15c280f45 *(not qualified)*

SAMPLES

Authentication Request

```
https://idtest.gov.bc.ca/login/oidc/authorize?response_type=code&scope=openid%20address&c
lient_id=urn:ca:bc:gov:clientservice:environment&redirect_uri=www.ministry.gov.bc.ca/serv
ice/login&state=ngWG1AG4IjvbgB83B1YqjrIYvxR04nQaG1SlpUeUo9U&nonce=BLbwX-
gvGaei0omWWwuRCe4YjM0jQNAwv-AoKy_u9Gc
```

Authentication Response

```
https://www.ministry.gov.bc.ca/service/login?code=GfA8TP&state=ngWG1AG4IjvbgB83B1YqjrIYvx
R04nQaG1SlpUeUo9U
```

Token Response

Access Token and ID Token provided as JWT:

```
{
"access_token":
"eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJhdWQiOiJ1cm46aWRjaGVjazpkZW1vOnBoYXJtYWNpZXM6c
2l0MSIsImlzcyI6Imh0dHBzOlwvXC9pZHNpdC5nb3YuYmMuY2FcL29hdXRoMlwvIiwiZXhwIjoxNTQzMDE1Mzg2LC
JpYXQiOjE1NDMwMTQ3ODYsImp0aSI6IjdmMmI5YjA5LWNmZmMtNGE5Ni05MGViLTc3NDVjMWJiN2M3MSJ9.GVS0L2
t0xevdMvoAjRgpUujdHIy6GS6Sz__BIvuWQi4dRGYKkZBENouWR-
hE_4JQMt3C5XiEPktxGoY4nYHbEYLIw6nePzLo_MVIX1OtyF0acVWc1rgZ575CwrJRvYOVquoKIQalztCGTwqqZoD
IShw6fCMhG9XbS-
Lr3p3RgM36HDQ4fzGd1nkZJffk5jSsgxk2DfuYdxV1yiGujAOo27pF2YeC3GREADnGag8oyF_H23--
zHRqw2SJz1RLDurkBELJQNgz3MjFxbviFnIteWpyuQBcxIVfAJ6pICrXeaEUH7pCfnoVY1_i22DvtjHhLkfOqTw1f
xYnXOJsD3bd2A",
"scope": "address openid",
"id_token":
"eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiJ1cm46ZGlkOjdFWkNDVExKSVk2RDJaT040MjU0M
lFOS0hSMkEzT0RVfHVybjppZGNoZWNrOmRlbW86c2l0MSIsImF1ZCI6InVybjppZGNoZWNrOmRlbW86cGhhcm1hY2
llczpzaXQxIiwiYWNyIjoiMiIsImF1dGhfdGltZSI6MTU0MzAxNDc1OCwiYW1yIjoidXJuOm9hc2lzOm5hbWVzOnR
jOlNBTUw6Mi4wOmFjOmNsYXNzZXM6U21hcnRjYXJkIiwia2lkIjoicnNhMSIsImlzcyI6Imh0dHBzOlwvXC9pZHNp
dC5nb3YuYmMuY2FcL29hdXRoMlwvIiwiZXhwIjoxNTQzMDE1Mzg3LCJpYXQiOjE1NDMwMTQ3ODYsIm5vbmNlIjoiV
WoxcUVsRFVnS09BamQzZmN6V0x6aGdvUVpadWQ4c2xWbUdCd3Z1TTI2TSIsImp0aSI6IjdmMmI5YjA5LWNmZmMtNG
E5Ni05MGViLTc3NDVjMWJiN2M3MSJ9.IoS2bIlUlM32f5oZX3xqz1TWTMl3vcIHd2MbRP1LXN7oym_ox0gy-
u1D8eIwa1ohD3pYTIGSHlaZWgq58wSzFYTcOUDZAf4z2OBizloDFGhUQMDDWWLOF48H9CoIyEDHtK03rqFRth18Sx
3kWBrtmTDmZLyy0xKnmkABoUjrTlThZjwvn6oROz8hYMFrfgaJi2Mj826t9pin4M2omlpYjRKnB9q4G4fs17orzj9
cTScHKATcLedSAnT1J3ZRLD0vYxvjdk-BbO_mKcMT-OhN125AAJySE7ZVd72IeYM0bFA8Hh1-
ou40k4h9YyXuvOTpT2aOcZMcPvQwHMEyM-SjTQ",
"token_type": "Bearer",
"expires_in": 599
}
```

ID Token decoded:

```
{
"sub": "urn:did:7EZCCTLJIY6D2ZON42542QNKHR2A3ODU|urn:ca:bc:gov:idim:oidc:sample",
"aud": "urn:ca:bc:gov:clientservice:environment",
"acr": "2",
"auth_time": 1543014758,
"kid": "rsa1",
"iss": "https://idtest.gov.bc.ca/oauth2/",
"exp": 1543015387,
"iat": 1543014786,
"nonce": "Uj1qElDUgKOAjd3fczWLzhgoQZZud8slVmGBwvuM26M",
"jti": "7f2b9b09-cffc-4a96-90eb-7745c1bb7c71"
}
```

UserInfo Request

```
GET /oauth2/userinfo HTTP/1.1
Host: idtest.gov.bc.ca
Authorization: Bearer
eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJhdWQiOiJ1cm46aWRjaGVjazpkZW1vOnBoYXJtYWNpZXM6c2
l0MSIsImlzcyI6Imh0dHBzOlwvXC9pZHNpdC5nb3YuYmMuY2FcL29hdXRoMlwvIiwiZXhwIjoxNTQzMDE1Mzg2LCJ
pYXQiOjE1NDMwMTQ3ODYsImp0aSI6IjdmMmI5YjA5LWNmZmMtNGE5Ni05MGViLTc3NDVjMWJiN2M3MSJ9.GVS0L2t
0xevdMvoAjRgpUujdHIy6GS6Sz__BIvuWQi4dRGYKkZBENouWR-
hE_4JQMt3C5XiEPktxGoY4nYHbEYLIw6nePzLo_MVIX1OtyF0acVWc1rgZ575CwrJRvYOVquoKIQalztCGTwqqZoD
IShw6fCMhG9XbS-
Lr3p3RgM36HDQ4fzGd1nkZJffk5jSsgxk2DfuYdxV1yiGujAOo27pF2YeC3GREADnGag8oyF_H23--
zHRqw2SJz1RLDurkBELJQNgz3MjFxbviFnIteWpyuQBcxIVfAJ6pICrXeaEUH7pCfnoVY1_i22DvtjHhLkfOqTw1f
xYnXOJsD3bd2A
```

UserInfo Response – Decoded

```
{
"user_identifier_type": "did",
"sub": "urn:did:7EZCCTLJIY6D2ZON42542QNKHR2A3ODU|urn:ca:bc:gov:idim:oidc:sample",
"aud": "urn:ca:bc:gov:clientservice:environment",
"address": {
"street_address": "910 GOVERNMENT STREET\nRR 3",
"locality": "VICTORIA",
"region": "BC",
"postal_code": "V8W3Y5"
},
"iss": "https://idtest.gov.bc.ca/oauth2/",
"iat": 1543014859,
"jti": "9ac5c792-5ee4-4d13-b53e-8709bf4a2334"
}
```

Discovery Endpoint

A discovery endpoint is available for relying parties to reference the available BCSC IAS OpenID Connect configuration information. The discovery endpoint is:

- BCSC IAS TEST - https://idtest.gov.bc.ca/login/.well-known/openid-configuration
- BCSC IAS PROD - https://id.gov.bc.ca/login/.well-known/openid-configuration

Sample Discovery Document

```
{
"response_types_supported": [
"code"
       ],
"request_parameter_supported": false,
"request_uri_parameter_supported": false,
"claims_parameter_supported": false,
"introspection_endpoint": "https://idtest.gov.bc.ca/oauth2/introspect",
"grant_types_supported": [
    "authorization_code"
],
"revocation_endpoint": "https://idtest.gov.bc.ca/oauth2/revoke",
"scopes_supported": [
    "openid",
    "profile",
    "email",
    "address"
],
"issuer": "https://idtest.gov.bc.ca/oauth2/",
"authorization_endpoint": "https://idtest.gov.bc.ca/login/oidc/authorize/",
"userinfo_endpoint": "https://idtest.gov.bc.ca/oauth2/userinfo",
"token_endpoint_auth_signing_alg_values_supported": [
    "HS256",
    "HS384",
    "HS512",
    "RS256",
    "RS384",
    "RS512",
    "ES256",
    "ES384",
    "ES512",
    "PS256",
    "PS384",
    "PS512"
],
"userinfo_signing_alg_values_supported":
[
    "HS256",
    "HS384",
    "HS512",
    "RS256",
    "RS384",
    "RS512",
    "ES256",
    "ES384",
                "ES512",
    "PS256",
    "PS384",
    "PS512"
],
"jwks_uri": "https://idtest.gov.bc.ca/oauth2/jwk",
"subject_types_supported": [
    "pairwise"
],
"id_token_signing_alg_values_supported":[
    "HS256",
    "HS384",
    "HS512",
    "RS256",
    "RS384",
    "RS512",
    "ES256",
    "ES384",
    "ES512",
    "PS256",
    "PS384",
    "PS512",
    "none"
],
"token_endpoint_auth_methods_supported":[
    "client_secret_post",
    "client_secret_basic",
    "client_secret_jwt",
    "private_key_jwt"
],
"token_endpoint": "https://idtest.gov.bc.ca/oauth2/token"
}
```

Demo Application

A demo application is available in the BCSC IAS TEST environment to help demonstrate the functionality provided by the service. The URL to access the demo application is:

TEST - https://idtest.gov.bc.ca/demo/oidc_client/index

The landing page for the demo application lists 6 services, only the **Renew Licences** link is functional and allows a user to test the login process with BC Services Card.

Access to the demo application is limited to those on the SPANBC network. If the relying party is outside of this network a request will need to be made to add the IP addresses/range that require access. The IDIM Technical Integration Specialist will work with the relying party and facilitate this request.