Inland Revenue

Build Pack: Address API

Date: 11/06/2024

Contents

1   Overview

1.1   This solution

Inland Revenue has a suite of digital services available for consumption by our service providers that supports efficient, electronic business interactions with Inland Revenue. The application programming interface (API) described in this build pack document provides current information about the addresses held by Inland Revenue.

Before continuing, please consult
www.ird.govt.nz/digital-service-providers/services-catalogue
for business-level context, use cases and links to relevant policy.
The information available here explains how to integrate with Inland Revenue's services.

1.2   Intended audience

Access to the API end point is open to any software provider that has been on-boarded to the API (referred to throughout the remainder of this document as 'Digital Service Providers'). Access to the account data is open to any logon that currently has access to these resources on eServices. This includes tax intermediaries (such as tax agents and bookkeepers) and to customers using software on their own behalf.

1.3   Related services

The following application programming interfaces (APIs) complement this Gateway Service. Instructions on where to find the build packs for these APIs can be found in of this document.
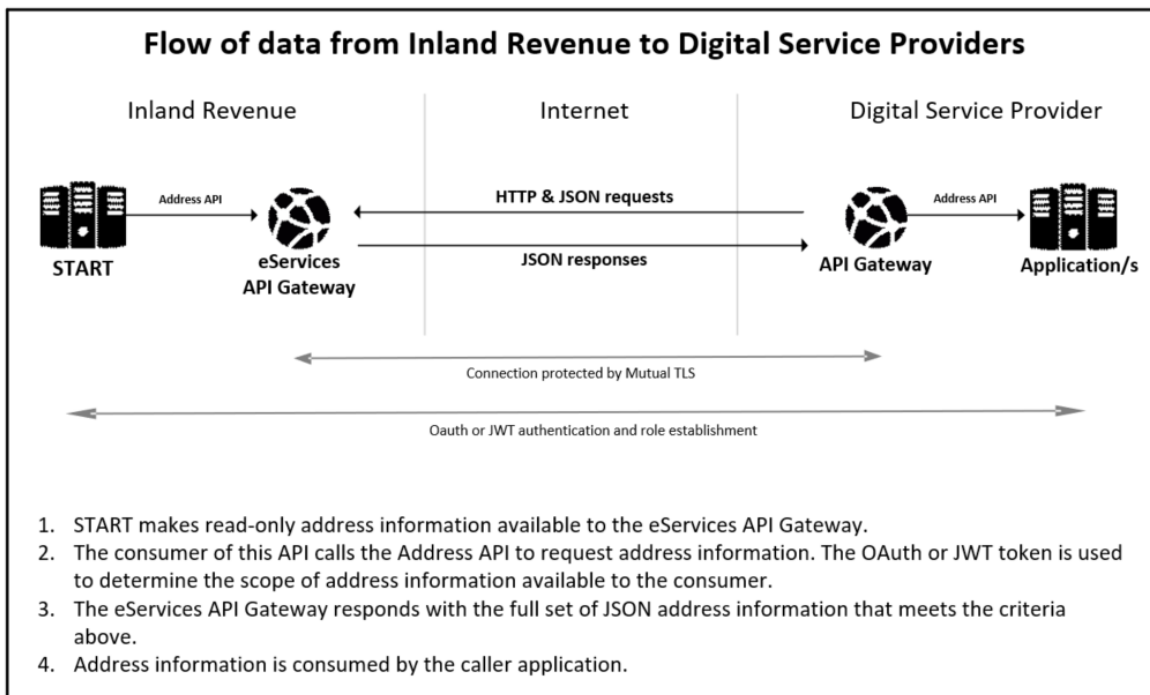
1.3.1   Identity and Access Services (required)

The Identity and Access Services (IAS) are used to authenticate access. Authentication tokens will need to be retrieved via IAS prior to making calls to this API.

2   Solution design

2.1   Architecture

Inland Revenue is offering a suite of web applications in order to facilitate interactions via software packages. This API will be used by approved organisations to retrieve addresses from Inland Revenue.

The diagram below illustrates the flow of data from Inland Revenue to the Digital Service Providers.

Flow of data from Inland Revenue to Digital Service Providers

1. START makes read-only address information available to the eServices API Gateway.
2. The consumer of this API calls the Address API to request address information. The OAuth or JWT token is used to determine the scope of address information available to the consumer.
3. The eServices API Gateway responds with the full set of JSON address information that meets the criteria above.
4. Address information is consumed by the caller application.

Inland Revenue
Te Tari Taake

2.1.1 Dependencies between the customer service APIs

This API is one of eight 'customer service' APIs designed to be used together—Account, Address, Bank, BIC, Contact, Customer, Name and Period. It is important to understand the dependencies between these when deciding which ones to implement, how to correctly sequence their adoption, how authorisation rules impact access, and how to use them in general.

These APIs align to START's data model as depicted below:
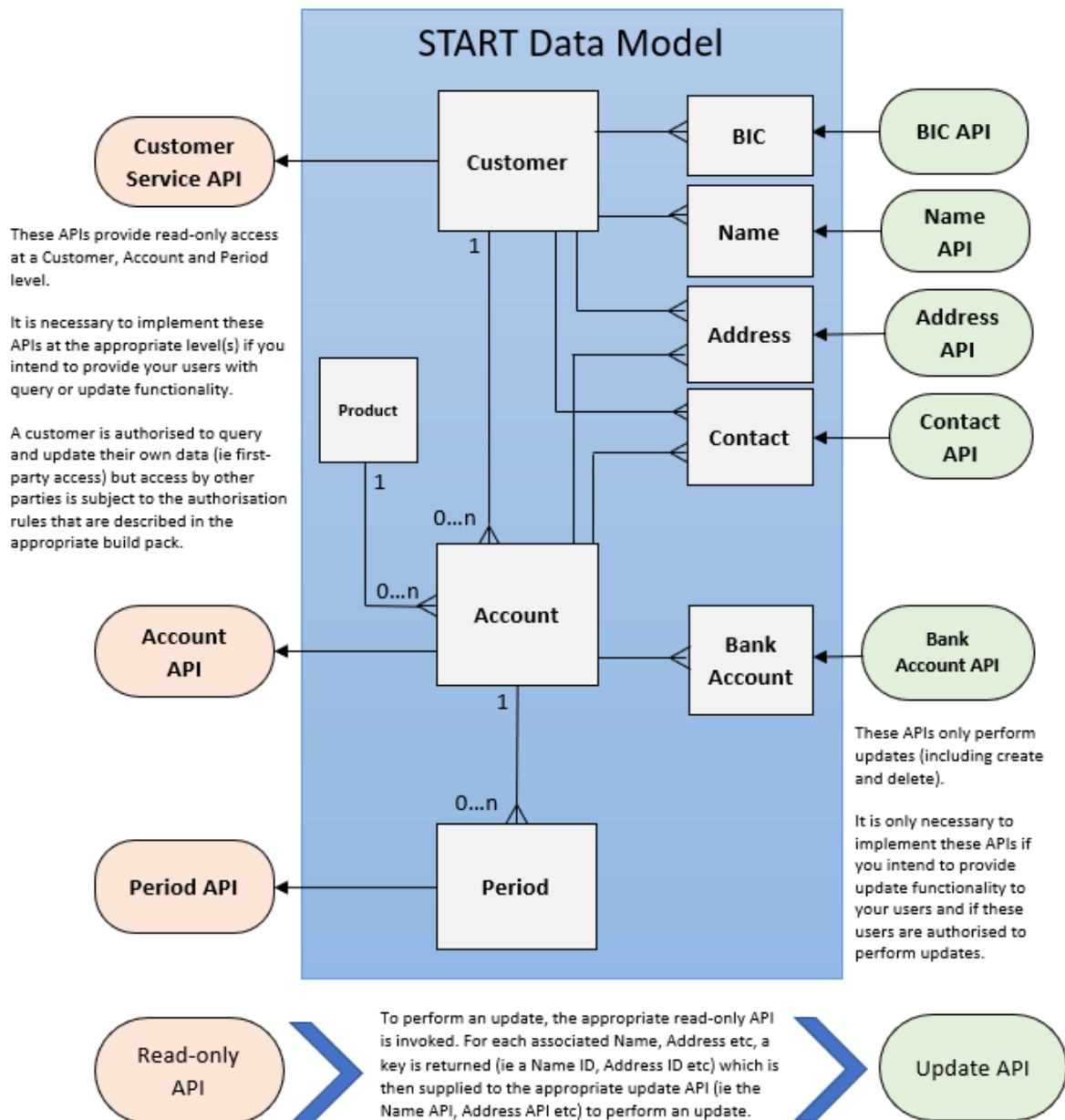
2.2 Messaging

This service supports the POST, PUT and DELETE methods. This service has three operations that use these HTTP methods:

- **CREATE:** POST—Creates a new address on a given customer or account
- **UPDATE:** PUT—Updates an existing address for a given customer or account
- **DELETE:** DELETE—Deletes an existing address.

2.2.1 Create

This operation is invoked by submitting a POST request to create a new address. This includes information that is unique to certain address types and may not always be present in a response.

Note that more information about each field can found in the accompanying YAML file.

RSP accounts are not supported.

A New Zealand address should be supplied using its Delivery Point Identifier (DPID). However, for unverified addresses the use of the Address object is permitted. Inland Revenue strongly recommends the use of DPID for identifying New Zealand addresses when interacting electronically with Inland Revenue and other public sector agencies. Delivery Point Identifiers can be sourced from NZ Post via either of the following places:

- The Postal Address File (PAF)
- The address checker API at:
  https://anypoint.mulesoft.com/exchange/portals/nz-post-group/b8271f09-2ad8-4e1c-b6b1-322c5727d148/nzpost.addresschecker/.
  - o Access to NZ Post's APIs and supporting resources can be obtained at https://www.nzpost.co.nz/business/developer-resource-centre.

Either an Address or NewZealand object must be provided, but not both.

2.2.1.1 Request payload

Field	Description
CustomerID	ID of the customer for whom an address should be added
CustomerIDType	Type of ID provided
AccountID	Unique ID to identify an account
AccountIDType	Type of ID submitted in Account ID field
Type	Type of address (mailing or physical)
Address.Street	Street address line 1
Address.Street2	Street address line 2
Address.Unit	Unit identifier
Address.UnitType	Unit type
Address.City	City name

Field	Description
Address.State	State name
Address.PostCode	Postal code
Address.Country	ISO two-digit standard (Australia is AU)
Address.Attention	The person to whom the correspondence is addressed
Address.Urbanisation	Urbanisation (See address notes)
Address.District	District type (See address notes)
Address.SubDistrict	District identifier (See address notes)
Address.SubProvince	SubProvince name (See address notes)
NewZealand.DPID	Unique ID for an address, provided by NZ Post
NewZealand.Attention	The person to whom the correspondence is addressed

2.2.1.2 Response payload

Note that the requirement status of each field is provided in the accompanying YAML file.

Field	Description
AddressID	Unique ID for the address just created.

2.2.2 Update

This operation is invoked by submitting a PUT request to update an existing address. All successful updates will return an HTTP 200 status with no response payload.

A New Zealand address should be supplied using its DPID. However, for unverified addresses the use of the Address object is permitted. Inland Revenue strongly recommends the use of DPID for identifying New Zealand addresses when interacting electronically with Inland Revenue and other public sector agencies. DPIDs can be sourced from NZ Post via either of the following places:

- The Postal Address File (PAF)
- The address checker API at:
  https://anypoint.mulesoft.com/exchange/portals/nz-post-group/b8271f09-2ad8-4e1c-b6b1-322c5727d148/nzpost.addresschecker/.
    - o   Access to NZ Post's APIs and supporting resources can be obtained at
      https://www.nzpost.co.nz/business/developer-resource-centre.

Either an Address or NewZealand object must be provided, but not both.

2.2.2.1   Request payload

Field	Description
AddressID	Unique ID for the address to update.
Attention	The person to whom the correspondence is addressed
Address.Street	Street address line 1
Address.Street2	Street address line 2
Address.Unit	Unit identifier
Address.UnitType	Unit type
Address.City	City name
Address.State	State name
Address.PostCode	Postal code
Address.Country	ISO two-digit standard (Australia is AU)
Address.Attention	The person to whom the correspondence is addressed
Address.Urbanisation	Urbanisation (See address notes)
Address.District	District type (See address notes)
Address.SubDistrict	District identifier (See address notes)
Address.SubProvince	SubProvince name (See address notes)
NewZealand.DPID	Unique ID for an address, provided by NZ Post
Address.Attention	The person to whom the correspondence is addressed

2.2.3 Delete

This operation is invoked by submitting a DELETE request to remove an existing address. All successful deletes will return an HTTP 200 status with no response payload. Once an address is removed, the AddressID will be ceased and cannot be reactivated. If this is done by mistake, a new address can be added which will generate a new AddressID.

2.2.3.1 Request payload

Field	Description
AddressID	Unique ID for the address to delete.

2.2.3.2 Address notes

The following fields contain different data depending on the country of the address:

Field	Region	Data
Urbanisation	New Zealand	Suburb/Rural
	Australia	Suburb/Place (Required)
	Europe	Distribution
District	New Zealand	Floor type
	Australia	Floor type
	Finland	Entrance
	Poland	Post Office
SubDistrict	New Zealand	Floor number
	Australia	Floor number
SubProvince	New Zealand	Building
	Australia	Building
Unit	Caribbean	PO Box

Unless otherwise specified in this table, the 'street' and 'city' fields are required:

Country	Required fields
Australia	Street, Urbanisation, State, PostCode
Canada	Street, City, State, PostCode
United States of America	Street, City, State, PostCode

2.3 Security

2.3.1 Information classification

The information exchanged via this API has an information classification of "**IN CONFIDENCE**". The following security standards therefore apply.

2.3.2 Transport layer security and certificates

Mutual Transport Layer Security (TLS) is implemented for this service. This requires the use of a publicly-issued X.509 certificate from one of the trusted certificate authorities. Please refer to the Identity and Access Services build pack for more details.

2.3.3 Ciphers
Inland Revenue currently supports TSL1.2 and TLS1.3. Please refer to Identity and Access Services build pack for supported ciphers.

2.3.4 Authentication options

This design will use JSON Web Tokens (JWT) or OAuth2.0 tokens and protocol to establish the calling party's identity. The OAuth2.0 method requires a myIR user to logon, while JWT is a machine-to-machine credential.

This API will require a unique identifier in order to establish the calling party's identity and to allow the access model to authenticate.

Refer to the Identity and Access Services build pack for more information.

2.3.4.1 OAuth

When using OAuth, the interaction with Inland Revenue is transacted under the identity of a myIR user. OAuth requires the presence of a myIR user, as this person must be available to supply their user ID, password and consent at run-time in order to be authenticated. OAuth is especially suited to cloud-based applications where the transacting parties are application users rather than providers.

HTTP headers intended for OAuth access services will be have the JWT prefixed with "Bearer ":

HTTP header	Example value
Authorization	Bearer {JWTAccessToken}

2.3.4.2 JWT

The alternative to OAuth is JWT, which does not require the presence of a myIR user. Authentication is based on the verification of a digital signature that (provably) belongs to a customer. In order to digitally sign their messages, the customer must acquire a digital certificate from a trusted certificate authority, or generate a self-signed certificate, and supply it to Inland Revenue during the on-boarding process. JWT is therefore appropriate when the following conditions apply:

- The interaction with Inland Revenue is conducted under the identity of an organisation, as opposed to a person AND

- The organisation has the technical and operational capability to securely obtain and manage digital certificates AND
- The organisation's interactions with Inland Revenue can occur in the absence of specific people due to staffing issues such as out-of-hours non-availability, staff turnover and absence from work.

These factors tend to limit the use JWT to larger corporations and public sector organisations. It is not suitable for cloud-based applications as it requires all application users to have their own digital certificates—this is administratively burdensome and requires these users to lodge their private keys with their application provider, which is insecure.

Gateway Services will use this token in the HTTP header of a message in the same manner that an OAuth token has been used, namely:

HTTP header	Example value
Authorization	{JWTAccessToken}

2.3.4.2.1.   startLogon

A myIR logon can be provided in order to use the myIR delegation model for identifying which customer or account can have their addresses modified. If the myIR logon is provided, then addresses can only be modified for customers or accounts the logon can access. If a myIR logon is not used, the field should be included with a value of null, and the subject will determine which customer or account can have their addresses modified.

2.3.4.2.2.   sub

A subject must be provided, which is the thumbprint of the signing certificate, and can be used to determine which customer or account can have their addresses modified. The subject will always be used to validate the signature of the JWT but will only be used for determining which customer or account can have their addresses modified when a value for **startLogon** is not provided. The subject can be used for access when the subject is a tax preparer—addresses can be modified for customers or accounts currently linked to the tax preparer.

3 Additional development resources

Current environment information for this service—including the end points for each environment—is available within the relevant Software Development Kit (SDK).

To access the SDK, do one of the following:

- Go to https://github.com/InlandRevenue and select this service
- Go to https://developerportal.ird.govt.nz and click the link to the SDK within the Gateway Service documentation (please register first).

3.1 OpenAPI specifications

An OpenAPI file allows for the description of the entire API, end points, operations on each end point, and operation parameters. The included .yaml file can be used along with an OpenAPI editor such as editor.swagger.io to view technical specifications for this operation and generate example client code.

To access the latest OpenAPI definition for this service, please do the following:

- Login to the developer portal at https://developerportal.ird.govt.nz (register first)
- Download and view the OpenAPI definition within the Gateway Service documentation.

4   Change log

This table lists all material changes that have been made to this build pack document since the release of V1 (most recent changes listed first). It does not encompass non-material changes, such as to formatting etc.

Date of change	Document section	Description
11/06/2024	2.3.2, 2.3.3	Removed details of supported certificate and ciphers from this document and replaced with the link to latest Identity and Access services build pack for the most current details
17/09/21		October 2021 changes
		New YAML file issued
	2.1.1	List and diagram of customer service APIs expanded to include new BIC API
	1.3	'Prerequisites' section removed and absorbed into new 'Security' section (2.4)
		'Related services' section added to build pack
	1.3.1	'Mutual Transport Layer security and certificates' section updated and moved into section 2.4.2
	1.3.2	'Authentication options' section modified and moved into section 2.4.4
	2.1	Diagram updated to include JWT
	2.1.1	'Dependencies between the customer services APIs' section moved here
	2.2	Heading changed from 'Supported HTTP methods' to 'Messaging'
	2.4	Security section upgraded: • 'Information classification' section added • 'Transport layer security and certificates' updated • 'Ciphers' section added • 'Authentication options' section modified
	3	'End points and OpenAPI specifications' section renamed 'Additional development resources'
	4	Glossary removed
06/05/21	2.4	Added note that RSP accounts are not supported for create
30/09/20		V1 released