Inland Revenue
Te Tari Taake

Inland Revenue

Build Pack: Customer API

Date: 17/09/2021

Inland Revenue
Te Tari Taake

Contents

Inland Revenue
Te Tari Taake

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 customer information as 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 customer 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.

The solution outlined in this document is intended to be used by technical teams and development staff, as it describes the technical interactions provided by this service. The reader is assumed to have a suitable level of technical knowledge to comprehend the information provided.

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 section 3 of this document.

1.3.1 Identity and Access Services (required)

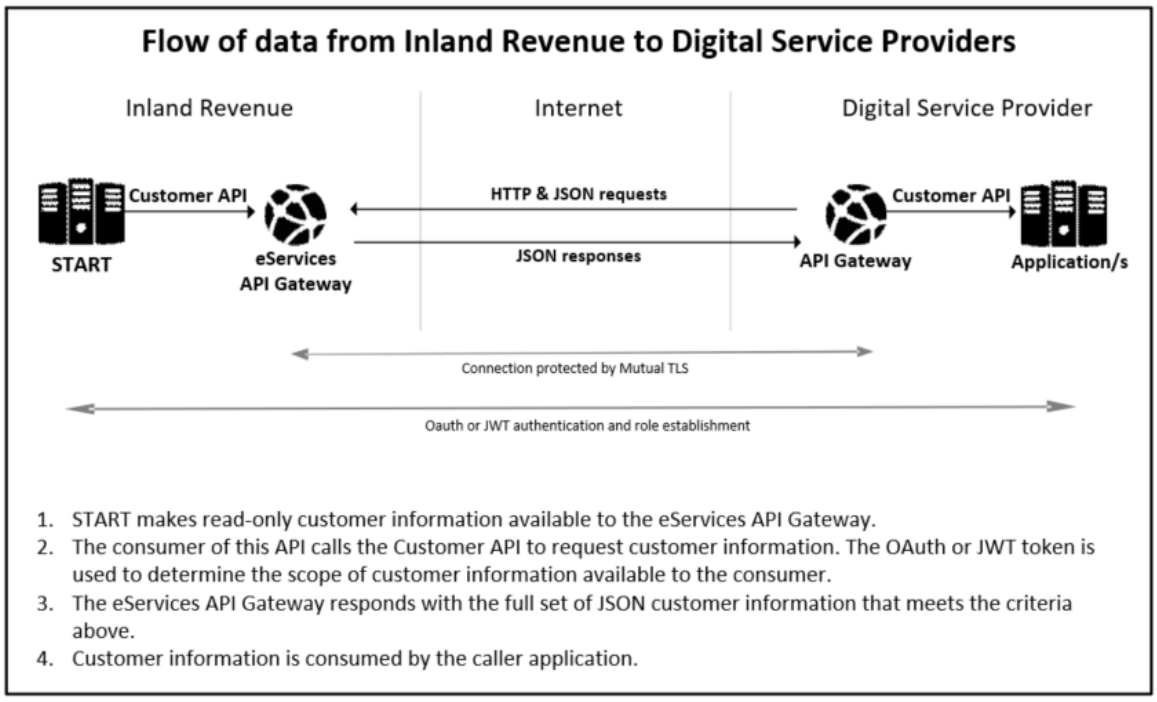
The Identity and Access Services (IAS) are used to authenticate access. Authentication tokens will need to be retrieved via IAS prior to making calls to this API.

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 customer information from Inland Revenue.

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



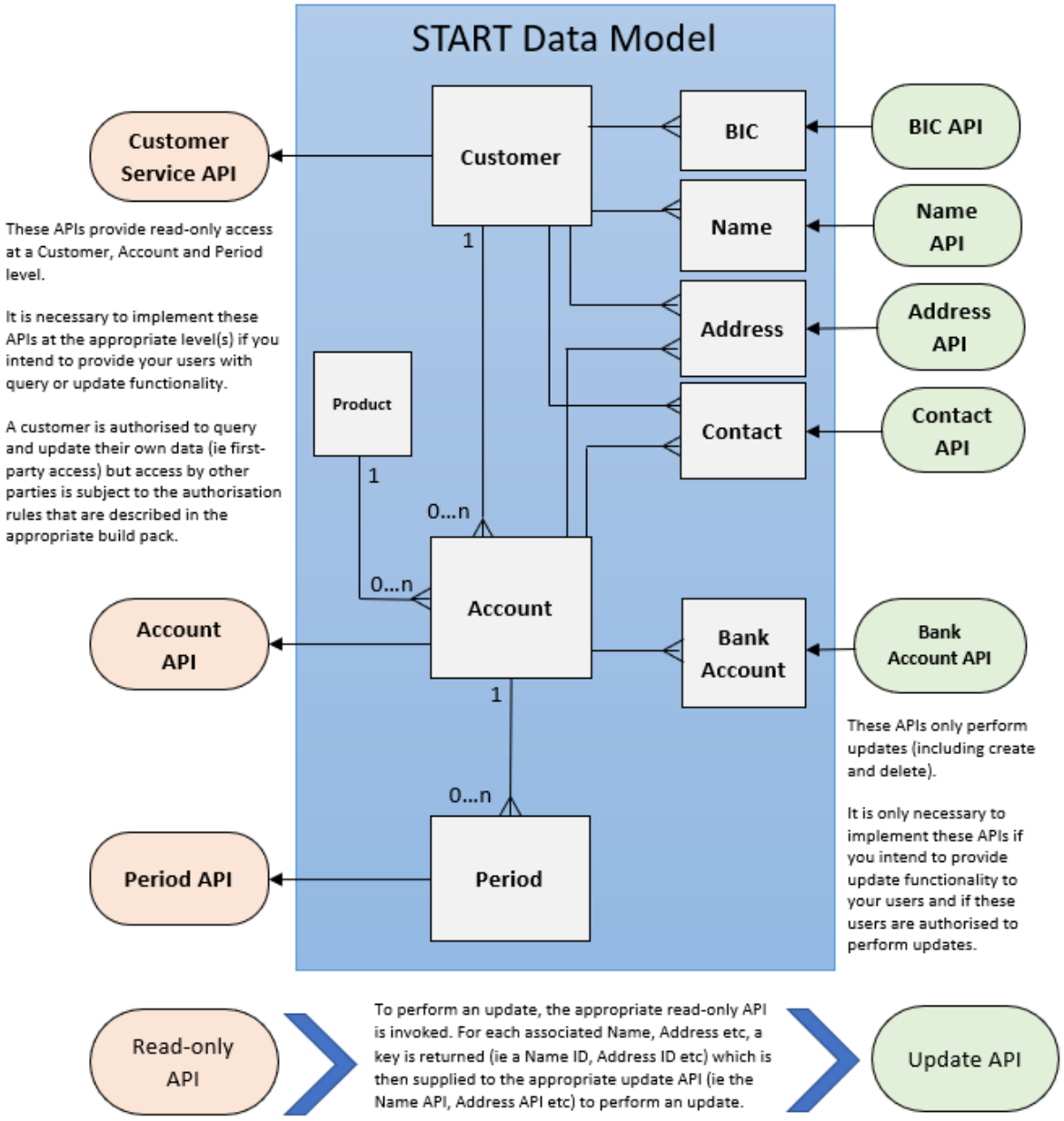
1. START makes read-only customer information available to the eServices API Gateway.
2. The consumer of this API calls the Customer API to request customer information. The OAuth or JWT token is used to determine the scope of customer information available to the consumer.
3. The eServices API Gateway responds with the full set of JSON customer information that meets the criteria above.
4. Customer 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 is a read-only service that supports the POST HTTP method and will not allow any updates.

2.2.1 Read

2.2.1.1 Request payload

Field	Requirement	Description
CustomerID	Mandatory	Unique ID to identify customer
CustomerIDType	Mandatory	Type of ID submitted in Customer ID field

2.2.1.2 Response payload

Field	Description
ID	The ID of the customer
IDType	The type of ID submitted in the ID field
EntityType	Customer subtype for non-individuals, INDVDL for Individuals
EntitySubType	Operating structure for non-individual and Customer segment for Individual
Commence	Commencement date of customer
Cease	Cessation date of customer
NZBN	New Zealand Business Number of the requested customer
BIC.BICCode	The Business Identification Code of a non-individual
Indicator.Indicator	A field that indicates additional specific information about this customer
Address.AddressID	Unique ID for address
Address.Type	Type of address (mailing or physical)
Address.Formatted	Formatted, single-line address
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.County	County name
Address.State	State name
Address.PostCode	Postal code
Address.Country	ISO two-digit standard (New Zealand is NZ)

Field	Description
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	Sub-province name (See address notes)
Address.Updated	Date on which address was last updated
Name.NameID	Unique ID for name
Name.Type	Name type (legal, preferred, trade, profile)
Name.Formatted	Formatted name
Name.LastName	Family name value
Name.MiddleName	Middle name value
Name.FirstName	Given name value
Name.Title	Title name
Name.Suffix	Name suffix
Name.Updated	Date on which name was last updated
Contact.ContactID	Unique ID for contact
Contact.ContactType	Contact type (ie primary, secondary)
Contact.Name	Name of contact
Contact.Updated	Date on which contact was last updated
Contact.Phone.PhoneID	Unique ID for phone
Contact.Phone.PhoneType	Mobile, home and/or business phone
Contact.Phone.Country	Country for phone—used to determine country code
Contact.Phone.AreaCode	Area code portion of phone number
Contact.Phone.PhoneNumber	Phone number, without country code
Contact.Phone.Extension	Extension number

Note: The BIC, Indicator, address, name, contact and phone objects can be repeated depending on what other customer information exists.

Inland Revenue
Te Tari Taake

2.2.1.3 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
	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

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 listed further below in this section. (Note that Inland Revenue does not issue certificates to external vendors for web service security implementations.)

Inland Revenue has the following requirements for accepting public X.509 keys:

- ECDSA (preferred) key length: 384 bits (or RSA key length: 2048 bits)
- Self-signed certificates are not accepted
- Certificates issued by private/internal certificate authorities are not accepted
- The same certificate cannot be used for the Test and Production environments.

Inland Revenue has adopted a trust-based authentication model and will only accept certificates that contain a pre-approved subject common name and have been issued by one of the following root certificate authorities, trusted and approved by Inland Revenue:

- Amazon
- Comodo
- DigiCert
- Entrust
- GeoTrust
- Let's Encrypt
- Sectigo
- Thawte.

Inland Revenue expects Digital Service Providers to use their Inland Revenue Developer Portal account to create their common name for both Test and Production certificates.

Please refer to the Digital Service Providers pages on the Inland Revenue website or contact your Inland Revenue onboarding representative at GatewayServices@ird.govt.nz for further details.

2.3.3 Ciphers

Inland Revenue currently supports TSL1.2 and TLS1.3, with the latter specifying a much smaller and more prescriptive suite of ciphers. As Inland Revenue's security gateways do not currently support the CCM mode (*counter with cipher block chaining message authentication code*) of operation, only the following ciphers will be supported over TLS1.3:

Status	TLS1.3 ciphers
Supported now and in the future	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256

The following TLS1.2 ciphers are currently supported but some will be deprecated as below:

Status	TLS1.2 ciphers
Supported now and in future	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Supported now but will be deprecated on 31 March 2022	• TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
Supported now but will be deprecated on 31 December 2022	• TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384

2.3.4 Authentication options

This design uses 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 requires 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 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 customers for whom customer information should be retrieved. If the myIR logon is provided, then information will only be shown for customers the logon can access.

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 information should be retrieved. The subject will always be used to validate the signature of the JWT but will only be used for determining which customer information to retrieve when a value for **startLogon** is not provided. The subject can be used for access when the subject is a tax preparer—customer information will be returned for customers currently linked to the tax preparer.

Inland Revenue
Te Tari Taake

3 Additional development resources

3.1 End points

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).

3.2 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.

Inland Revenue
Te Tari Taake

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).

Date of change	Document section	Description
17/09/21		October 2021 release changes
		New YAML file issued
	2.1.1	List and diagram of customer service APIs expanded to include new BIC API
	1	'Prerequisites' section removed and absorbed into new 'Security' section (2.4)
	1.3	'Related services' section added to build pack
	1	'Mutual Transport Layer security and certificates' section updated and moved into section 2.3
	1	'Authentication options' section modified and moved into section 2.3
	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'
	2.3	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
17/02/21	N/A	(Minor formatting changes – no development changes)
26/11/20	2.4.2	Added new name type of PRF (Profile), which indicates that a name is only used for a profile, and not the entire customer. Also updated YAML file with this change.
30/09/20		V1 released