Inland Revenue
Te Tari Taake

Inland Revenue

Build Pack: Prescribed Investor Rate (PIR) Service

Date: 18/11/2022

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. This service is an application programming interface (API) that external applications can call in order to request a "suggested" Prescribed Investor Rate (PIR) value for an individual customer. This API is one of a set of calculators that will be exposed via Gateway Services.

It is important to note that this API will only provide the suggested PIR when enough information about the member/investor is stored in START to calculate the rate. Inland Revenue does not know with certainty that the PIR value calculated reflects the customer's current position therefore the customer is entitled to override the value that this API returns.

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

The solution outlined in this document is intended to be used by software providers developing solutions for Portfolio Investment Entity (PIE) providers as well as intermediaries (tax preparers). Portfolio Investment Entity providers are financial institutions, and each PIE is a separate legal entity. KiwiSaver schemes are a specialised type of PIE, whose investors are referred to as members.

Tax preparers (or intermediaries) act as go-betweens for Inland Revenue and their clients. They can be tax agents, PAYE intermediaries, or other intermediaries. Tax preparers act on behalf of their clients, who can be individuals or non-individuals, including PIE providers.

The reader is assumed to have a suitable level of technical knowledge in order to comprehend the terms and abbreviations are used throughout this document.

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 4 of this document.

1.3.1 Identity and Access Services (required)

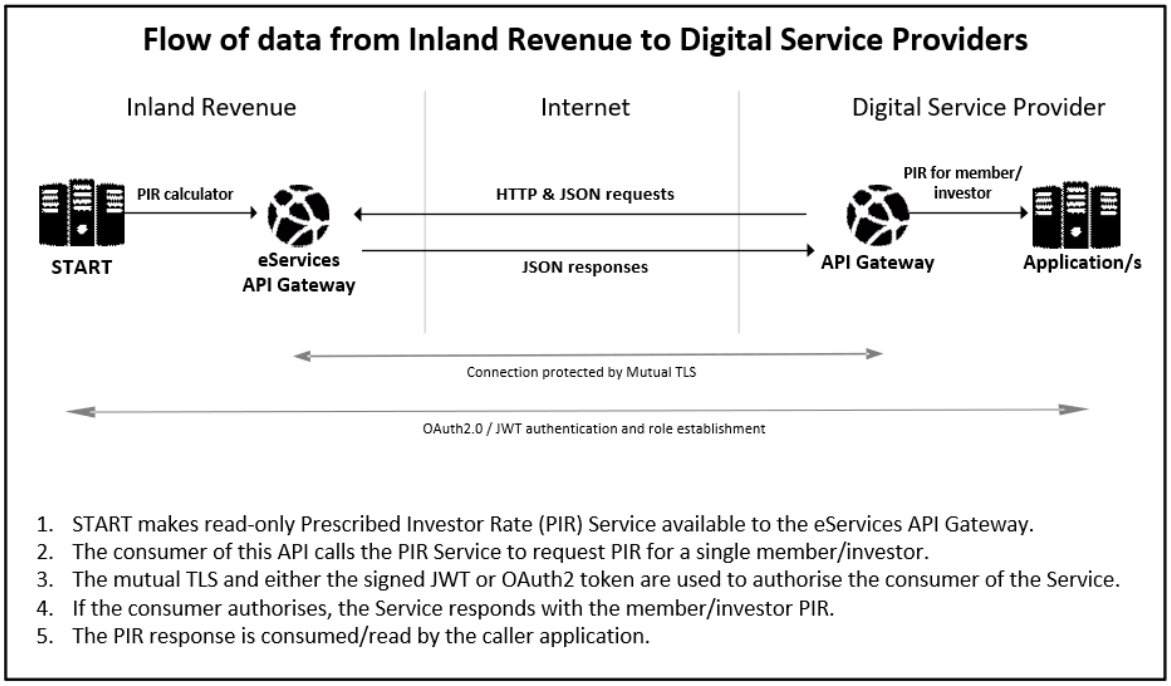
The Identity and Access Services (IAS) are used to authenticate access. Authentication tokens will need to be retrieved via IAS prior to making calls to this API.

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 prescribed investor rates from Inland Revenue.

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



2.2 Messaging

This service has one operation—the POST HTTP method:

- **PIR:** Retrieves the suggested prescribed investor rate for the investor whose IRD number is provided in the request payload.

2.2.1 Request payload

Field	Requirement	Description
IRD	Mandatory	Investor IRD number (individuals only). This field is validated to ensure that it exists and is active. The calculated suggested PIR value will be this investor's current PIR. The IRD field will be the PIE investor or KiwiSaver scheme member. • For supported formats. Must comply with Modulus 11 check (see IR Number Validation Modulus 11 Digit Check) • If IR number is eight characters, then pad with a leading zero '0' to make a total of nine characters. Numeric only, any letters or special characters will cause the check digit validation to fail.
PieIRD	Optional	PIE IRD number. This field is validated to ensure that it exists, is active and is a PIE entity. The PIE IRD will be either a PIE financial institution or KiwiSaver scheme provider. • For supported formats. Must comply with Modulus 11 check (see IR Number Validation Modulus 11 Digit Check) • If IR number is eight characters, then pad with a leading zero '0' to make a total of nine characters. The PIE IRD number is not expected when the consumer of the service is a tax preparer (intermediary) but is required when the request is made by a PIE entity or a KiwiSaver scheme. If the request is made by one of the latter two types of consumers and PIE IRD is not provided, error code **PIR101** will be returned.
FormattedName	Optional	Formatted name of the investor. Used for soft matching.
FirstName	Optional	First name of the investor. Used for soft matching.
MiddleName	Optional	Middle name of the investor. Used for soft matching.
LastName	Optional	Last name of the investor. Used for soft matching.
Dob	Optional	Date of birth of the investor. Used for soft matching.
FormattedAddress	Optional	Investor formatted address. Used for soft matching.

Field	Requirement	Description
Street	Optional	Investor street. Used for soft matching.
City	Optional	Investor city. Used for soft matching.
PostCode	Optional	Investor post code. Used for soft matching.
State	Optional	Investor state. Used for soft matching.
Country	Optional	Investor country, ISO 2A format. Used for soft matching.
FilingPeriod	Optional	Filing period (tax year) of investor's income tax account for which the suggested PIR should be calculated. If not provided, current filing period will be assumed. NOTE: The filing period is always the final day of March for any given tax year. For example, "2021-03-31" for 2021, regardless of the balance date on the investor's income tax account.

2.2.2 Response payload

Field	Description
IRD	Investor IRD number (individuals only). The IRD field will be the PIE investor or KiwiSaver scheme member.
PieIRD	PIE IRD number. The PIE IRD will be either a PIE financial institution or KiwiSaver scheme provider. To protect investor privacy, PieIRD will be part of the response payload only if it was provided in the request payload.
SuggestedPirRate	Suggested PIR for investor. Only contained in response when an investor PIR could be calculated.
PirRateNotFound	Only contained in response when an investor PIR could not be calculated.

Inland Revenue
Te Tari Taake

2.3 Security

2.3.1 Information classification

The information exchanged via this service 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.

Inland Revenue
Te Tari Taake

2.3.3 Ciphers

While Inland Revenue currently supports TSL1.2 and TLS1.3 which specifies 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

2.4 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 can either provide a myIR user or a credential for machine-to-machine authentication.

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.

2.4.1 OAuth

When using OAuth, the interaction with Inland Revenue is transacted under the identity of a myIR user, with the OAuth token being used to identify which customers the consumer of service has access to. If the member/investor does not exist in this list, access will be denied. The myIR user 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}

To authenticate successfully using OAuth token, **one of the following must be true** about the myIR user being authenticated:

- They belong to the PIE entity or KiwiSaver scheme identified by the "PieIRD" number in the request.
- They belong to the KiwiSaver scheme provider who is linked to the KiwiSaver scheme identified by the "PieIRD" number in the request *and* the customer identified by the "IRD" number in the request is a KiwiSaver member of said scheme provider.
- They belong to the KiwiSaver scheme administration manager managing a KiwiSaver scheme provider who is linked to a KiwiSaver scheme identified by the "PieIRD" number in the request *and* the customer identified by the "IRD" number in the request is a member of said KiwiSaver scheme.
- They belong to a tax preparer of the PIE entity or KiwiSaver scheme identified by the "PieIRD" number in the request.
- They belong to a tax preparer of the investor client identified by the "IRD" number in the request.

In addition, **one of the following must be true** to establish the relationship between the investor (identified by the "IRD" number in the request) and the PIE entity or KiwiSaver scheme (identified by the "PieIRD" number in the request):

- The investor is a member of the KiwiSaver scheme.
- The investor information exists on the PIE Reconciliation return filed by the PIE entity or the KiwiSaver scheme.
- The investor can be confidently verified via soft matching process based on name, date of birth and address information provided in the request.
- The myIR user authenticated has client list access to the client identified by the "IRD" number in the request. This client list access must exist in the form of either customer master link or account level link to said client's income tax account.

2.4.2 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 etc).

These factors tend to limit the use of 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}

There are two ways in which the JWT token can be validated—these are explained in the sections that follow.

NOTE: If the 'startLogon' claim is not left as null then only the 'startLogon' will be used for validation. If it is left null than only the 'sub' claim will be used for validation.

Inland Revenue
Te Tari Taake

2.4.2.1 'startLogon' claim

As outlined in the Identity and Access Services build pack, the resource owner can provide a myIR user for the 'startLogon' claim in the JWT payload. If the start logon is provided there are two validations that take place:

To validate an API consumer, **one of the following must be true** about the myIR user being authenticated:

- They belong to the PIE entity or KiwiSaver scheme identified by the "PieIRD" number in the request.
- They belong to the KiwiSaver scheme provider who is linked to the KiwiSaver scheme identified by the "PieIRD" number in the request and the customer identified by the "IRD" number in the request is a KiwiSaver member of said scheme provider.
- They belong to the KiwiSaver scheme administration manager managing a KiwiSaver scheme provider who is linked to a KiwiSaver scheme identified by the "PieIRD" number in the request *and* the customer identified by the "IRD" number in the request is a KiwiSaver member of said scheme.
- They belong to a tax preparer of the PIE entity or KiwiSaver scheme identified by the "PieIRD" number in the request.

2.4.2.2 'sub' claim

For this service the resource owner has the option to leave the 'startLogon' claim as null. If this is the case, the 'sub' claim's certificate thumbprint will be used to validate the resource owner.

To validate an API consumer, **one of the following must be true**:

- The entity associated to Gateway credential is the KiwiSaver scheme provider who is linked to the KiwiSaver scheme identified by the "PieIRD" number in the request and the customer identified by the "IRD" number in the request is a KiwiSaver member of said scheme provider.
- The entity associated to the Gateway credential is the KiwiSaver scheme administration manager managing a KiwiSaver scheme provider who is linked to a KiwiSaver scheme identified by the "PieIRD" number in the request *and* the customer identified by the "IRD" number in the request is a KiwiSaver member of said scheme.
- The entity associated to the Gateway credential is a tax preparer of the PIE entity or KiwiSaver scheme identified by the "PieIRD" number in the request.
- The entity associated to the Gateway credential is a tax preparer of the investor identified by the "IRD" number in the request. The entity is considered a tax preparer of the investor.

In addition to successfully authenticate using either the "startLogon" claim or "sub" claim, **one of the following must be true** to establish the relationship between the investor (identified by the "IRD" number in the request) and the PIE entity or KiwiSaver Scheme (identified by the "PieIRD" number in the request):

- The investor is a member of the KiwiSaver scheme.
- The investor information exists on the PIE Reconciliation return filed by the PIE entity or the KiwiSaver scheme.
- The investor can be confidently verified via soft matching process based on name, date of birth and address information provided in the request.
- When "startLogon" claim is used, the myIR user must have client list access to the client identified by the "IRD" number in the request. This client list access must be either customer master access to the client or account level access to the client's income tax account.
- When the "sub" claim is used, the customer authenticated must be linked to the client identified by the "IRD" number in the request. This link must be either customer master link to the client or account level link to the client's income tax account.

3 Error codes

3.1 Field validation error codes

Error code	Occurs
EV1000	No incoming POST content found
EV1100	Invalid input parameters. Please check documentation.
PER100	Filing period provided in FilingPeriod parameter does not exist on the investor customer's income tax account.

For field validation errors the HttpStatusCode returned will be '400—bad request'.

3.2 Authentication validation error codes

Error code	Occurs
EV1023	No customer associated to TLS cert
EV1024	Authentication error
EV1025	Missing OAuth or JWT token in the HTTP header
EV1026	Authentication error—Issued date or expiry date is invalid
EV1027	Certificate or credential could not be found
EV1028	Authentication error—JWT signature validation failed
EV1029	Authentication error—JWT algorithm not configured on credential doc
EV1030	Unknown authentication error
EV1040	Start logon associated to OAuth token does not have access to any accounts or customers
EV1041	Start logon associated to OAuth token does not have access to member/investor customer
EV1042	Unable to validate API consumer to JWT provided
EV1043	Unable to validate JWT to member/investor IRD number provided
IR003	The IRD supplied has been queried too many times within the past 24 hours.

For authentication errors the HttpStatusCode returned will be '401—unauthorised'.

Inland Revenue
Te Tari Taake

3.3 Other error codes

Error code	Occurs
PIR101	Returned when PieIRD field is required (the call is made by a PIE entity or a KiwiSaver scheme) but is not provided. PieIRD is not expected when the call is made by a tax preparer. The tax preparer status of the caller is determined by the myIR web logon through JWT or OAuth authorisation. That is, if the myIR logon belongs to a tax preparer (intermediary), the service will not expect PieIRD. If the myIR web logon does ***not*** belong to a tax preparer (intermediary), then the service will assume that the caller is a PIE entity or a KiwiSaver scheme and require PieIRD. **NOTE:** If authentication is done without a myIR web logon (only possible with JWT), the service will assume the caller is a PIE entity or a KiwiSaver scheme and require PieIRD.
PIR150	Unknown error occurred while processing

For other errors, the HttpStatusCode returned will be '500—internal server error'.

Inland Revenue
Te Tari Taake

4 Additional development resources

4.1 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).

4.2 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

5 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
18/11/22	2.2.1	• Updated the URL link to point to the GitHub page "IR Number Validation Modulus 11 Digit Check".
18/08/21	1.2	• Intended audience information updated to include tax preparers / intermediaries
	1.3	• 'Prerequisites' section removed and consolidated into new 'security' section
	5	• 'End points and OpenAPI specifications' section renamed 'Additional development resources'

	2	• Restructured section 2 (Solution design)
		  ○ Updated security section (2.3)
		  ○ Added 'Ciphers' section
		  ○ Updated TLS and certificate information

	2.2.2	• Added detail to PieIRD field description
	2.2.1	• PieIRD field changed from 'mandatory' to 'optional', and note added to field description
	2.3.4	• Opening paragraph corrected (used to say JWT is machine-to-machine only)
	2.3.4	• Authorisation section removed and incorporated into 'Authentication options' section
	2.4	• JWT and OAuth sections updated
		• Glossary removed
22/02/21	2.2.2	• Description updated for 'startLogon claim' in table of validation methods • 'Tax agent' changed to 'tax preparer'
	3.1.2	• New field added: filingPeriod
	4.1	• New error code added: PER100
	N/A	• New YAML issued
21/10/20	1.3.2	• New section added – 'Authentication options'

Inland Revenue
Te Tari Taake

Date of change	Document section	Description
11/08/20	2.2.2	• Note added: NOTE: If the 'startLogon' claim is not left as null then only the 'startLogon' will be used for validation. If it is left null than only the 'sub' claim will be used for validation. • Description of 'StartLogon' claim updated
14/07/20	2.2.2	• Minor typo corrected with numbering in table
		•
28/05/20	YAML	• PIR calculator YAML updated
	1.1	• Updates made to boxed instructions for where to find additional information such as business-level context, use cases and links to relevant policy.
	5	• Updated entire section with new instructions on where to find end points, YAML files etc.
09/04/20		• V1.0 released