Inland Revenue
Te Tari Taake

Inland Revenue

# Build Pack: Prescribed Investor Rate (PIR) Service

**Date:** 11/08/2020
**Version:** v1.0

# 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. 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 the Portfolio Investment Entity (PIE) providers. PIE providers are financial institutions and each PIE is a separate legal entity. KiwiSaver schemes are a specialised type of PIE, there investors are referred to as members.

The reader is assumed to have a suitable level of technical knowledge in order to comprehend the information provided. A range of technical terms and abbreviations are used throughout this document, and while most of these will be understood by the intended readers, a glossary is provided at the end.

## 1.3    Prerequisites

| Party | Requirement | Description |
|---|---|---|
| **Digital Service Provider** | Acquire a X.509 certificate from a competent authority for the Test and Production environments | This is required when using mutual TLS with cloud-based service providers or financial institutions.<br>Note that the same certificate cannot be used for the Test and Production environments. |

### 1.3.1    Mutual Transport Layer Security and certificates

Mutual transport layer security (TLS) is implemented for this API. This requires the use of a publicly-issued X509 certificate from one of the trusted certificate authorities. Inland Revenue does not issue certificates to external vendors for web service security implementations.

Inland Revenue has the following minimum requirements for accepting public X509 keys:

- Minimum Key Length: 2048
- Signature Algorithm: SHA256[RSA]
- Self-signed certificates are not accepted
- Certificates issued by a private/internal certificate authority are not accepted.

In general, shorter-lived certificates offer a better security posture since the impact of key compromise is less severe but there is no minimum requirement for certificate expiry periods.

Below is a list for examples of certificate authority providers with no recommendations or rankings incorporated. It is recommended that a business researches which certificate authority meets their requirements:

- Comodo
- GeoTrust
- DigiCert
- GlobalSign
- Symantec
- Thawte
- IdenTrust
- Entrust
- Network Solutions
- RapidSSL
- Entrust Datacard
- GoDaddy.

## 2 Authorisation

### 2.1 Authorisation header using OAuth2 or JWT

This API will require either an Oauth2 or signed JSON web token (JWT) in the authorisation header. The provided token will be used in order to determine the digital service provider's identity.

#### 2.1.1 OAuth2 authorisation token

Inland Revenue's implementation of the OAuth 2 standard conforms to the authorisation code grant flow described in section 4.1 of RFC 6749. For further details and requirements, please see the Identity and Access Services build pack.

#### 2.1.2 M2M using client signed JWT authorisation

Inland Revenue's machine-to-machine (M2M) authentication mechanism will use client-signed JSON web tokens (JWT). When applying this pattern, the external parties fulfil the following roles:

- **Resource Owner**—this is the party under whose identity the transaction is being undertaken. This has the same meaning as 'Resource Owner' in the OAuth protocol. The resource owner's identity binds to a myIR user ID within START, and from this to START's authorisation rules and the user's access rights. Each service/API call is verified and trusted because it is digitally signed with a public/private key pair belonging to the resource owner using an approved signing algorithm (currently RSA or preferably ECDSA). The resource owner's public key is exchanged during the on-boarding process.

- **Service Provider**—this is the party that operates the application that consumes Inland Revenue's gateway services. This is the equivalent of the client application when using the OAuth protocol. The service provider encrypts the data that they exchange with Inland Revenue.

For further details/requirements please see the Identity and Access Services build pack.

## 2.2 Authorisation validation

### 2.2.1 OAuth2 authorisation validation

The myIR logon associated to the OAuth2 token will be 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.

### 2.2.2 JWT authorisation validation

The table below describes the two ways in which the JWT token can be validated.

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.

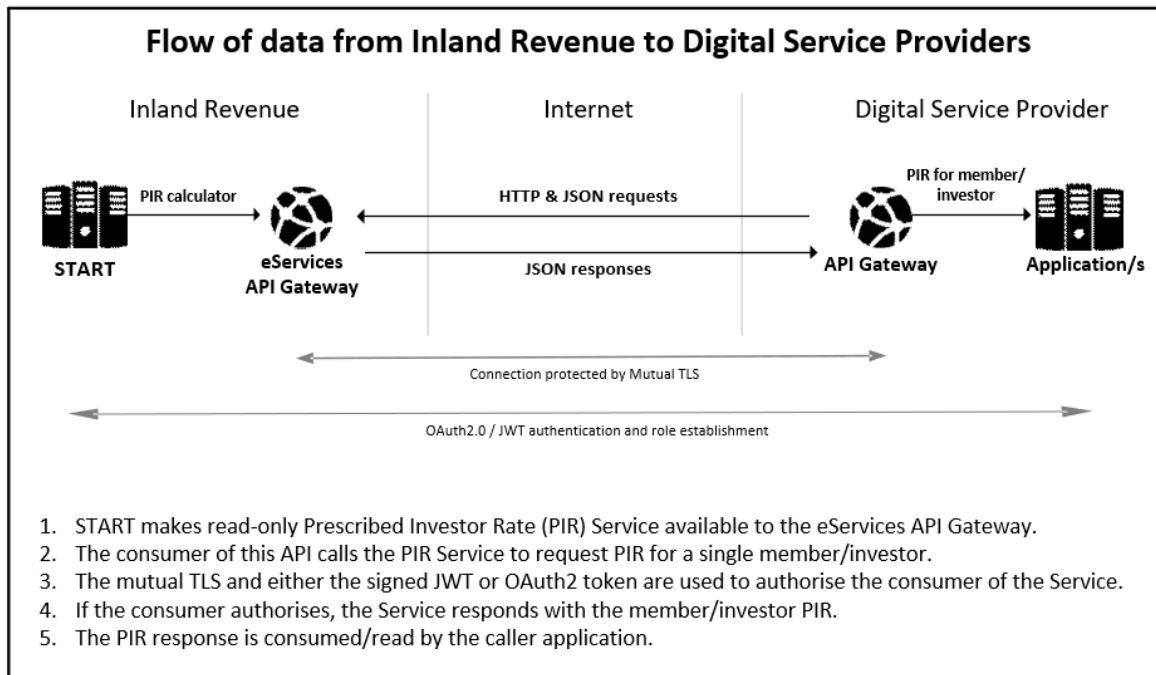| Validation method | Description |
|---|---|
| **'startLogon' claim** | As outlined in the Identity and Access Services build pack, the resource owner can provide a myIR logon for the 'startLogon' claim in the JWT payload. If the start logon is provided there are two validations that take place:<br>1. To validate an API consumer, one of the following must be true:<br> o Customer associated to TLS credential is the same as the customer associated to start logon.<br> o Customer associated to TLS credential is a software intermediary and they are linked to the customer associated to the start logon.<br> o Customer associated to TLS credential is a tax agent and they are linked to the customer associated to the start logon.<br> o Customer associated to TLS credential is a software intermediary and they are linked to a tax agent who is linked to the customer associated to the start logon.<br>2. To validate start logon has access to the investor/members PIR rate one of the following must be true:<br> o The start logon belongs to a KiwiSaver scheme and scheme to member relationship exists.<br> o The start logon belongs to a KiwiSaver scheme admin and an admin to scheme to member relationship exists.<br> o The start logon belongs to a PIE financial institution and a PIE certificate exists for the PIE institution and investor.<br> o Soft-matching of investor IRD number, name, date of birth and address which were provided as optional parameters in request payload. |

| Validation method | Description |
|---|---|
| **'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. There are two validations that take place:<br><br>1. To validate an API consumer, one of the following must be true:<br>    o Customer associated to TLS credential is the same as the customer associated to JWT credential (signing)<br>    o Customer associated to TLS credential is a software intermediary and they are linked to the customer associated to the JWT credential.<br>    o Customer associated to TLS credential is a tax agent and they are linked to the customer associated to the JWT credential.<br>    o Customer associated to TLS credential is a software intermediary and they are linked to a tax agent who is linked to the customer associated to the JWT credential.<br><br>2. To validate relationship between JWT credential customer and member/investor one of the following must be true:<br>    o The JWT credential belongs to a KiwiSaver scheme and scheme-to-member relationship exists.<br>    o The JWT credential belongs to a KiwiSaver scheme admin and an admin-to-scheme-to-member relationship exists.<br>    o The JWT credential belongs to a PIE financial institution and a PIE certificate exists for the PIE institution and investor.<br>    o Soft-matching of investor IRD number, name, date of birth and address which were provided as optional parameters in request payload. |

# 3 Solution design

## 3.1 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.



**Flow of data from Inland Revenue to Digital Service Providers**

1. START makes read-only Prescribed Investor Rate (PIR) Service available to the eServices API Gateway.
2. The consumer of this API calls the PIR Service to request PIR for a single member/investor.
3. The mutual TLS and either the signed JWT or OAuth2 token are used to authorise the consumer of the Service.
4. If the consumer authorises, the Service responds with the member/investor PIR.
5. The PIR response is consumed/read by the caller application.

## 3.2 PIR messages

### 3.2.1 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. <br>• For supported formats. Must comply with Modulus 11 check (see https://www.classic.ird.govt.nz/resources/d/a/dac415c0-456f-4b2f-87b6-0e76cbedd3ec/2020+RWT%26NRWT+Specification+Document+v1.0.pdf) <br>• If IR number is 8 characters, then pad with a leading zero '0' to make a total of 9 characters. <br>Numeric only, any letters or special characters will cause the check digit validation to fail. |
| **PieIRD** | Mandatory | 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. <br>• For supported formats. Must comply with Modulus 11 check (see https://www.classic.ird.govt.nz/resources/d/a/dac415c0-456f-4b2f-87b6-0e76cbedd3ec/2020+RWT%26NRWT+Specification+Document+v1.0.pdf) <br>• If IR number is 8 characters, then pad with a leading zero '0' to make a total of 9 characters. |
| **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. |
| **Street** | Optional | Investor street. Used for soft matching. |
| **City** | Optional | Investor city. Used for soft matching. |

| Field | Requirement | Description |
|---|---|---|
| **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. |

### 3.2.2    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. |
| **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. |

# 4 Error codes

## 4.1 Field validation error codes

| Error code | Occurs |
|------------|--------|
| EV1000 | • No incoming POST content found |
| EV1100 | • Invalid input parameters. Please check documentation. |

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

## 4.2 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'.

## 4.3 Other error codes

| Error code | Occurs |
|------------|--------|
| PIR150—Unknown | • Unknown error occurred while processing |

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

# 5    End points and OpenAPI specifications

## 5.1    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).

## 5.2    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.

# 6    Glossary

| Acronym/term | Definition |
|---|---|
| API | Application Programming Interface—set of functions and procedures that allow applications to access the data or features of another application, operating system or other service. |
| Authentication | The process that verifies the identity of the party attempting to access Inland Revenue |
| Authorisation | The process of determining whether a party is entitled to perform the function or access a resource |
| End points | A term used to describe a web service that has been implemented |
| FIPS | Federal Information Processing Standard—a suite of IT standards from the US Federal Government |
| Gateway | Inland Revenue's web services gateway |
| HTTP, HTTPS | Hyper Text Transmission Protocol (Secure)—the protocol by which web browsers and servers interact with each other. When implemented over TLS1.2 HTTP becomes HTTPS. |
| IAMS | Identity and Access Management—a logical component that performs authentication and authorisation. Physically it is a set of discrete hardware and software products, plug-ins and protocols. Usually implemented as separate External IAMS (XIAMS) and Internal IAMS. |
| IAS | Identity and Access Service |
| IP | Internet Protocol—the principal communication protocol in the Internet protocol suite for relaying datagrams across networks |
| IRD | Inland Revenue Department (ie IRD Numbers) |
| JWT | JSON Web Token—a compact, URL-safe means of representing claims to be transferred between two parties |
| M2M | Machine-to-machine communication |
| OAuth | An HTTPS based protocol for authorising access to a resource, currently at version 2 |
| OpenAPI specifications | Formerly known as Swagger specifications—a specification for machine-readable interface files for describing, producing, consuming and visualising RESTful web services. |
| Payloads | This refers to the data contained within the messages that are exchanged when a web service is invoked. Messages consist of a header and a payload. |
| Schemas | An XML schema defines the syntax of an XML document, in particular of a payload. The schema specifies what a valid payload must or can contain, as well as validating the payload. |
| SHA | Secure Hashing Algorithm. There is a family of them that provide different strengths. SHA-2 is currently favoured over SHA-1, which has been compromised. |

| Acronym/term | Definition |
|---|---|
| SOAP | Simple Object Access Protocol—a set of standards for specifying web services. GWS uses SOAP version 1.2 |
| SSL | Secure Sockets Layer certificates—used to establish an encrypted connection between a browser or user's computer and a service or website |
| START | Simplified Taxation and Revenue Technology—IR's new core tax processing application. It is an implementation of the GenTax product from FAST Enterprises. |
| TLS1.2 | Transport Layer Security version 1.2—the protocol that is observed between adjacent servers for encrypting the data that they exchange. Prior versions of TLS and all versions of SSL have been compromised and are superseded by TLS1.2. |
| URL | Universal Resource Locator—also known as a web address |
| X.509 certificate | An international standard for encoding and describing a digital certificate. In isolation a public key is just a very large number, the X.509 certificate to which it is bound identifies whose key it is, who issued it, when it expires etc. When a counterparty's X.509 digital certificate is received, the recipient takes their public key out of it and store the key in their own keystore. The recipient can then use this key to encrypt and sign the messages that they exchange with this counterparty. |
| XIAMS | External IAMS—an instance of IAMS that authenticates and authorises access by external parties, for example customers, trading partners etc, as opposed to internal parties such as staff |
| YAML | "YAML Ain't Markup Language"—a human-readable data-serialisation language commonly used for configuration files and in applications where data is stored or transmitted. |

# 7 Change log

This table lists all material changes that have been made to this build pack document since the release of v1.0 (most recent changes listed first). It does not encompass non-material changes, such as to formatting etc.

| Version | Date of change | Document section | Description |
|---------|----------------|------------------|-------------|
| **1.0** | 11/08/20 | 2.2.2 | • Note added:<br>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.<br>• 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 |