Inland Revenue
Te Tari Taake

Inland Revenue

Build Pack: IRD Number Validation Service API

Date: 05/12/2019
Version: v0.8

Inland Revenue
Te Tari Taake

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 real-time when enrolling a customer to validate the customer's IRD number. The objective of this API is to reduce the occurrences of customers being enrolled with an incorrect IRD number which, when it does occur, can be very disruptive for external partners, customers and Inland Revenue.

It is important to note that this API does not return an IRD number. It enables the consumer of the API to assess whether the IRD number and the accompanying biographic attributes of a customer are consistent, and therefore whether the IRD number is likely to be correct.

Additionally, this service does not validate that the information provided in the request is correct, simply that Inland Revenue can identify a customer with enough certainty. This is especially pertinent to the NZBN, as Inland Revenue does not have a record of every NZBN, and as such the Companies Office should be consulted to verify an NZBN.

Before you continue, please be sure to consult
http://www.ird.govt.nz/software-providers/
for the products that use this service, business-level context and use cases, links to relevant policy, and information on how to integrate with Inland Revenue's products and services.

1.2 Intended audience

The solution outlined in this document is intended to be used by KiwiSaver scheme providers, employers, financial institutions and accounting/tax management applications.

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. 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 Solution design

2.1 Architecture

Inland Revenue offers a suite of web applications in order to facilitate interactions via software packages. This API will be used by approved organisations to validate customer information with Inland Revenue.

2.2 Supported message type

This service supports the following message type:

- **READ:** Retrieves match from Inland Revenue. Requires an IRD number and other information about the customer.

2.3 IRD validation

2.3.1 Request payload

Field	Description
IRD	Inland Revenue Department ID
Classification	The customer type, either individual or non-individual
Date	The birth date or commencement date of the customer
FormattedName	Name of a non-individual customer or a concatenation of the last and first names of an individual customer. Example: Smith, John Doe
FirstName	First name of an individual customer
MiddleName	Middle name of an individual customer
LastName	Last name of an individual customer
FormattedAddress	The address of the customer as a single string. Example: 123 Easy Street, Te Aro, Wellington 6011
Street	Street of the address
City	City of the address
PostCode	Postcode of the address
State	State of the address
Country	Country of the address in ISO 2A format
NZBN	New Zealand Business Number of a non-individual. This is only used by the validation service if Inland Revenue has a record of an NZBN for the non-individual.

The valid values for 'Classification' are as follows:

Type	Description
COM	Non-individual customer
IND	Individual customer

2.3.2 Response payload

Field	Description
Match	Indicates if a match was found for the information provided

The valid values for 'Match' are as follows:

Type	Description
Match	A match was found for the information provided
No match	A match was **not** found for the information provided

3 End points and OpenAPI specifications

IMPORTANT
For the authoritative definitions, please refer to the OpenAPI specifications at
https://www.ird.govt.nz/software-providers/

3.1 End points

End point	URL
Mock Data Testing	https://test3.services.ird.govt.nz:4046/Gateway/customer/validateIRD
Production Data Testing	https://test4.services.ird.govt.nz:4046/Gateway/customer/validateIRD
Production	https://services.ird.govt.nz:4046/Gateway/customer/validateIRD

NOTE: These endpoints are subject to change due to environment updates in the future.

3.2 OpenAPI specifications

An OpenAPI file describes the entire API, along with endpoints, operations on each endpoint, 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.

4 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.
End points	A term used to describe a web service that has been implemented
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.
IRD	Inland Revenue Department (ie IRD Numbers)
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.
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 key store. The recipient can then use this key to encrypt and sign the messages that they exchange with this counterparty.
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.

5 Change log

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

Version	Date of change	Document section	Description
0.8	05/12/19	1.1	• Clarified purpose of the solution
		1.3	• Added note to table of prerequisites: ○ Note that the same certificate cannot be used for the Test and Production environments.
	01/11/19		• V0.8 created