Inland Revenue
Te Tari Taake

Inland Revenue

Build Pack: Bill API

Date: 30/09/2020

Inland Revenue
Te Tari Taake

Contents

Inland Revenue
Te Tari Taake

1 Overview

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.

1.1 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 to retrieve information for a particular customer bill item. The response also includes provisional tax method details and history associated to the account to which the bill item belongs.

The objective of this API is to allow transaction data services (TDS) software providers to query information that was formerly available in the Tax Agent Web Services (TAWS) data feed.

1.2 Intended audience

The solution outlined in this document is intended to be used by TDS software providers.

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:** 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.

1.3.2 Authentication options

1.3.2.1 OAuth

When using OAuth the interaction with IR 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.

1.3.2.2 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.

Inland Revenue
Te Tari Taake

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.

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 retrieve bill item and provisional tax information from Inland Revenue.

2.2 Supported message type

This service supports the following message type:

- **BILL:** Retrieves bill item information and associated provisional tax method and history from Inland Revenue. Requires a bill ID, which is available in the TDS file as the value of element <billID>.

2.3 Bill item and provisional tax information

2.3.1 Request payload

Field	Description
Id	This refers to the bill ID as it appears in the TDS file (value of element <billID>). Id is the only parameter within the Bill object.

2.3.2 Response payload

Field	Description
Bill ➢CustomerId	Customer ID of customer to whom requested bill item belongs. This ID is the customer's IRD number.
Bill ➢CustomerIdType	**NOTE:** This will only ever be "IRD".
Bill ➢AccountId	Account ID of the account to which requested bill item belongs.
Bill ➢AccountIdType	**NOTE:** This will only ever be "ACC".
Bill ➢Period	End date of the filing period to which requested bill item belongs.
Bill ➢Id	This refers to the bill ID as it appears in the TDS file. This is identical to the value provided in the request payload.
Bill ➢RetrieveDate	Date that the requested bill item information was retrieved.
Bill ➢DueDate	The date that the requested bill item is due

Field	Description
Bill ➢UnderArrangement	Indicates that this bill item is included in an instalment arrangement
ProvMethodHistory[]	Array containing all versions of all provisional methods belonging to the account.
ProvMethodHistory[] ➢MethodKey	Unique identifier for the provisional method. If multiple versions of a particular method exist (ie the method has been updated by either the taxpayer or an Inland Revenue employee), they will be listed from newest to oldest in the array. **NOTE:** A customer may have multiple provisional tax filing methods. This array will contain the history of all of the methods used by this customer, including the one used to generate the requested bill item.
ProvMethodHistory[] ➢Method	Method used. Available options are STD (standard), EST (estimation), RATIO, and AIM.
ProvMethodHistory[] ➢TaxYear	Tax year associated with provisional tax method.
ProvMethodHistory[] ➢Commence	Provisional tax method commencement date.
ProvMethodHistory[] ➢Cease	Provisional tax method cessation date.
ProvMethodHistory[] ➢Amount	Total provisional tax method amount.
ProvMethodHistory[] ➢Ratio	Provisional tax method ratio (applicable to ratio method only).
ProvDetails TransactionId	Unique identifier of provisional tax instalment transaction.
ProvDetails ➢TransactionType	Type of transaction associated with the bill item. Possible values are CNVPRV (Converted provisional tax debit), PRVDBT (Provisional instalment), RTNADR (AIM debit) and RTNACR (AIM credit).
ProvDetails ➢FilingPeriod	Provisional tax method filing period. This date is the last day of the tax year.
ProvDetails ➢DueDate	Provisional tax instalment due date.
ProvDetails ➢Amount	Provisional tax instalment amount due.
ProvDetails ➢FITReduction	Provisional tax instalment FIT reduction.
ProvDetails ➢Method	Provisional tax instalment method that the instalment and bill item were generated for. Available options are STD (standard), EST (estimation), RATIO, and AIM.

Field	Description
ProvDetails ➢Reversed	Provisional tax instalment reversed date.
ProvDetails ➢Processed	Provisional tax instalment processed date.

2.4 Security

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

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

Each HTTPS header contains the authorisation attribute JWT/OAuth:

1. A signed JSON Web Token (JWT) token. This will establish a registered digital services provider identity via the asymmetric public key held in the key store established during onboarding.
2. An OAuth2.0 token that is a customer or intermediary-level XIAMS user account recognised by START.

The Bill API uses an HTTPS transport layer, with HTTP1.1 transport protocol supported.

Regarding transport layer security (TLS), note that while TLS1.3 is now an industry standard, it is not yet widely adopted, as doing so requires upgrades to perimeter security devices and software. Inland Revenue will upgrade to TLS1.3 once it is adopted widely enough, and where practical, external software partners should also anticipate upgrading to this version. TLS1.0 and TLS1.1 are not supported by myIR or Gateway Services.

Asymmetric keys of approved strength must be used. Inland Revenue requires the following ciphers and key strengths to be used:

Encryption:	Advanced Encryption Standard (AES)	FIPS 197	256-bit key
Hashing:	Elliptic Curve Digital Signature Algorithm (ECDSA) using P-256 or Secure Hash Algorithm (SHA-2) NOTE: ECDSA is preferred but RSA will be supported.	FIPS 180-3	SHA-256 (or greater)

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:

```
"Authorization: {JWTAccessToken}"
```

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

	End point for connections
Purpose	• End point to which digital service providers will connect
Client application type	• Cloud applications or in-house servers
Constraints	• Only for source locations with client-side TLS certificates • On the cloud end point Inland Revenue has controls to shield service providers from issues caused by heavy usage from other providers
Mutual TLS	• Inland Revenue explicitly trusts the certificate the service provider associates with the TLS connection as client for Mutual TLS connections and uses it to identify the web service's sending party
Minimum TLS version	• 1.2
URL	• Contains …/gateway/..
Port	• 4046
Web service consumer identification	• Machine-to-machine authentication using client-signed JSON web tokens (JWT) • OAuth2 authorisation using tokens generated by XIAMS
Firewalling in production	• No IP address restrictions • Access limited by certificate enrolment
Firewalling in non-production environments	• No IP address restrictions • Access limited by certificate enrolment

Delegated permissions: The service will allow one to retrieve bill item data for an income tax account to which the calling user (as represented by the JWT or OAuth2 token) has access. If the user does not have access to the income tax account associated with the bill item in the request parameters, an error will be returned.

2.4.1 OAuth

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

HTTP header	Example value
Authorization	Bearer {JWTAccessToken}

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

2.4.2 M2M JWT

Authorisation intended for M2M (machine-to-machine) communication will not use "Bearer " flag on the HTTP header and only contain the JWT.

The JWT will contain a field “startLogon” which can resolve to a myIR logon.

The M2M JWT will be identified by a value of “M2M” in the Key ID (“kid”).

The M2M JWT will be signed with a self-signed certificate, for which the public key was provided during onboarding.

HTTP header	Example value
Authorization	{JWTAccessToken}

Example data structure used for M2M authorisation:

```
Base64Url encoded {
      "alg": <algorithm value>,
      "typ": "JWT",
      "kid": "M2M"
}
.
Base64Url encoded {
      "sub": <token subject>,
      "iss": <issuer value>,
      "startLogon": <myIR_user>,
      "iat": <epoch issued value>,
      "exp": <epoch expired value>
}
.
JWS Signature (
      base64UrlEncode(header) + “.” + base64UrlEncode(payload)
)
```

2.4.2.1 Header

Field	Requirement	Description	Valid values
alg	Required	Signature or encryption algorithm	RS256, RS384, RS512 ES256, ES384, ES512
typ	Required	Type of token	JWT
kid	Required	Key ID	M2M

Inland Revenue
Te Tari Taake

2.4.2.2 Payload

Field	Requirement	Description	Valid values
sub	Required	Subject (to whom the token refers)	SHA-1 Thumbprint/fingerprint of signing certificate
iss	Required	Issuer who created this token	eg CompanyNameA
startLogon	Required	The myIR logon of a representative of the token subject. The subject must be the data owner.	Valid myIR logon
iat	Required	Issued at. The number of seconds since Unix epoch 1 Jan 1970, UTC.	Must not precede the signing certificate issue date Example: 1560144847
exp	Required	Expiration time. The number of seconds since Unix epoch 1 Jan 1970, UTC.	Must not exceed 8 hours from the **iat** (issued at) time value Example: 1574323940

2.4.2.3 startLogon

A myIR logon must be provided in order to use the myIR delegation model for identifying whether bill item information can be retrieved for the provided bill ID. The myIR logon must have access to the income tax account associated with the bill item requested in the payload, otherwise an error will be returned.

Inland Revenue
Te Tari Taake

3 End points and OpenAPI specifications

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 Glossary

Acronym/term	Definition
ACC	A unique account ID that includes an IRD number and an account type code
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.
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.

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 v1.0. It does not encompass non-material changes, such as to formatting etc.

Version	Date of change	Document section	Description
V1.0	30/09/20	1.3.2	New section added – 'Authentication options'
		2.3.2	Added new fields for DueDate and UnderArrangement • YAML file updated
	06/08/20	2.4.2.1	Typo corrected in value values field for 'alg'
		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.
		3	All of section 3 updated with new instructions on where to find current end points and YAML files etc.
	14/04/20	3.1	End points removed and replaced with instruction to instead visit https://www.ird.govt.nz/software-providers/
		2.4	Security section added
	09/03/20		V1.0 released