Inland Revenue
Te Tari Taake

Business Transformation

Inland Revenue

Build pack: Intermediation service

Date: 24/11/2017
Version: v0.5

Contents

1 Overview

1.1 This solution

Inland Revenue has a suite of digital services available for consumption by our service providers that support efficient, electronic business interactions with Inland Revenue. The Intermediation service described in this build pack document forms part of a suite of Gateway Services.

This is a stand-alone document intended to provide the technical details required to support the end-to-end onboarding Gateway Services. It describes the architecture of the technical solution, schemas, endpoints, sample payloads to use in non-production environments, and also its interaction with other build packs that cover different aspects of Gateway Services. The associated onboarding documents (see sections 1.3 and 1.4, below) describe the end-to-end business level solution, of which this build pack forms part.

1.2 Intended audience

The solution outlined in this document is intended to be used by technical teams and development staff. It describes the technical interactions, including responses, provided by the Intermediation service.

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 Supported onboarding packs

Before using this build pack, ensure the relevant onboarding pack has been consulted to provide business-level context. The Inland Revenue onboarding packs listed below are supported by this build pack, all of which are available on Inland Revenue's Gateway Services GitHub site: https://github.com/InlandRevenue/Gateway-Services

These onboarding packs also contain the relevant policy and supporting legislation.

1.3.1 Transaction data services onboarding pack

The Transaction data services (TDS) onboarding pack provides a guide for how consumers can onboard the various TDS components. It gives details of prerequisites, setup requirements, testing, contact lists and more. It is intended to help an organisation start using the TDS solution as quickly and easily as possible.

This document will not be available on the Inland Revenue Gateway Services GitHub website—instead it will be sent to service providers when necessary.

1.4 Related build packs

The following Gateway Services build packs complement this one.

1.4.1 Transaction data services overview and transition build pack

The Transaction data services overview and transition build pack was created to support service providers in their transition from Tax Agent Web Services to the use of TDS. It provides an overview of TDS, describes the data which will be made available through the services and the processes, as well as giving use cases for how these services will be employed.

1.4.2 Identity and access services build pack

The Identity and access (IAS) services build pack describes the operations provided under Identity and access services, which is another part of the Gateway Services suite. These services are used to authenticate access.

1.5 Prerequisites

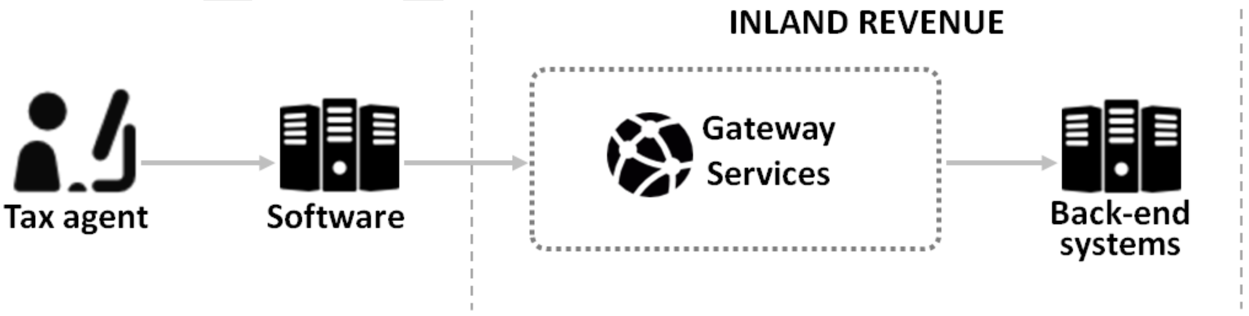
Party	Requirement	Description
Inland Revenue	Provide the Inland Revenue public certificate for mutual TLS	Inland Revenue's public X.509 certificate to support TLS will be provided as part of connectivity testing.
Service provider	Acquire a X.509 certificate from a competent authority for the Test and Production environments	This is required when using mutual TLS with cloud-based service providers.

2 Solution design

2.1 Architecture

Inland Revenue is offering a suite of web services in order to facilitate interactions with Inland Revenue via software packages. The Gateway Services suite will be used by approved software vendors to facilitate everything from registration activities, filing returns, making payments and other service offerings in order to allow customers to interact with Inland Revenue.

The diagram below illustrates the flow of data from the tax agent to Inland Revenue.



The WSDLs for the Gateway Services define an 'any' XML request and response structure, which then relies on a group of XSDs to define the data structure of those requests and responses. Each request and response type will define a lower, 'wrapper' element.

Any malformed XML will instantly be rejected by the Gateway Services prior to any schema validation.

2.2 Service scope

The Intermediation service supports the following operation:

- **RetrieveClientList:** This is used to retrieve a list of a tax agency's clients.

2.3 Messaging

All SOAP messages require a SOAP header containing **Action:** parameters, as well as a SOAP body containing a structured XML payload. Please refer to the WSDL for the correct addresses.

The Gateway Services allow the consumption of any structured XML payload but will be validated against the Inland Revenue -published XSDs.

This is a late binding validation, performed after authentication has been reviewed. The message structure of these services is a simple request/response. The XML request will be checked for well-formed XML before the schema validation. Responses to these requests will be in XML format as well and will be defined in the same schemas that define the requests.

Any XML submissions in the SOAP body that do not meet the provided schemas will not be accepted by the Gateway Services. Incorrect namespaces will also fail validation against the published schemas.

Example SOAP request structure

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
        xmlns:int="https://services.ird.govt.nz/GWS/Intermediation/"
        xmlns:ret=https://services.ird.govt.nz/GWS/Intermediation/:types/RetrieveClientListRequest
        xmlns:a="http://www.w3.org/2005/08/addressing">
    <soap:Header/>
    <soap:Header>
            <a:Action>https://services.ird.govt.nz/GWS/Intermediation/Intermediation/RetrieveClientList</a:Action>
    </soap:Header>
    <soap:Body>
            <int:RetrieveClientList>
                    <int:RetrieveClientListRequestMsg>
                          <ret:RetrieveClientListRequestWrapper>
                                <!-- Intermediation Fields -->
                          </ret:RetrieveClientListRequestWrapper>
                    </int:RetrieveClientListRequestMsg>
            </int:RetrieveClientList>
    </soap:Body>
</soap:Envelope>
```

Example SOAP response structure

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
          xmlns:a="http://www.w3.org/2005/08/addressing">
        <s:Header>

        <a:Actions:mustUnderstand="1">https://services.ird.govt.nz/GWS/Intermediation/Intermediati
on/RetrieveClientListResponse</a:Action>
        </s:Header>
        <s:Body>
                <RetrieveClientListResponse xmlns="https://services.ird.govt.nz/GWS/Intermediation/">
                        <RetrieveClientListResult
xmlns:b="https://services.ird.govt.nz/GWS/Intermediation/:types/RetrieveClientListResponse"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
                                <b:RetrieveClientListResponseWrapper>
                                        <retrieveClientListResponse
xmlns="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
                                                <!-- Response fields -->
                                        </retrieveClientListResponse>
                                </b:RetrieveClientListResponseWrapper>
                        </RetrieveClientListResult>
                </RetrieveClientListResponse>
        </s:Body>
</s:Envelope>
```

2.4 Security

Gateway Services requests are access-controlled using an OAuth token that identifies the user making the request. Users will authenticate using their Inland Revenue myIR credentials. For instructions on how to acquire an OAuth token, review the Identity and access build pack. For TDS Real Time web service requests, an OAuth access token is required in the HTTP header.

Authorisation for using the Gateway Services is defined in the permissions set in myIR. Permissions will reflect those granted in myIR. For example, if a user does not have permission to file a return online, they will not be able to file a return via Gateway Services either. This applies to users who are granted access as staff inside an organisation or as staff in a tax agency.

The Gateway Services use an HTTPS transport layer, with HTTP1.1 transport protocol supported.

The Gateway Services also use the SOAP version 1.2 protocol.

The SOAP service contract is published using WSDL version 1.1.

Transport layer encryption is mandatory and Gateway Services generally use the TLS version 1.2 specification.

Inland Revenue requires the following ciphers and key strengths to be used:

Encryption:	Advanced Encryption Standard (AES)	FIPS 197	256-bit key
Hashing:	Secure Hash Algorithm (SHA-2)	FIPS 180-3	SHA-256

There will be two endpoints, which are summarised in the bullet points below (the table immediately afterwards provides more detail):

1. There is an endpoint to which service providers' centralised **cloud** locations can connect. This will involve mutual TLS certificates that need to be exchanged during the onboarding phase. On the cloud endpoint Inland Revenue has controls to shield service providers from issues caused by heavy usage from other providers.

2. For service providers connecting from **desktops,** there is a separate endpoint that does not use mutual TLS. For this service, certificates do not need to be exchanged during onboarding. On the desktop endpoint Inland Revenue has less ability to shield consumers of the service from heavy usage by others.

	Endpoint for cloud-based connections	**Endpoint for desktop connections**
Purpose	• Primary preferred endpoint to connect to from service providers for Gateway Services.	• Additional transitory endpoint provided to facilitate connecting from desktops which might be high volumes of sources addresses, transient DHCP addresses, not realistically associated with client side TLS certificates, not individually onboarded to setup certificate trust.
Client application type	• Cloud applications.	• Desktop/native applications. • For connecting from multiple decentralised clients.
Constraints	• Only for source locations with client side TLS certificates. • On the cloud endpoint Inland Revenue has controls to shield service providers from issues caused by heavy usage from other providers.	• Less scalable. • Subject to tighter security controls. • On the desktop endpoint Inland Revenue has less ability to shield consumers of the service from heavy usage by others. • OAuth2 refresh tokens will not be offered to desktop clients.
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 service provider in conjunction with the web service identification below.	• Server side certificates only.

	Endpoint for cloud-based connections	Endpoint for desktop connections
Minimum TLS version	• 1.2	• 1.0(+)
URL	• Contains …/gateway/..	• Contains …/gateway2/..
Port	• 4046	• 443 (Default https port)
Web service consumer identification	• To be identified in web service calls—each cloud application will be given client_id/client_secret credentials during onboarding to allow it to call this endpoint.	• Desktop clients will be given different client_id/client_secret credentials to cloud application clients.
Firewalling in production	• No IP address restrictions. • Access limited by certificate enrolment.	• No IP address restrictions.
Firewalling in non-production environments	• No IP address restrictions. • Access limited by certificate enrolment.	• Firewalled—IP whitelisting needed.

Delegated permissions: The services will allow one to retrieve all of the data for a customer that the calling user (as represented by the OAuth token) has access to. There may be additional accounts this identity does not have access to, those will not be mentioned. If an account or data in it is targeted by the request parameters but the user does not have permission an error will be returned. This access will depend on delegation permissions set up in myIR. If the token represents a user in a tax agency or other intermediary, then the agent-client linking is also considered.

3 Operations

IMPORTANT: *The schemas listed here are subject to change. For the authoritative definitions, please refer to the information provided on the Inland Revenue Gateway Services GitHub site—* https://github.com/InlandRevenue/Gateway-Services

The structures of all Gateway Service operations are intended to produce the most efficient requests and responses. Any common structures and fields will be used across many schemas and tax types through an intentional inheritance method. The section below describes the structure of each operation and the scenarios in which certain fields will be used in XML requests and responses.

This section contains schema aliases:

- Cmn: Common.xsd
- Int: Intermediation.xsd

All requests and responses live in the Intermediation.xsd.

All operations for the Intermediation service will contain two standard header fields: **softwareProviderData** and **identifier**.

For example:

```
<cmn:softwareProviderData>
        <cmn:softwareProvider>SoftwareProvider</cmn:softwareProvider>
        <cmn:softwarePlatform>SoftwarePlatform</cmn:softwarePlatform>
        <cmn:softwareRelease>v1</cmn:softwareRelease>
</cmn:softwareProviderData>
<cmn:identifier IdentifierValueType="IRD">012345678</cmn:identifier>
```

Field	Description
softwareProvider	The company that developed the software
softwarePlatform	The software package that is making the request
softwareRelease	The version of the software package
IdentifierValueType	The ID type being submitted—can be IRD and NZBN. The value submitted for this field should contain only digits, with no dashes.

Proper use:

- The only softwareProviderData fields users will be able to input are the ones that were provided to Inland Revenue at the time of on-boarding.
- The identifier is that of the tax agency on whose behalf the operations are being performed.

Example scenario:

- Tax agency with IRD 898989898 submits a retrieveClientList operation
    - Tax agent calls /Intermediation/RetrieveClientList/ with <cmn:identifier IdentifierValueType="IRD">898989898</cmn:identifier>

3.1 RetrieveClientList

The RetrieveClientList operation will be used to retrieve all of a tax agency’s clients. There is an option to retrieve all of a tax agency’s clients of a given account type.

3.1.1 Request

```
<int:retrieveClientListRequest
       xmlns:int="urn:www.ird.govt.nz/GWS:types/Intermediation.v1"
       xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v1">
           <cmn:softwareProviderData>
                     <cmn:softwareProvider>…</cmn:softwareProvider>
                     <cmn:softwarePlatform>…</cmn:softwarePlatform>
                     <cmn:softwareRelease>…</cmn:softwareRelease>
           </cmn:softwareProviderData>
           <cmn:identifier IdentifierValueType= "IRD"></cmn:identifier>
           <int:retrieveClientListBody>
                     <int:accountType>GST</int:accountType>
           </int:retrieveClientListBody>
</int:retrieveClientListRequest>
```

Field	Required	Description
accountType	Optional	Account type—used to limit the resulting account types to only this specified account type.

3.1.2 Response

```
<clientList>
          <client>
                    <clientIRD>…</clientIRD>
                    <clientAccountType>…</clientAccountType>
          </client>
          <client>
                    <clientIRD>…</clientIRD>
                    <clientAccountType>…</clientAccountType>
          </client>
</clientList>
```

Field	Required	Description
clientIRD	Required	Client’s account IRD number
clientAccountType	Required	Client’s account type.

4 End points, schemas and WSDLs

IMPORTANT: *The end points, schemas and WSDLs listed here are subject to change. For the authoritative definitions, please refer to the information provided on the Inland Revenue Gateway Services GitHub site:* https://github.com/InlandRevenue/Gateway-Services

4.1 End points

The end points for the Digital Test Environment XZT (Sliced data):

Service	Environment	URL
Authentication	Cloud	https://q.services.ird.govt.nz
	Desktop/native app	https://q.services.ird.govt.nz
Gateway Services	Cloud	https://xzt.services.ird.govt.nz:4046/gateway/gws/intermediation/
	Desktop/native app	https://xzt.services.ird.govt.nz/gateway2/gws/intermediation/

The end points for the Digital Test Environment XZS (Unsliced data):

Service	Environment	URL
Authentication	Cloud/desktop/native apps	https://q.services.ird.govt.nz
Gateway Services	Cloud	https://xzs.services.ird.govt.nz:4046/gateway/gws/intermediation/
	Desktop/native app	https://xzs.services.ird.govt.nz/gateway2/gws/intermediation/

The end points for Production are as follows:

Service	Environment	URL
Authentication	Cloud/desktop/native apps	https://services.ird.govt.nz:443
Gateway Services	Cloud	https://services.ird.govt.nz:4046/gateway/gws/intermediation/
	Desktop/native app	https://services.ird.govt.nz/gateway2/gws/intermediation/

4.2 Schemas

All schemas for the Intermediation service import a common.xsd which has some data types specific to Inland Revenue. This common.xsd will be used in other gateway services outside of the /Intermediation/ namespace so it must be kept up-to-date, without numerous redundant versions remaining.

The Intermediation.xsd imports the Common.xsd and creates data types to be used within the operations. It also includes the request and response root elements for the supported operations.

4.3 WSDLs

The Intermediation Gateway Service has one WSDL, which has a target namespace of https://services.ird.govt.nz/GWS/Intermediation/ and can be found at

https://services.ird.govt.nz/GWS/Intermediation/?singleWsdl.

All WSDL messages follow this naming convention:

```
Return_<operation>_InputMessage or Return_<operation>_OutputMessage.

<wsdl:portType name="Intermediation">
          <wsdl:operation name="RetrieveClientList">
<wsdl:service name="Intermediation">
```

5 Responses

The response message from the Gateway Services always includes a status code and status message that describes how successfully the gateway service call was carried out. Following the status message will be the responseBody, which will return the operations response.

5.1 Generic gateway response codes

The following response codes are common to all gateway service calls:

Standard codes	Standard message	Description
-1	An unknown error has occurred	This error will be logged by the Gateway Services and evaluated the next business day.
0	Success	This resembles a successful web service call.
1	Authentication failure	Authentication failure means the token provided is not a valid token.
2	Missing authentication token(s)	No OAuth token in HTTP header.
3	Unauthorised access	The logon making the call does not have access to make the request on behalf of the client or agency.
5	Unauthorised vendor	The vendor provided is not authorised to use these suite of services.
20	Unrecognised XML request	The XML submitted is not recognisable and no schema can be determined.
21	XML request failed validation	The XML structure did not meet the definition laid out by the schemas published by Inland Revenue.

5.2 Generic intermediation response codes

The following response codes are specific to intermediation gateway service calls:

Standard codes	Standard message	Description
100	Invalid request data	Could not extract data from xml payload
101	The provided IRD number is not a tax agency	
102	This agency IRD has no linked accounts	
103	This agency IRD has no linked accounts with the given account type	

6 Processing flows

6.1 Generic use cases

This section will convey how Inland Revenue intends the Gateway Services to be used. These are base cases and Inland Revenue recognises that these services can be used in many different ways to satisfy business needs.

Additional information on use cases is available in the Transaction data services onboarding pack.

6.1.1 RetrieveClientList

Scenario 1:

1) The user representing the intermediary wishes to retrieve a list of all clients linked to that intermediary.
2) The user invokes the ‘RetrieveClientList’ operation to attempt to retrieve a list of clients that belong to the intermediary.
3) Upon receipt of the request, the intermediation services will ensure the requestor has permission to make the request on behalf of the intermediary.
4) After validation the client list will be returned.

7 Appendix A—Glossary

Acronym/term	Definition
ACC, ACCID	Accident Compensation Corporation (and ID number)
Activity statement	Formally known as the Statement of Activity—the name for the data that is filed for AIM.
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.
Endpoints	A term used to describe a web service that has been implemented.
ESCT	Employer Superannuation Contribution Tax—one of the many deductions that come from payroll.
FIPS	Federal Information Processing Standard—a suite of IT standards from the US Federal Government.
Gateway	Inland Revenue's web services gateway.
GWS	Gateway Services—the brand name for the suite of web services that Inland Revenue is providing. The Intermediation service is a Gateway Service.
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.
IAS	Identity and access service.
IP	Internet Protocol—the principal communication protocol in the Internet protocol suite for relaying datagrams across networks.
NZBN	New Zealand Business Number.
NZISM	NZ Information Security Manual—the security standards and best practices for Government agencies. Maintained by the NZ Government Communications Security Bureau (GCSB).
OAuth	An HTTPS based protocol for authorising access to a resource, currently at version 2.
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 (such as a GST return) must/can contain, as well as validating the payload.
SHA	Secure Hashing Algorithm. There is a family of them that provide different strengths. Secure Hashing Algorithm 2 (SHA-2) is currently favoured over SHA-1, which has been compromised.
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

Acronym/term	Definition
	website.
START	Simplified Taxation and Revenue Technology— Inland Revenue's new core tax processing application. It is an implementation of the GenTax product from FAST Enterprises.
Statement of Activity	See Activity Statement
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.
WSDL	Web Service Definition Language—an XML definition of a web service interface.
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 X509 certificate to which it is bound tells us whose key it is, who issued it, when it expires etc. When we receive a counterparties' X509 digital certificate we take their public key out of it and store the key in our keystore. We can then use this key to encrypt and sign the messages that we exchange with this counterparty.
XIAMS	External Identity and Access Management System (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. Physically it is a set of discrete hardware and software products, plug-ins and protocols.
XML	Extensible Mark-up Language—a language used to define a set of rules used for encoding documents in a format that can be read by humans and machines.
XSD	XML Schema Definition—the current standard schema language for all XML data and documents.

8 Appendix B—Change log

This table lists all changes that have been made to this build pack document since version 0.5 was created.

Version	Date of change	Document section	Description
0.5	24/11/2017	All	Draft created
	27/11/2017	4.1 End points	URLs updated