Inland Revenue

Build Pack: Notifications Service

Date:	4/10/2019
Version:	v0.8

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. The Notifications Service described in this build pack document enables actionable event notifications to be retrieved by external software platforms.

Notifications are very lean. They are delivered to software rather than people. It is the responsibility of the software to prioritise, filter and decide when and how to respond to each notification using the data within it. The data in the notification is sufficient for this purpose and nothing more—for example, it may identify that an address or a filing frequency has changed, but it does not contain the newly-changed address or the new filing frequency.

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 payroll providers, tax practitioners, Kiwi Saver providers, banks and other financial institutions (referred to throughout the remainder of this document as 'Digital Service 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.

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:

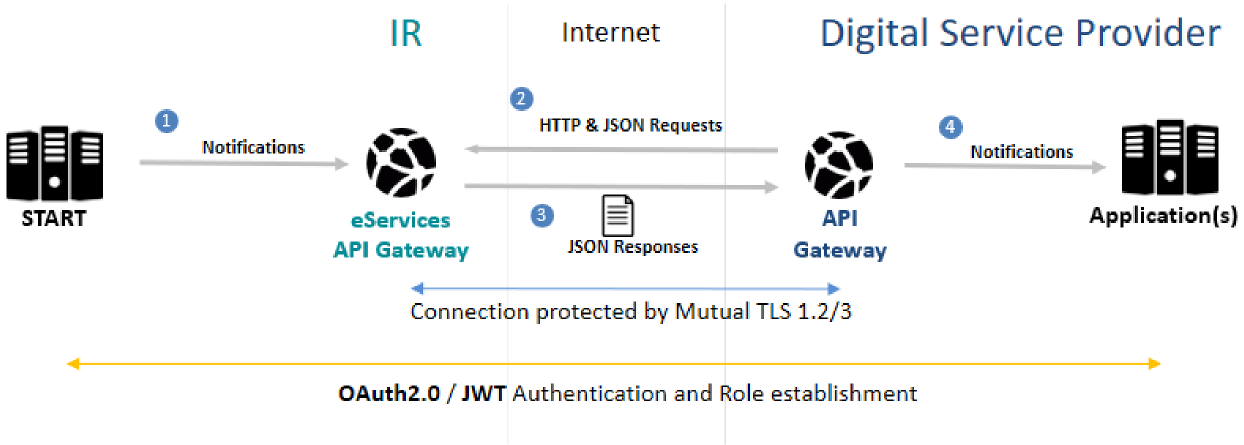
- Comodo
- GeoTrust
- DigiCert
- GlobalSign
- Symantec
- Thawte
- IdenTrust
- Entrust
- Network Solutions
- RapidSSL
- Entrust Datacard
- GoDaddy.

2 Solution design

2.1 Architecture

Inland Revenue 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 notifications from Inland Revenue.

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



1. START makes read only Notifications available to the eServices API Gateway.

2. Trading Partners call the IR Notifications API to request notifications. The signed JWT, OAuth2.0 token and request object optional date range and result focusing ID are used to determine the scope of notifications available to the calling party.

3. eServices API Gateway responds with the full set of JSON notification objects that meet the criteria (2 above)

4. Notifications are consumed/read by the digital service providers application and potentially propagated out to the providers internal and external users and customers – the tenants of their software application.

2.2 Supported message type

This service supports the following message type:

- **READ:** Retrieve notifications from Inland Revenue. Requires a 'from' date (with optional query ID), query ID type and a 'to' date.

2.3 Notifications

2.3.1 Request payload

Field	Description
QueryIDType	A set of ID types used to filter notifications
QueryID	The value of the above type
FromDateTime	The earliest point in time from which notifications can be selected based on their date-time stamp
ToDateTime	The latest point in time up to which notifications can be selected based on their date-time stamp. May be useful as a form of pagination.

A list of the valid values for **QueryIDType** is as follows:

Type	Description	
CLTLID	Non tax agent client list identifier	Multiple recipients
CST	A non-IRD Number type identifier	Single recipient
IRD	Inland Revenue Department ID	Single recipient
KSF	KiwiSaver Scheme ID	Single recipient
LSTID	Tax agent client list identifier	Multiple recipients

Note: **QueryID** and **QueryIDType** are to be used for filtering notifications, either down to a specific recipient or a set of recipients, depending on the **QueryIDType**. For both **CLTLID** and **LSTID**, notifications are returned for linked clients on the given client list. To return notifications for other combinations of multiple recipients, **QueryID** and **QueryIDType** should be omitted and **FromDateTime** should be used to limit the notifications returned.

2.3.2 Record ID

Field	Description
NotificationKey	Unique notification identifier
RecordCreated	Point in time the notification object was created
EventDate	Date time corresponding to event that created this notification.
Category	Notification category
SubCategory	Notification sub-category
Type	Notification type
Description	A description of the notification
DocumentID	An identifier of a document that can be retrieved through the document service
DocumentLocationID	An identifier that is used to properly route a document submitted through the document service

Field	Description
ExtID	An external ID for providing more information with a notification
ExtIDType	The type of ExtID, if one is provided
IDType	An ID type for the customer to whom the notification corresponds
ID	The ID for the customer to whom the notification corresponds
SubjectIDType	The ID type of the subject of the notification, if applicable.
SubjectID	The ID of the subject of the notification, if applicable. If the notification pertains to a second customer, such as an employee of an employer or a member of a KiwiSaver scheme.
FilingPeriod	The end of the filing period to which the notification corresponds, if applicable
DueDate	A due date corresponding to the notification, if applicable

2.3.3 Notification limit

Due to the potentially high number of notifications for a recipient, there is a limit to the number of notifications that will be returned, and an error will be returned if the number of notifications exceeds this. If this is the case, the notifications need to be filtered with FromDateTime and a combination of **ToDateTime** and a **QueryID**/**QueryIDType** pair.

2.4 Security

The API will use and require a unique identifier to be provided to establish the calling party identity and authentication required by the access model. 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 the other 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 Notification Service uses an HTTPS transport layer, with HTTP1.1 transport protocol supported.

Transport Layer Encryption is mandatory, using the TLS version 1.2 specification.

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	FIPS 180-3	SHA-256 (or greater)

	Secure Hash Algorithm (SHA-2) NOTE: ECDSA is preferred but RSA will be supported.		

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 machine-to-machine connections
Purpose	• End point for digital service providers to connect to.
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 services will allow one to retrieve all of the notification data for a customer or group of customers to which the calling user (as represented by the JWT or OAuth2 token) has access. There may be additional accounts this identity does not have access to, but those will not be mentioned. If an account or data within it is targeted by the request parameters but the user does not have permission, 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, RS512
typ	Required	Type of token	JWT
kid	Required	Key ID	M2M

2.4.2.2 Payload

Field	Requirement	Description	Valid Values
sub	Required	Subject (to whom the token refers)	Thumbprint/fingerprint of signing certificate
iss	Required	Issuer who created this token	eg CompanyNameA

Field	Requirement	Description	Valid Values
startLogon	Required	The myIR logon of a representative of the token subject. The subject must be the data owner.	Valid myIR logon, or null
iat	Required	Issued at	Must not precede the signing certificate issue date. Example: 1560144847
exp	Required	Expiration time	Must not exceed 8 hours from the **iat** (issued at) time value

2.4.2.3 startLogon

A myIR logon can be provided in order to use the myIR delegation model for identifying customers for whom notifications should be retrieved. If the myIR logon is provided, then notifications will only be shown for customers the logon can access. If a myIR logon is not used, the field should be included with a value of null, and the subject will determine the notifications shown.

2.4.2.4 sub

A subject must be provided, which is the thumbprint of the signing certificate, and can be used to determine which notifications should be retrieved. The subject will always be used to validate the signature of the JWT but will only be used for determining which notifications to retrieve when value for **startLogon** is not provided. The subject can be used for access in two distinct situations, when the subject is a KiwiSaver scheme provider, or when the subject is a tax preparer. If the subject is a KiwiSaver scheme provider, notifications will be returned for the current members of the scheme. If the subject is a tax preparer, notifications will be returned for customers currently linked to the tax preparer.

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/notifications/list
Production Data Testing	https://test4.services.ird.govt.nz:4046/Gateway/notifications/list
Production	https://services.ird.govt.nz:4046/Gateway/notifications/list

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

3.2 OpenAPI specifications

An OpenAPI file allows you to describe your entire API, 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.
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.
SOAP	Simple Object Access Protocol—a set of standards for specifying web services. GWS uses SOAP version 1.2

Acronym/term	Definition
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.

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
	21/10/19	2.4.1, 2.4.2	• Updated spelling of 'Authorisation' to 'Authorization' to match industry standard
0.8	04/10/19		• V0.8 created