Inland Revenue
Te Tari Taake

Inland Revenue

Build Pack: Document Service

Date: 29/03/2022

Inland Revenue
Te Tari Taake

Contents

Inland Revenue
Te Tari Taake

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 Document Service described in this build pack document enables documents to be retrieved by external software platforms as well as be submitted by external software platforms.

Documents can comprise of mail generated by Inland Revenue for communicating with customers, as well as documents request by Inland Revenue from a customer, and documents a customer voluntarily provides to Inland Revenue. Documents from Inland Revenue are PDFs, while documents provided to Inland Revenue can be of many different file formats.

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 payroll providers, tax practitioners, KiwiSaver 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 terms and abbreviations are used throughout this document.

1.3 Related services

The following application programming interfaces (APIs) complement this Gateway Service. Instructions on where to find the build packs for these APIs can be found in section 3 of this document.

1.3.1 Identity and Access Services (required)

The Identity and Access Services (IAS) are used to authenticate access. Authentication tokens will need to be retrieved via IAS prior to making calls to this API.

Inland Revenue
Te Tari Taake

1.3.2 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.

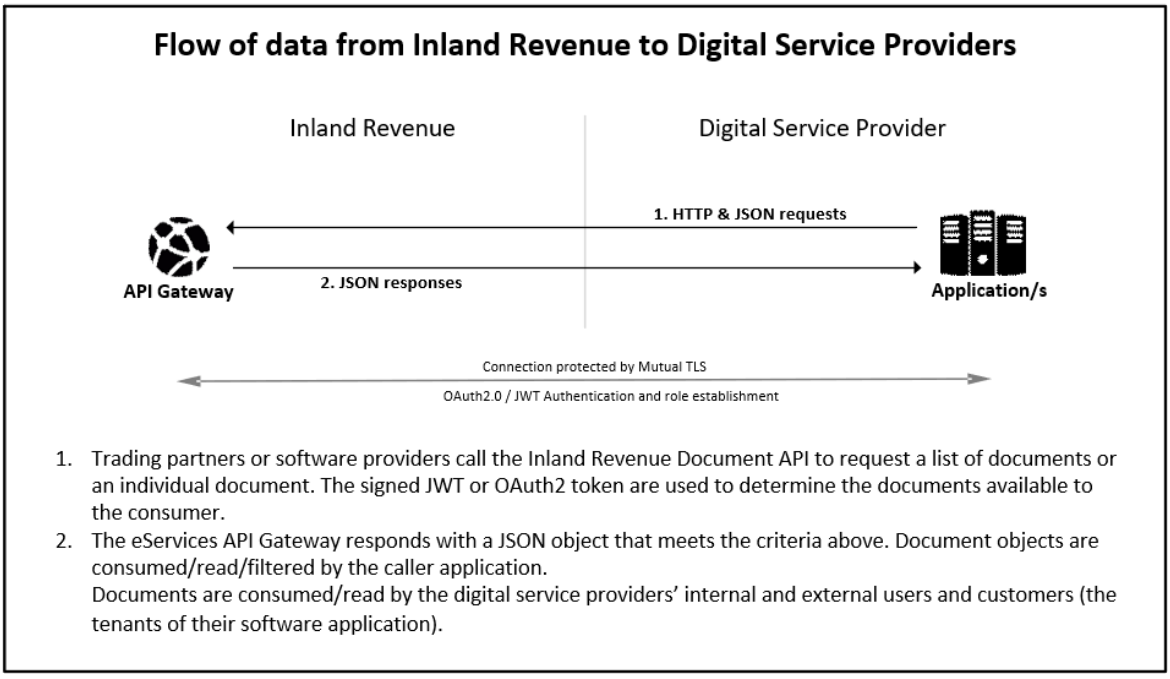
These factors tend to limit the use JWT to larger corporations and public sector organisations. It is not suitable for cloud-based applications as it requires all application users to have their own digital certificates—this is administratively burdensome and requires these users to lodge their private keys with their application provider, which is insecure.

2 Solution design

2.1 Architecture

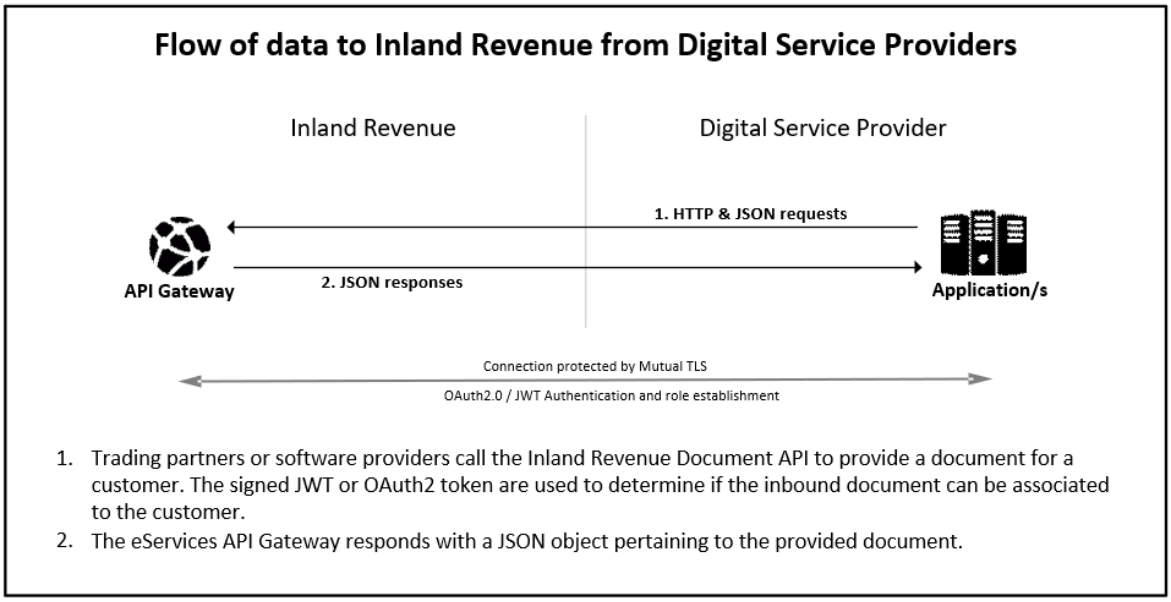
Inland Revenue is offering a suite of web applications in order to facilitate interactions via software packages. This API will be used by approved organisations to interact with the Inland Revenue document service.

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



1. Trading partners or software providers call the Inland Revenue Document API to request a list of documents or an individual document. The signed JWT or OAuth2 token are used to determine the documents available to the consumer.
2. The eServices API Gateway responds with a JSON object that meets the criteria above. Document objects are consumed/read/filtered by the caller application.
   Documents are consumed/read by the digital service providers' internal and external users and customers (the tenants of their software application).

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



1. Trading partners or software providers call the Inland Revenue Document API to provide a document for a customer. The signed JWT or OAuth2 token are used to determine if the inbound document can be associated to the customer.
2. The eServices API Gateway responds with a JSON object pertaining to the provided document.

2.2 Messaging

This service supports the following message types:

- **READ:** Retrieve a list of document identifiers from Inland Revenue. Requires either an IRD number or a return submission key.
- **READ/{documentID}:** Retrieve a single document from Inland Revenue. Requires a document identifier.
- **CREATE:** Submit a single document to Inland Revenue. Requires either a document location identifier or a return submission key.
- **UPDATE:** Inform Inland Revenue that a previously-submitted document is invalid. Requires a document identifier.

2.3 Document list

These are used by the consumer to either retrieve a list of documents associated with an IRD number (for example, letters generated by Inland Revenue and visible on myIR), or a list of documents linked to a return.

Note, certain types of letters generated by Inland Revenue must be posted and are not visible on myIR or through the Document Service.

2.3.1 Request payload

Field	Description
IRDNumber	IRD number of the customer for which the document list should be retrieved. If provided, only documents generated by Inland Revenue will be returned.
ExtID	Reference to a START object to which documents can be linked. If provided, only documents submitted through the Document Service will be returned.
ExtIDType	Enumerates the area in START where the documents referenced by ExtID is organised
FromDateTime	The earliest point in time up to which documents can be selected based on their date-time stamp—may be useful as a form of pagination. This date must not be before 1753-01-01.
ToDateTime	The latest point in time up to which documents can be selected based on their date-time stamp—may be useful as a form of pagination. This date must not be before 1753-01-01.

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

Type	Description
RTNSUB	The submission key of a return submitted through the Returns Service

2.3.2 Response payload

Field	Description
DocumentID	An identifier of a document that can be retrieved through the document service
DateTimeCreated	Date the document was created or submitted
MailType	Internal identifier of a letter type, if applicable
Description	A description of the document or the title of a letter
AccountType	Account type associated with the document, if applicable
AccountID	Identifier of the account associated with the document, if applicable
FilingPeriod	The end of the filing period to which the document corresponds, if applicable
Redirected	Indicates if the mail item was redirected, if applicable
FileName	The file name of the document, if applicable
DocumentCategory	The category of the document provided upon submission, if applicable

2.4 Document Retrieve

This is used by the consumer to retrieve a specific document identified by including the unique DocumentID as a query parameter.

Documents generated by Inland Revenue will always contain a MailType value and will not have a FileName. Instead, these documents will always have a file extension of .pdf.

2.4.1 Request parameters

Field	Description
DocumentID	An identifier of a document that can be retrieved through the document service. **NOTE:** The DocumentID is required to be provided and have a value that is greater than zero.

2.4.2 Response payload

Field	Description
DocumentID	An identifier of a document that can be retrieved through the document service
DateTimeCreated	Date the document was created or submitted
MailType	Internal identifier of a letter type. This is only applicable to documents generated by Inland Revenue.
Description	A description of the document or the title of a letter
AccountType	Account type associated with the document, if applicable

Field	Description
AccountID	Identifier of the account associated with the document, if applicable
FilingPeriod	The end of the filing period to which the document corresponds, if applicable
FileName	The file name of the document. This is only applicable to documents submitted through the Document Service.
DocumentCategory	The category of the document provided upon submission, if applicable
Document	A base64 encoded string containing the byte array of the document

2.5 Document Create

Used by the consumer to submit a new document to Inland Revenue, either as a result of receiving a request from Inland Revenue via a notification or to link to a previously filed return.

The maximum file size of a document submitted through the Create service is 9,000,000 bytes before Base64 encoding.

Multiple documents can be submitted for a given DocumentLocationID or ExtID/ExtIDType. When possible, a DocumentLocationID should be used, as this may enable certain automated actions to be performed and may speed up the processing of the document.

Note: The DocumentID returned by this operation must be stored, as documents submitted with a DocumentLocationID will not be displayed in the Document List operation.

Note: If a document is submitted for a return, the status of the return must not be 'Submitted'.

2.5.1 Request payload

Field	Description
DocumentLocationID	An identifier that is used to properly route a document submitted through the document service
ExtID	Reference to a START object to which documents can be linked.
ExtIDType	Enumerates the area in START where the documents referenced by ExtID is organised
DocumentCategory	The category of the document provided upon submission, if applicable
Description	A description of the document
FileName	The file name of the document, including the file extension

Field	Description
Document	A base64 encoded string containing the byte array of the document

File extension must be one of the following: gif, jpg, jpeg, pdf, png, csv, doc, docx, xls, xlsx, ppt, pps, pptx, ppsx, odt, ods, odp.

2.5.2 Response payload

Field	Description
DocumentID	An identifier of a document that can be retrieved through the Document Service

2.6 Document Update

This is used by the consumer to mark a previously supplied document as submitted in error. The document is identified by including the unique DocumentID as a query parameter.

2.6.1 Request parameters

Field	Description
DocumentID	An identifier of a document that can be retrieved through the Document Service

2.6.2 Request payload

Field	Description
Reason	Text description of the reason for marking a previously supplied document as submitted in error

2.6.3 Response payload

No response payload will be returned. The successful HTTP response (200/202) will be treated as acknowledgment of success.

Inland Revenue
Te Tari Taake

2.7 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.

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 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 access or provide documents for a customer 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.

2.7.1 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.

2.7.2 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)
)
```

2.7.2.1 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

2.7.2.2 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, or null
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 eight hours from the **iat** (issued at) time value. Example: 1574323940

2.7.2.3 startLogon

A myIR logon can be provided in order to use the myIR delegation model for identifying customers for whom documents can be accessed. If the myIR logon is provided, then documents will only be shown and accepted 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 documents shown and allowed to access.

2.7.2.4 sub

A subject must be provided, which is the thumbprint of the signing certificate, and can be used to determine which documents can be accessed.

The subject will always be used to validate the signature of the JWT but will only be used for determining which documents to access 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, documents can be provided and accessed for the current members of the scheme.
- If the subject is a tax preparer, documents can be provided and access for customers currently linked to the tax preparer.

Inland Revenue
Te Tari Taake

3 Additional development resources

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 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.

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 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.

Date of change	Document section	Description
29/03/22	N/A	• YAML updated to include COVID-19 Support Payments (CSP) account type - account level mail for CSP will be available through this service
10/05/21	1.3	• 'Related services' section added
	2.2	• Section heading changed to 'Messaging'
	2.2.1	• Section heading changed 'Notification retrieve'

	2.3	• Entire 'Security' section reorganised
		  ○ 'Information classification' section added
		  ○ 'Transport layer security and certificates' section updated
		  ○ 'Ciphers' section added
		• 'Authentication options' section updated

		•
	1.3	• 'Prerequisites' section removed • 'Related services' section added
	3.2	• 'End points and OpenAPI specifications' section renamed 'Additional development resources'
		• Glossary removed
10/05/21	2.4.1	• Added note to DocumentID that value must be greater than zero
	N/A	• YAML updated to include RSP account type
17/02/21	N/A	• YAML updated
27/11/20	2.4	• Removed extraneous "either"
10/11/20	2.3.1	• Clarified dates cannot be before 1753-01-01
29/09/20	1.3.2	• New section added – 'Authentication options'
08/17/20	2.5	• Added a note clarifying what the status of a return may not be in to be used for submitting a document
08/09/20	2.3, 2.4, 2.5	• Updated the descriptions of these operations and their request fields to clarify how the operations should be used
06/08/20	2.7.2.1	• Typo corrected in value values field for 'alg'
	1.1	• Updated URL in boxed text

Inland Revenue
Te Tari Taake

Date of change	Document section	Description
	3	• Entire section updated with new information on where to find end points and OpenAPI specs
06/04/20		• V1.0 released