

Inland Revenue

Build pack: Intermediation Service

Date: 26/02/2019
Version: v2.03

Contents

1 Overview.....	4
1.1 This solution	4
1.2 Intended audience.....	4
1.3 Related build packs	4
1.3.1 Identity and Access Services Build Pack	4
1.4 Prerequisites.....	5
1.4.1 Mutual Transport Layer Security and certificates	5
2 Solution design	6
2.1 Architecture.....	6
2.2 Service scope	6
2.3 Messaging	7
2.4 Security	8
3 Operations	11
3.1 RetrieveClientList	12
3.1.1 Request	12
3.1.2 Response	13
3.2 Link.....	14
3.2.1 Request	14
3.2.2 Response	15
3.3 Delink.....	16
3.3.1 Request	16
3.3.2 Response	17
3.4 RetrieveClient	18
3.4.1 Request	18
3.4.2 Response	19
3.5 Update.....	20
3.5.1 Request	20
3.5.2 Response	21
4 End points, schemas and WSDLs.....	22
4.1 End points.....	22
4.2 Schemas	22
4.3 WSDLs.....	22
5 Responses.....	24
5.1 Generic Gateway response codes	24
5.2 Generic Intermediation response codes	26
6 Glossary.....	27
7 Expected values	30

7.1	Client list ID types.....	30
7.2	Client list type	30
7.3	Access levels	30
8	Change log.....	31

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 Intermediation Service described in this build pack document forms part of a suite of Gateway Services.

Intermediation is the process of linking an intermediary (such as a tax agent) to an individual or organisation so the intermediary can act on their behalf for tax purposes. This Intermediation Gateway Service provides the ability for intermediaries to manage links to clients as well as provides the ability to retrieve client lists already established in myIR.

This build pack document is intended to provide the technical information required to support the end-to-end onboarding of the Intermediation Service. It describes the architecture of the technical solution, schemas, end points, sample payloads to use in non-production environments, and also its interaction with other build packs that cover different aspects of Gateway Services.

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 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 understand 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 of this document.

1.3 Related build packs

The following Gateway Services build packs complement this one and can be found at Inland Revenue's Gateway Services GitHub site: <https://github.com/InlandRevenue/Gateway-Services>.

1.3.1 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.

1.4 Prerequisites

Party	Requirement	Description
Service provider	Acquire a X.509 certificate from a certificate authority for the Test and Production environments	This is required when using mutual TLS with cloud-based service providers

1.4.1 Mutual Transport Layer Security and certificates

Mutual Transport Layer Security (TLS) is implemented for the Intermediation Service. 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:

1. Minimum Key Length: 2048
2. Signature Algorithm: SHA256[RSA]
3. Self-signed certificates are not accepted
4. 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.

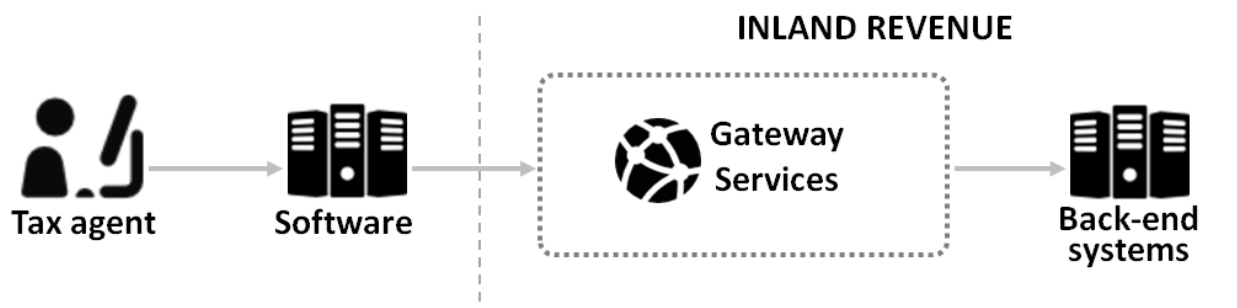
- [Comodo](#)
- [GeoTrust](#)
- [DigiCert](#)
- [GlobalSign](#)
- [Symantec](#)
- [Thawte](#)
- [IdenTrust](#)
- [Entrust](#)
- [Network Solutions](#)
- [RapidSSL](#)
- [Entrust Datacard](#)
- [GoDaddy](#).

2 Solution design

2.1 Architecture

Inland Revenue is offering a suite of web services in order to facilitate interactions via software packages. The Gateway Services suite will be used by approved software providers 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 operations:

- **RetrieveClientList:** This operation is used to retrieve client lists belonging to a tax agency as well as the clients in each list.
- **Link:** This operation is used to link an intermediary to a client or an intermediary's client list to a client account.
- **Delink:** This operation is used to delink a client from an intermediary or a client account from a intermediary's client list.
- **RetrieveClient:** This operation is used to retrieve the link attributes between an intermediary and client or client accounts.
- **Update:** This operation is used to update an existing intermediary to client relationship. This can also be used to switch clients between client lists.

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 ([section 4.3](#) of this document) for the correct addresses.

The online 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. To simplify analysis and code generation, a development-oriented version of the WSDL and XSDs is provided with the build pack that has the 'any' elements replaced with relevant types.

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
  xmlns:int1="https://services.ird.govt.nz/GWS/Intermediation/"
  xmlns:int2="urn:www.ird.govt.nz/GWS/types/Intermediation.v1"
  xmlns:b=https://services.ird.govt.nz/GWS/Intermediation:/types/RetrieveClientListResponse
  xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
  <s:Header>
    <a:Actions:mustUnderstand="1">
      https://services.ird.govt.nz/GWS/Intermediation/Intermediation/RetrieveClientList
    </a:Action>
  </s:Header>
  <s:Body>
    <int1:RetrieveClientListResponse>
      <int1:RetrieveClientListResult>
        <b:RetrieveClientListResponseWrapper>
          <int:retrieveClientListResponse >
            <!-- Response fields -->
          </int:retrieveClientListResponse>
        </b:RetrieveClientListResponseWrapper>
      </int1:RetrieveClientListResult>
    </int1: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 Services 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 end points, which are summarised in the bullet points below (the table immediately afterwards provides more detail):

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

	End point for cloud-based connections	End point for desktop connections
Purpose	<ul style="list-style-type: none"> This is the default end point to connect software providers to the Gateway Services 	<ul style="list-style-type: none"> Additional end point provided to facilitate connecting from desktops which may have 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	<ul style="list-style-type: none"> Cloud applications 	<ul style="list-style-type: none"> Desktop/native applications For connecting from multiple decentralised clients
Constraints	<ul style="list-style-type: none"> Only for source locations with client-side TLS certificates On the cloud end point Inland Revenue has controls to shield software providers from issues caused by heavy usage from other providers 	<ul style="list-style-type: none"> Less scalable Subject to tighter security controls On the desktop end point 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	<ul style="list-style-type: none"> Inland Revenue explicitly trusts the certificate the software provider uses as client for Mutual TLS connections and uses it to identify the software provider in conjunction with the web service identification below 	<ul style="list-style-type: none"> Server-side certificates only
Minimum TLS version	<ul style="list-style-type: none"> 1.2 	<ul style="list-style-type: none"> 1.0(+)

	End point for cloud-based connections	End point for desktop connections
URL	<ul style="list-style-type: none"> Contains ../gateway/.. 	<ul style="list-style-type: none"> Contains ../gateway2/..
Port	<ul style="list-style-type: none"> 4046 	<ul style="list-style-type: none"> 443 (Default https port)
Web service consumer identification	<ul style="list-style-type: none"> Each software provider is given a software platform ID during onboarding. This ID type is "Customer ID" and is independent of the end point To be identified in web service calls each cloud application will be given identity and access system client_id/client_secret credentials during onboarding to allow it to get OAuth tokens to call this end point The mutual TLS certificate is used to identify the service provider 	<ul style="list-style-type: none"> Each software provider is given a software platform ID during onboarding. This ID type is "Customer ID" and is not specific to the end point Desktop clients will be given different identity and access system client_id/client_secret credentials to cloud application clients
Firewalling in production	<ul style="list-style-type: none"> No IP address restrictions Access limited by certificate enrolment 	<ul style="list-style-type: none"> No IP address restrictions
Firewalling in non-production environments	<ul style="list-style-type: none"> No IP address restrictions Access limited by certificate enrolment 	<ul style="list-style-type: none"> Firewalled—IP whitelisting required

Delegated permissions: The services will allow the retrieval of all of the data for a customer to whom the calling user (as represented by the OAuth token) has access. There may be additional accounts to which this identity does not have access—those will not be mentioned. An error will be returned if an account is targeted by the requestor but the user does not have permission. This access will depend on the 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 end points, schemas and WSDLs listed here are subject to change.
For the authoritative definitions, please visit
<https://www.ird.govt.nz/software-providers/>

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 these schema aliases:

- Cmn: Common.v2.xsd
- Int: Intermediation.v1.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**.

The **identifier** field is common across all Gateway Services but refers to different parties in different services. In all cases it is the party with delegated permissions to whom an OAuth token is provided. If the value cannot be resolved to a known context, or if it can but the provided OAuth token does not have the necessary delegated permissions, then the error code 4 "unauthorised delegation" is returned. Please refer to individual operations for the nature of the identifier expected in this parameter in any given context.

For example:

```
<cmn:softwareProviderData>
  <cmn:softwareProvider>SoftwareProvider</cmn:softwareProvider>
  <cmn:softwarePlatform>SoftwarePlatform</cmn:softwarePlatform>
  <cmn:softwareRelease>v2</cmn:softwareRelease>
</cmn:softwareProviderData>
<cmn:identifier IdentifierValueType="IRD">012345678</cmn:identifier>
```

Field	Description
softwareProvider	The company that developed the software
softwarePlatform	The field value will be provided by Inland Revenue during the onboarding process
softwareRelease	The version of the software package
IdentifierValueType	The ID type being submitted—most cases will be IRD
identifier	The value submitted for this field should contain only digits, with no dashes. IRD numbers that are eight digits must be padded with a leading zero.

Field	Description
accountType	NOT USED. No intermediation links will originate from an intermediary account. This field will be omitted from all below examples.

Proper use:

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

Example scenario:

- Tax agency with IRD 898989898 wants to retrieve a client list
 - Tax agent with access to agency calls /Intermediation/RetrieveClientList/ with <cmn:identifier IdentifierValueType="IRD">898989898</cmn:identifier>

3.1 RetrieveClientList

The RetrieveClientList operation will be used to retrieve all or some of a tax agency's clients. There is also an option to retrieve all of a tax agency's clients of a given account type. For those who are not registered as either a tax agent, bookkeeper or payroll intermediary, this operation will also provide a client's status.

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.v2">
  <cmn:softwareProviderData>
    <cmn:softwareProvider>...</cmn:softwareProvider>
    <cmn:softwarePlatform>...</cmn:softwarePlatform>
    <cmn:softwareRelease>...</cmn:softwareRelease>
  </cmn:softwareProviderData>
  <cmn:identifier IdentifierValueType= "IRD">123123123</cmn:identifier>
  <!--Optional-->
  <int:filterAccountType>FBT</int:filterAccountType>
  <!--Optional-->
  <int:filterClientListID>123154150</int:filterClientListID>
</int:retrieveClientListRequest>
```

Field	Required	Description
filterAccountType	Optional	This is used to limit the resulting accounts to only this specified account type.
filterClientListID	Optional	This filter will be used to only retrieve one client list. This can be used in conjunction with filterAccountType.

NOTE: The IRD number submitted in the identifier field will **ALWAYS** be that of the tax agency and NOT that of the client list. If a single client list is desired be sure to use the filterClientListID field.

3.1.2 Response

```
<agency agencyID="123154150" agencyIDType="IRD">
  <clientList clientListId="123154150" clientListIdType="CLTLID" clientListType="TAXCLI"
    hasRefundAccount="false">
    <client>
      <clientIRD>123154134</clientIRD>
      <clientAccountType>GST</clientAccountType>
    </client>
    <client status="Approved">
      <clientIRD>123154126</clientIRD>
      <clientAccountType>FBT</clientAccountType>
    </client>
  </clientList>
  <clientList clientListId="1231544" clientListIdType="CLTID" clientListType="BKPCLI"
    hasRefundAccount="true">
    <client>
      <clientIRD>123163915</clientIRD>
      <clientAccountType>GST</clientAccountType>
    </client>
  </clientList>
</agency>
```

Field	Required	Description
agencyID	Required	This attribute of the <agency> tag will display the ID of the agency
clientListId	Required	This attribute of the <clientList> tag will display the ID of the client list
clientListIdType	Required	This attribute will show the client list ID type. For expected values see section 7.1 .
clientListType	Required	This attribute is used to distinguish the type of client list being returned. This is useful for intermediaries that work in multiple capacities (Tax Agent and Bookkeeper) and have different client lists for the different roles. For expected values see section 7.2 .
hasRefundAccount	Required	This attribute will be used to state whether or not the client list has an refund account on it.
clientIRD	Required	This field is the client's IRD number.
clientAccountType	Optional	This field is the client account. If the link associated to this client list is a customer master link, then this field will not be provided.
status	Optional	This field is for bookkeepers, payroll bureaus, and other representatives. If a link to a client has been requested but not approved yet, this attribute will be supplied as TRUE.

3.2 Link

The Link operation will be used to establish a relationship between an intermediary and a client. There are two different uses for this operation—linking to an account and declaring as the customer master of the client. To link to a client as the customer master a link to a client account must be made prior to making the customer master link call.

3.2.1 Request

```
<int:linkRequest
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:int="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:softwareProviderData>
    <cmn:softwareProvider>...</cmn:softwareProvider>
    <cmn:softwarePlatform>...</cmn:softwarePlatform>
    <cmn:softwareRelease>...</cmn:softwareRelease>
  </cmn:softwareProviderData>
  <cmn:identifier IdentifierValueType="IRD">11111111</cmn:identifier>
  <int:clientListID IdentifierValueType="LSTID">3213211</int:clientListID>
  <int:target>
    <int:clientID IdentifierValueType="ACCIRD">123123123</int:clientID>
    <int:clientAccountType>GST</int:clientAccountType>
  </int:target>
  <int:redirectMail>true</int:redirectMail>
  <int:redirectDisbursements>false</int:redirectDisbursements>
  <int:updateCustomerMaster>false</int:updateCustomerMaster>
</int:linkRequest>
```

Field	Required	Description
clientListID	Required	This is the identifier for the client list. The identifier value types expected here can be found in section 7.1 .
clientID	Required	This is the identifier for the client. The expected value for the identifier value type here is ACCIRD unless the link request is for a customer master, then the expected value is IRD.
clientAccountType	Optional	This field is the client account. If the link request is for a customer master link, then this field should not be provided.
redirectMail	Optional	This field is used to set the redirect mail flag. If this field is not supplied the default value will be false.
redirectDisbursements	Optional	This field is used to set the redirect disbursements flag on a link. This can only be done on account links and not for customer master links. Redirect disbursements can only be used if a refund account has been setup on the source client list.
updateCustomerMaster	Required	This field is to designate whether the requested link is to establish customer master or not. This action is only accessible to tax agents and should always be false for all other intermediaries.

NOTE: The IRD number submitted in the identifier field will **ALWAYS** be that of the tax agency and NOT that of the client list.

3.2.2 Response

```
<int:linkResponse
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:int="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:statusMessage>
    <cmn:statusCode>0</cmn:statusCode>
    <cmn:errorMessage> </cmn:errorMessage>
    <cmn:errorDescription> </cmn:errorDescription>
  </cmn:statusMessage>
  <int:clientListID IdentifierValueType="CLTLID">1234567</int:clientListID>
  <int:clientID status="true">
    <int:clientID IdentifierValueType="ACCIRD">123123123</int:clientID>
    <int:clientAccountType>GST</int:clientAccountType>
  </int:clientID>
</int:linkResponse>
```

Field	Required	Description
clientListID	Required	This field is the identifier for the client list. The identifier value types expected here can be found in section 7.1
clientID	Required	This field is the identifier for the client that was linked to.
clientAccountType	Optional	This field is the account that was linked. This field will not be provided if the link request was to establish a customer master.
status	Optional	This field is for bookkeepers, payroll bureaus, and other representatives. If a link to a client has been requested but not approved yet, this attribute will be supplied as TRUE.

3.3 Delink

The Delink operation will be used to cease a relationship between an intermediary and a client. There are two different uses for this operation—delinking from an account and removing the intermediary as the customer master for the client.

3.3.1 Request

```
<n1:delinkRequest
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:n1="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:softwareProviderData>
    <cmn:softwareProvider>...</cmn:softwareProvider>
    <cmn:softwarePlatform>...</cmn:softwarePlatform>
    <cmn:softwareRelease>...</cmn:softwareRelease>
  </cmn:softwareProviderData>
  <cmn:identifier IdentifierValueType="IRD">11111111</cmn:identifier>
  <n1:clientListID IdentifierValueType="LSTID">123123123</n1:clientListID>
  <n1:target>
    <n1:clientID IdentifierValueType="ACCIRD">123321123</n1:clientID>
    <n1:clientAccountType>GST</n1:clientAccountType>
  </n1:target>
  <n1:updateCustomerMaster>>false</n1:updateCustomerMaster>
</n1:delinkRequest>
```

Field	Required	Description
clientListID	Required	This is the identifier for the client list. The identifier value types expected here can be found in section 7.1 .
clientID	Required	This is the identifier for the client. The expected value for the identifier value type here is ACCIRD unless the delink request is for a customer master—then the expected value is IRD.
clientAccountType	Optional	This field is the client account. If the delink request is for a customer master link, then this field should not be provided.
updateCustomerMaster	Required	This field is to designate whether the request is to remove customer master. This action is only accessible to tax agents and should always be false for all other intermediaries.

NOTE: The IRD number submitted in the identifier field will **ALWAYS** be that of the tax agency and NOT that of the client list.

3.3.2 Response

```
<n1:delinkResponse
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:n1="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:statusMessage>
    <cmn:statusCode>0</cmn:statusCode>
    <cmn:errorMessage> </cmn:errorMessage>
    <cmn:errorDescription> </cmn:errorDescription>
  </cmn:statusMessage>
  <n1:clientListID IdentifierValueType="IRD">123123123</n1:clientListID>
  <n1:target>
    <n1:clientID IdentifierValueType="ACCIRD">123321123</n1:clientID>
    <n1:clientAccountType>GST</n1:clientAccountType>
  </n1:target>
</n1:delinkResponse>
```

Field	Required	Description
clientListID	Required	This field is the identifier for the client list. The identifier value types expected here can be found in section 7.1
clientID	Required	This field is the identifier for the client that was linked to.
clientAccountType	Optional	This field is the account that was linked. This field will not be provided if the link request was to establish a customer master.

Note: All values returned here should match the values submitted in the request.

3.4 RetrieveClient

The RetrieveClient operation will be used to retrieve the attributes of a client relationship. If there are multiple links for the designated client and a client account type is not provided then all links will be retrieved.

3.4.1 Request

```
<n1:retrieveClientRequest
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:n1="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:statusMessage>
    <cmn:statusCode>0</cmn:statusCode>
    <cmn:errorMessage> </cmn:errorMessage>
    <cmn:errorDescription> </cmn:errorDescription>
  </cmn:statusMessage>
  <cmn:identifier IdentifierValueType="IRD">123123123</cmn:identifier>
  <n1:client>
    <n1:clientID IdentifierValueType="ACCIRD">111111111</n1:clientID>
    <n1:clientAccountType>GST</n1:clientAccountType>
  </n1:client>
</n1:retrieveClientRequest>
```

```
<n1:retrieveClientRequest
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:n1="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:statusMessage>
    <cmn:statusCode>0</cmn:statusCode>
    <cmn:errorMessage> </cmn:errorMessage>
    <cmn:errorDescription> </cmn:errorDescription>
  </cmn:statusMessage>
  <cmn:identifier IdentifierValueType="IRD">123123123</cmn:identifier>
  <n1:client>
    <n1:clientID IdentifierValueType="IRD">111111111</n1:clientID>
  </n1:client>
</n1:retrieveClientRequest>
```

Field	Required	Description
clientID	Required	This field is the identifier for the client that is linked to.
clientAccountType	Optional	This field is to narrow a request down to a particular linked account. If this field is not provided then all links to this client will be returned.

NOTE: The IRD number submitted in the identifier field will **ALWAYS** be that of the tax agency and NOT that of the client list.

3.4.2 Response

```
<n1:retrieveClientResponse xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
xmlns:n1="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:statusMessage>
    <cmn:statusCode>0</cmn:statusCode>
    <cmn:errorMessage> </cmn:errorMessage>
    <cmn:errorDescription> </cmn:errorDescription>
  </cmn:statusMessage>
  <n1:clientID IdentifierValueType="IRD">132123123</n1:clientID>
  <n1:link clientAccount="IPS">
    <n1:clientListID IdentifierValueType="LSTID">1231231</n1:clientListID>
    <n1:redirectMail>false</n1:redirectMail>
    <n1:redirectDisbursements>true</n1:redirectDisbursements>
  </n1:link>
  <n1:link clientAccount="GST">
    <n1:clientListID IdentifierValueType="IRD">111111111</n1:clientListID>
    <n1:redirectMail>true</n1:redirectMail>
    <n1:redirectDisbursements>true</n1:redirectDisbursements>
  </n1:link>
  <n1:link customerMaster="true">
    <n1:clientListID IdentifierValueType="IRD">111111111</n1:clientListID>
    <n1:redirectMail>true</n1:redirectMail>
  </n1:link>
</n1:retrieveClientResponse>
```

Field	Required	Description
clientID	Required	This field is the identifier for the client that is linked to.
clientAccount	Optional	This attribute will display the account type of the client link. This attribute will only be displayed if it is an account level link.
clientListID	Required	This field is the identifier for the client list. The identifier value types expected here can be found in section 7.1 .
redirectMail	Required	This field shows the current redirect mail flag set on the given link.
redirectDisbursements	Optional	This field shows the current redirect disbursements flag set on the given link. This will not be returned if it is a customer master link.
customerMaster	Optional	This attribute designates that the link is a customer level link establishing a customer master relationship. This will not be returned if the link is an account level link.

3.5 Update

The Update operation will be used to update an existing relationship between an intermediary and a client. Most fields in this request are optional and should be supplied if those fields are intended to be updated. If the desired outcome of the update is to change the source of the client link from one client list to another then ALL optional fields need to be provided or else defaults will be assigned and the existing link attributes will not be preserved.

3.5.1 Request

```
<n1:updateRequest
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:n1="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
    <cmn:statusCode>0</cmn:statusCode>
    <cmn:errorMessage> </cmn:errorMessage>
    <cmn:errorDescription> </cmn:errorDescription>
  </cmn:statusMessage>
  <cmn:identifier IdentifierValueType="IRD">123123123</cmn:identifier>
  <n1:clientListID IdentifierValueType="IRD">123123123</n1:clientListID>
  <n1:target>
    <n1:clientID IdentifierValueType="ACCIRD">123321123</n1:clientID>
    <n1:clientAccountType>GST</n1:clientAccountType>
  </n1:target>
  <n1:redirectMail>true</n1:redirectMail>
  <n1:redirectDisbursements>true</n1:redirectDisbursements>
  <n1:updateCustomerMaster>true</n1:updateCustomerMaster>
  <n1:newClientListID IdentifierValueType="LSTID">1234567</n1:newClientListID>
</n1:updateRequest>
```

Field	Required	Description
clientListID	Required	This field is the identifier for the client list. The identifier value types expected here can be found in section 7.1 .
clientID	Required	This field is the identifier for the client that is being updated.
clientAccountType	Optional	This field is the account that is currently linked. This field will not be provided if the link request is to update a customer master.
redirectMail	Optional	This field is used to update the redirect mail flag. If the update request is not intended to change this field then this field should not be submitted.
redirectDisbursements	Optional	This field is used to set the redirect disbursements flag on a link. This can only be done on account links and not for customer master links. Redirect disbursements can only be used if a refund account has been setup on the source client list.
updateCustomerMaster	Required	This field is to designate whether the requested update is for a customer master link or not. This action is only accessible to tax agents and should always be false for all other intermediaries.
newClientListID	Optional	This field is used to change the source of the client link from one client list to another. If this action is

Field	Required	Description
		performed then all optional fields above should be supplied. Attributes of the existing link will not be preserved on the move from one list to another. If the new client list does not have proper settings (eg no refund account for redirect disbursements or different list type [see section 7.2]) then an error message will be returned.

NOTE: The IRD number submitted in the identifier field will **ALWAYS** be that of the tax agency and NOT that of the client list.

3.5.2 Response

```
<n1:updateResponse
  xmlns:cmn="urn:www.ird.govt.nz/GWS:types/Common.v2"
  xmlns:n1="urn:www.ird.govt.nz/GWS:types/Intermediation.v1">
  <cmn:statusMessage>
    <cmn:statusCode>0</cmn:statusCode>
    <cmn:errorMessage> </cmn:errorMessage>
    <cmn:errorDescription> </cmn:errorDescription>
  </cmn:statusMessage>
</n1:updateResponse>
```

Notes: The update response will only reply with a status response with a 0 success or an error code. We strongly recommend that the retrieveClient operation is used before the update call to ensure the correct link fields are being updated.

4 End points, schemas and WSDLs

IMPORTANT

The end points, schemas and WSDLs listed here are subject to change.
For the authoritative definitions, please visit
<https://www.ird.govt.nz/software-providers/>

4.1 End points

Onboarding instructions are available at <https://www.ird.govt.nz/software-providers/>.

4.2 Schemas

All schemas for the Intermediation service import a common.v2.xsd which has some data types specific to Inland Revenue. This common.v2.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 creates data types to be used within the RetrieveClientList operation. It also includes the request and response root elements for the supported operation.

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:4046/gateway/GWS/Intermediation/?singleWsdL>.

Note: The production URL above will not work until you have onboarded with Inland Revenue.

As explained in the '[Solution design](#)' section of this document, the online WSDLs have 'any' elements underneath the wrapper elements. There is a development version of the WSDL available with this build pack that replaces the 'any' element with an imported reference to the schema to facilitate initial development and testing. To consume the actual service, the binding will need to be done at the hosted end point. However, for initial development this static WSDL can be used.

All WSDL messages follow this naming convention:

Intermediation_<operation>_InputMessage or Intermediation_<operation>_OutputMessage

```
<wsdl:portType name="Intermediation">
  <wsdl:operation name="RetrieveClientList">
    <wsdl:operation name="Link">
      <wsdl:operation name="Delink">
        <wsdl:operation name="RetrieveClient">
          <wsdl:operation name="Update">
<wsdl:service name="Intermediation">
```

A development version of the WSDL is provided with this build pack. For easier WSDL consumption, the <xs:any> structure has been replaced with a reference to the corresponding element in the Intermediation.xsd. This will allow any tools that consume the WSDL to automatically pull in the data structures from the XSD. To use this, ensure the WSDL provided by Inland Revenue is in the same directory as Common.xsd, ReturnCommon.xsd and Intermediation.xsd.

Note: The WSDL hosted at the end point above will not contain these XSD references, only the static WSDL provided at <https://www.ird.govt.nz/software-providers/>.

5 Responses

The response message from the Gateway Services will always include a status code and status message. These values will describe any successes or failures of a web service call. Following the status message will be the response data for the given operation.

5.1 Generic Gateway response codes

The following response codes are common to all Gateway Service calls. This service applies framework security validation as follows, and the descriptions in the table below reflect that:

Standard codes	Standard message	Description	Customer level validation
-1	An unknown error has occurred	This is generally what will be returned for internal errors that are not due to the service request	Y
0	(Success)	Standard success code is 0	Y
1	Authentication failure	General authentication failure status. Could be the result of inability to validate security token.	Y
2	Missing authentication token(s)	Tokens were not included in the HTTP header as expected	Y
3	Unauthorised access	Access is not permitted for the requester to use the gateway services. Access could not be confirmed due to the failure of OAuth token validation. This could be due to invalid format of the token or infrastructure being unavailable.	Y
4	Unauthorised delegation	<p>Access is not permitted for the requester to perform this operation for the submitted identifier. This code will be returned in any of these situations:</p> <ul style="list-style-type: none"> The submitted cmn:identifier has an invalid value. The identifier type (IdentifierValueType attribute on cmn:identifier) supplied is invalid. All the values above are valid but the provided OAuth token does not have delegated access to that customer or account. <p>This service operation will NOT return</p>	Y

Standard codes	Standard message	Description	Customer level validation
		this code if the filterAccountType supplied does not exist for that identifier, or the OAuth token does not have access for that specific account.	
5	Unauthorised vendor	The vendor code provided does not permit access—has not been onboarded for this operation	Y
6	Authentication Expired	Token authentication has expired and needs to be refreshed. Note this will only be provided for a token that has been successfully used before. For an expired unused token response 3 above will be returned.	Y
(7)	(Account Type not supported)	Please note this service operation, unlike some other services, will never return the 7 response code for unsupported account types. An invalid or unsupported filterAccountType value might result in a 103 code as per the table below.	N/A
20	Unrecognised XML request	This could be due to the external sender sending in incorrect XML or it could be due to bad/poor/missing configuration	Y
21	XML request failed validation	The external requestor submitted XML that is not formatted according to our defined schemas.	Y
(none)	(non xml)	In some scenarios where the request message does not have a well formed XML structure or is not valid or does not adhere to the SOAP protocol formats, the framework generates a parsing exception that is not wrapped in XML nor has a response status code.	Y
(none)	(SOAP fault) UnAuthorised	When maximum concurrency has been exceeded by the service provider this SOAP fault will be returned	Y

5.2 Generic Intermediation response codes

The following response codes are specific to Intermediation Gateway Service calls:

Standard codes	Standard message	Description
100	Could not extract data from XML payload	Could not extract data from XML payload
101	Tax agency IRD is not valid	The provided IRD number does not belong to a tax agency
102	No client lists available for agent	The requesting agent has not been delegated access to any client lists
103	No client found for requested parameters	There are no client accounts for the request parameters provided
104	No tax preparer indicator	The intermediary attempting to link does not have the proper preparer indicator
105	Invalid client list	The client list details provided do not resolve to a valid client list
106	Client list doesn't allow refunds	The intended client list doesn't have a refund account to redirect disbursements
107	No existing customer master link	There is no customer master link to update
108	Insufficient client list access	The client list supplied is valid
109	Cannot redirect refunds on customer master	Customer master links do not allow the redirecting of refunds
110	Customer master requests cannot include client accounts	A client account cannot be provided when creating a customer master link
111	Account link must exist before customer master link	A customer master link cannot be created until a link to a client's account exists
112	New client list must be of the same client list type	The new client list must be of the same client list type
113	A customer master link already exists between this tax agent and client	A link already exists to the customer provided
114	Only tax agents can establish customer master links	Only tax agents can create a link to the customer master
115	A link to the client account already exists	A link already exists to the client's provided account
116	Tax preparer cannot redirect mail	The tax preparer cannot redirect the client's mail
117	Tax preparer cannot redirect refunds	The tax preparer cannot redirect the client's refunds
118	Invalid account type for intermediary link	Intermediaries cannot link to the specified account type

6 Glossary

Acronym/term	Definition
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
Build Pack	Details the technical requirements and specifications, processes and sample payloads for the specified activity
Client	As used in this build pack client generally refers to the party licensing and using the software intermediary/software provider's software
Credentials	Information used to authenticate identity, for instance an account username and password.
Customer	<p>A Customer is the party who is a tax payer or a participant in the social policy products that are operated by Inland Revenue. The Customer might be a person (an "individual") or a non-individual entity such as a company, trust, society etc.</p> <p>Practically all of the service interactions with Inland Revenue are about a Customer (eg their returns, accounts, entitlements etc) even though these interactions might be undertaken by an Intermediary such as a tax agent on their behalf.</p>
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state. [RFC 2828]
End points	A term used to describe a web service that has been implemented.
GWS	Gateway Services—the brand name for the suite of web services that Inland Revenue is providing. The Software 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.
IP	Internet Protocol—the principal communication protocol in the Internet protocol suite for relaying datagrams across networks
NZISM	NZ Information Security Manual—the security standards and best practices for Government agencies. Maintained by the NZ Government Communications Security Bureau (GCSB).
OAuth 2.0	OAuth 2.0 is an industry-standard protocol for authorisation
Pattern	A constraint on data type values that require the string literal used in the data type's lexical space to match a specific pattern
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.

Acronym/term	Definition
Schemas	An XML schema defines the syntax of an XML document, in particular of a payload. The schema specifies what a valid payload must/can contain, as well as validating the payload.
SHA	Secure Hashing Algorithm. There is a family of these that provide different strengths. SHA-2 is currently favoured over SHA-1, which has been compromised.
Software provider	The organisation developing the software connecting to Inland Revenue gateway services (also known as software intermediary, software developer or service provider)
Software provider software	<p>A client application is an operating instance of software that is deployed in one or more sites. A number of deployment patterns are possible:</p> <ol style="list-style-type: none"> 1. A single cloud based instance with multiple tenants and online users, 2. An on premise instance (such as an organisation's payroll system) 3. A desktop application with an online user. <p>This is the computer software that contains interfaces to consume the services that Inland Revenue exposes. Software is developed and maintained by a software developer and subsequently deployed as one or more client applications.</p>
SFTP	Secure File Transport Protocol. SFTP 3.0 is used.
Solution	The technology components, systems and interface specifications constituting the Tax Agent Web Services capability which enables integration and communication across the gateway channel between Inland Revenue and tax agents for the purpose of providing the service
SOAP	Simple Object Access Protocol—a set of standards for specifying web services. Gateway Services 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 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.
Tax agent	A tax agent who is formally registered as such with Inland Revenue
TDS	Transaction Data Services
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
User	The user referred to in this document is the user of the software provider accounting or tax package. This user needs delegated permissions on customer tax accounts (potentially via a tax agency or other intermediary) in order to use TDS. The web logon used in

Acronym/term	Definition
	eServices needs to be used in making Inland Revenue queries. This web logon must be granted permission there to access customer accounts.
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 identifies whose key it is, who issued it, when it expires etc. When a counterparty's X509 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.
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

7 Expected values

7.1 Client list ID types

List ID type	ID description	Available for tax agents	Available for payroll intermediaries	Available for payroll bureaus	Available for bookkeepers	Available for others
CLTLID	Client List Identifier	No	No	Yes	Yes	Yes
LSTID	List Identifier	Yes	Yes	No	No	No
IRD	IRD Number	Yes	Yes	No	No	No

7.2 Client list type

List type	List description
TAXCLI	Tax Agent Client List
BKPCLI	Bookkeeper Client List
PRBCLI	Payroll Bureau Client List
PAYCLI	Payroll Intermediary Client List
OTHCLI	Other Representative Client List

7.3 Access levels

Access level	Access description
FILE	File access allows the filing of returns on behalf of the client for any linked accounts.
NONE	File and pay access allows filings and payments on behalf of the client for any linked accounts.
VIEW	View access allows the viewing of all tax attributes, statuses and obligations on the linked client accounts.
FULL	Full access allows the filing, payment and viewing of all account information and obligations on behalf of the linked client.

NOTE: Web logons with the access level of 'restricted user' do not have access to any of the functions through the Intermediation Service.

8 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
2.03	26/02/19	3	<p>Description of softwarePlatform in table removed: <i>"The software package that is making the request"</i>.</p> <p>Replaced with new description: <i>"The field value will be provided by Inland Revenue during the onboarding process."</i></p>
V2.02	18/02/19	5.2	Added error codes 113-118
		7.1	Added 'Available for others' column to table
		7.3	Note added to bottom of table
		3.1	Opening paragraph amended to include reference to client status
		3.1.2, 3.2.2	Payloads changed – 'pendingApproval' changed to 'status'
		All response payloads	References to 'accessLevel' removed from all response payloads
V2.01	08/02/19	3.2, 3.4, 3.5	Removed all references to access type field
		3.1	Update operation description
		3.2	Update operation description
		5.18	Added error codes 105, 107-115
V2.0	18/01/19	1.3	<ul style="list-style-type: none"> Section on 'Transaction Data Services Overview and Transition Build Pack' removed from 'Related build packs' section
	16/01/19	1.1	<ul style="list-style-type: none"> Updated
		2.2	<ul style="list-style-type: none"> Updated
		3.1	<ul style="list-style-type: none"> Updated
		3.2	<ul style="list-style-type: none"> 'Delink' section added
		3.3	<ul style="list-style-type: none"> 'RetrieveClient' section added
		3.4	<ul style="list-style-type: none"> 'Update' section added
		4.1, 4.2, 4.3	<ul style="list-style-type: none"> End points, Schemas, WSDLs sections updated
		5	<ul style="list-style-type: none"> Responses updated
		7	<ul style="list-style-type: none"> Added "Expected Values" section
Version numbers removed henceforth	03/12/18	(formerly section 6)	<ul style="list-style-type: none"> REMOVED: Section on use cases and scenarios. Readers are instead advised to visit https://www.ird.govt.nz/software-providers/

Version	Date of change	Document section	Description
			for such information
		Table of contents	<ul style="list-style-type: none"> Removed 'List of tables' and 'List of figures'
		Entire document	<ul style="list-style-type: none"> Removed all 'table' and 'figure' captions
		1.1	<ul style="list-style-type: none"> Removed <i>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.</i>
		1.1	<ul style="list-style-type: none"> REMOVED: The associated onboarding and overview documents describe the end-to-end business level solution, of which this build pack forms part. Development versions of schemas, and sample requests and responses are also available with this build pack. ADDED: 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.
		(Formerly section 1.3)	<ul style="list-style-type: none"> Removed section 1.3 'Supported onboarding packs'
		1.4	<ul style="list-style-type: none"> Removed row from prerequisites table on Inland Revenue: INLAND REVENUE: <i>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.</i>
		3 4	<ul style="list-style-type: none"> Removed: IMPORTANT: <i>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</i> Replaced with: IMPORTANT The end points, schemas and WSDLs listed here are subject to change. For the authoritative definitions, please visit https://www.ird.govt.nz/software-providers/
1.01	19/11/20	1.5.1	<ul style="list-style-type: none"> Added section 1.5.1 to cover mutual TLS

Version	Date of change	Document section	Description
	18		security and certificates
		7 Glossary and 8 Change log	<ul style="list-style-type: none"> Removed word 'Appendix' from both headings
1.0	13/04/2018	2.4 Security	<ul style="list-style-type: none"> Reworded delegation note at end of section
		Entire document	<ul style="list-style-type: none"> Cosmetic/formatting changes
0.82	06/03/2018	Entire document	<ul style="list-style-type: none"> Cosmetic/formatting changes
0.81	23/02/2018	5.1 Generic gateway response codes	<ul style="list-style-type: none"> Expanded some generic error code descriptions, and added others
		Glossary	<ul style="list-style-type: none"> Replaced glossary
		Table of contents	<ul style="list-style-type: none"> Added figure and table captions and indexes
0.8	31/01/2018	2 Solution design	<ul style="list-style-type: none"> Updated definitions and XML formatting
		3 Operations	<ul style="list-style-type: none"> Updated operation information and formatting
		5 Responses	<ul style="list-style-type: none"> Updated response structures and attributes
	27/11/2017	2.4 Security	<ul style="list-style-type: none"> Updated information
	27/11/2017	4.1 End points	<ul style="list-style-type: none"> URLs updated
0.5	24/11/2017	All	<ul style="list-style-type: none"> Draft created