

ID Pass API Documentation

Secure identity verification service for Australian KYC checks

Generated 8 September 2026

Table of Contents

API Documentation

Idpass

API Documentation

ID Pass Overview

ID Pass is a secure, configurable identity verification service for Australian KYC checks.

You create a one-time verification link, your customer completes a guided online check, and you retrieve a clear pass/fail result plus the verified identity details.

This guide explains how ID Pass works, what your customers will experience, and how to integrate it at a high level.

- For full field-by-field definitions, see the [ID Pass API Reference](#).
- For a customer journey walkthrough, see the [ID Pass User Journey](#).

Document verification strategies

ID Pass supports three document verification strategies, selected via the `document_verification` parameter when creating an ID Pass:

- **DVS** (default) - Full verification of Australian documents via the Australian Document Verification Service (DVS), with the DVS result codes and details returned to you. A New Zealand Driver Licence under this strategy is verified with the New Zealand licence issuer instead, and its result is returned in the same shape.
- **IDSP** - Document verification is performed by Global Data on your behalf. An **identity opinion** (valid / not valid) is returned; DVS result codes and details are not returned in the API response.
- **Basic** - Format and checksum validation only. No formal document verification is performed.

See the dedicated section for each mode below for requirements, behaviour, and what the API returns.

DVS mode

In `dvs` mode (the default), each Australian identity document is verified directly against the Australian Document Verification Service (DVS). The full DVS result - including the result code and any mismatch detail - is returned to you on the response. The one exception is the New Zealand Driver Licence, which is verified with the New Zealand licence issuer rather than DVS; its result is returned in the same shape (see [New Zealand Driver Licence](#)).

This is the right mode for most KYC use cases where you want full visibility into the DVS outcome.

Requirements

- A DVS Identity (OAC) on your account for live environments. Registration is a free process available for Australian businesses - contact your Global Data account manager to register for the DVS.
- No DVS Identity is required in sandbox.

What is verified

Each document is checked against the authoritative issuer database. See [Biographic Data Verification](#) for the list of authorities and what fields are submitted.

What the API returns

The default response includes the top-level `verification_status` (`passed` when all documents match and cross-document identity data is consistent, `failed` otherwise), a `verification_description`, and a decrypted `validation_summary` with strategy-agnostic per-document results (`biographic_validated`, `biometric_validated`, `validated_fields`, `changes`, and similar).

To retrieve the raw DVS detail per document, pass `return_documents: true` on the details request. The response then also contains a `documents` object, and each `documents.document_N.validation_result` includes:

- `strategy` - `dvs`
- `verification_result_code` - DVS result: `Y` (match), `N` (no match), or `D` (document invalid)
- `verification_request_number` - DVS request identifier, required for any official queries on the result
- `additional_information` - detail about any mismatch (e.g. "Card number did not match")
- `originating_agency_code` - the OAC used for the request
- `checked_at` - timestamp of the DVS call

See the ID Pass - DVS mode quick start for example payloads, or the ID Pass API Reference for the full response schema.

IDSP mode

In `idsp` mode, Global Data returns an **identity opinion** - a single valid / not valid assessment produced by the combined checks of Global Data's Document Validation System and DVS. Global Data runs the document verification on your behalf and provides you with an identity opinion on whether the documents are valid or not.

This mode is intended for customers who are not registered with DVS but need a compliant identity verification service. Global Data acts as an Identity Service Provider (IDSP) on your behalf, and the identity opinion returned is Global Data's own assessment, not a DVS response.

Requirements

- Liveness detection must be enabled (`check_liveness` set to `true`). This ensures every verification is based on multiple independent checks - liveness, biometric face match (where a photo ID is supplied), and document verification - which together form the basis of a identity opinion.
- Your account must be enrolled as an IDSP Service Client. Contact your Global Data account manager to arrange enrolment.
- No DVS registration is required to use IDSP mode.

Multi-stage document validation

In `idsp` mode, each document is put through a number of checks, including Global Data's Document Validation System and a DVS check. The combined results of these checks determine the verification result for the document, which in turn contributes to Global Data's overall identity opinion for the ID Pass.

What the API returns

The default response includes the top-level `verification_status`, which carries Global Data's identity opinion: `passed` (valid) or `failed` (not valid). It also includes a `verification_description` and a decrypted `validation_summary` with per-document `biographic_validated`, `biometric_validated`, `validated_fields`, and similar friendly fields.

To retrieve the per-document verification boolean, pass `return_documents: true` on the details request. The response then also contains a `documents` object, and each `documents.document_N.validation_result` includes:

- `strategy - idsp`
- `verification_passed` - boolean (valid / not valid) for that document
- `checked_at` - timestamp

DVS result codes, DVS extended result codes, DVS error codes, DVS request identifiers, and the OAC used are not returned in the API response in any mode.

See the ID Pass - IDSP mode quick start for example payloads.

Basic mode

In `basic` mode, ID Pass performs format and checksum validation on the supplied document fields but does not perform any external verification. No DVS call is made, in either live or sandbox.

This mode is useful when you need OCR extraction, liveness, and biometric face match but intend to perform document verification yourself, or when DVS verification is not required for your use case.

Requirements

- No DVS Identity or special enrolment is required.

What is validated

Validation rules are applied to the fields supplied (or extracted by OCR) for each document:

- Document number formats (licence number patterns, passport number patterns, visa number patterns, and similar)
- Card number patterns and checksums, per jurisdiction where applicable
- Medicare card checksums and expiry-date formatting
- Centrelink CRN format
- Name field formats and lengths
- Date of birth format

What the API returns

The default response includes the top-level `verification_status` (`passed` when all documents pass format validation and cross-document identity data is consistent, `failed` otherwise), a `verification_description`, and a decrypted `validation_summary` with per-document `biographic_validated` and `biometric_validated` flags.

To retrieve the per-field validation errors for a failed document, pass `return_documents: true` on the details request. The response then also contains a `documents` object, and each `documents.document_N.validation_result` includes:

- `strategy - basic`
- `basic_validation_passed` - boolean
- `errors` - per-field validation errors (empty when validation passed)
- `checked_at` - timestamp

See the ID Pass - Basic mode quick start for example payloads.

What ID Pass verifies

The ID Pass service performs a number of verification steps to ensure the identity of the person is verified.

Liveness

Liveness detection ensures the person verifying their identity is physically present.

This step involves asking the customer to use their mobile camera or webcam to capture a short video of their face. This video is reviewed by an AI-driven liveness detector to ensure that the video is a real-time video of a human face.

The detector can not be fooled by presenting a previously recorded video of a face, a photo, screen, or mask, etc.

Identity Documents

The customer is asked to take a photo or upload a copy of their identity document.

ID Pass currently supports the following identity documents:

- Australian Driver's Licence
- Australian Passport
- Medicare Card
- Foreign Passport (for Australian Visa holders)
- Centrelink Card (manual entry, no OCR)
- Australian Birth Certificate (manual entry, no OCR)
- New Zealand Driver Licence

The most common use case is to verify two documents where at least one is a photo ID. For example:

- Document 1: Drivers Licence, Passport or Visa
- Document 2: Drivers Licence, Passport, Visa, Medicare card, Centrelink Card, Birth Certificate or New Zealand Driver Licence

Note: A document which has already been verified cannot be used again for a subsequent verification. So if the customer has already used their licence as the first document, then they cannot use it again for the second document.

When more than one document is verified, ID Pass also cross-checks that the name and date of birth are consistent across documents and fails the verification if they do not match. See the [Name Matching](#) section for how names are compared.

Biographic Data Verification

For strategies that perform DVS verification ([dvs](#) and [idsp](#)), each document is checked against the authoritative issuer database. This provides a source of truth for the biographic information on the document.

- **Passports** are verified against the **Department of Foreign Affairs and Trade (DFAT)** database.
- **Australian driver licences** are verified against the **National Exchange of Vehicle and Driver Information System (NEVDIS)**. A New Zealand Driver Licence is verified with the New Zealand licence issuer.
- **Medicare cards** are verified against the **Services Australia** database.
- **Visas** are verified against the **Department of Home Affairs** database.
- **Centrelink cards** are verified against the **Services Australia** database.
- **Birth certificates** are verified against the **Registry of Births, Deaths and Marriages** for the state or territory the birth was registered in.

In [basic](#) mode, no external verification is performed - only document field formats are validated.

Biometric Face Verification

During the liveness check, an image of the customers face (the probe image) is captured and compared to the image of the face on the identity document (the ID photo) using a biometric face verification algorithm.

This step stops a person from presenting another person's identity document by comparing the probe image with the photo on the identity document (eg the licence or passport photo) to ensure they are the same person.

How it works

1. Create an ID Pass link

You call `idpass/register` and choose how many documents to collect, whether to run a liveness check, link expiry, and other options. You receive a secure link, an ID, and a cipher key.

2. Send the link to your customer

If you are inlining the ID Pass process then you can just redirect the customer to the link, otherwise you can send the link via SMS or email. The customer opens it on mobile (recommended) or desktop. If they start on desktop, they'll be prompted to scan a QR code to continue on mobile.

3. Customer completes the verification

ID Pass guides them through consent, selfie liveness (if enabled), and 1, 2 or 3 document checks. They can review and correct OCR-read details before submission (for centrelink, details are entered manually).

4. You receive webhook updates

As the customer progresses, ID Pass can notify you of status changes like `opened`, `in_progress`, `complete`, or `failed`.

5. Retrieve the result

Call `idpass/details` any time (usually after complete) to get the final pass/fail decision and verified identity details.

What your customer experiences

ID Pass is a step-by-step flow optimised for mobile devices, but it will work on desktop with a web camera.

- **Introduction screen** shows what they need to do (liveness, number of documents, optional ID photo).
- **Consent screen** includes your company name and privacy policy link.
- **Liveness selfie video** (if enabled) verifies they are a real person.
- **Document capture** for each required document:
 - take or upload photos,
 - ID Pass OCR engine scans the document and reads the details,
 - customer reviews/edits if needed,
 - ID Pass verifies with DVS (or, for a New Zealand Driver Licence, with the New Zealand licence issuer).
 - for Centrelink card and Birth Certificate, no photo upload/OCR is used; the customer enters details manually before DVS validation.
- **Optional ID photo capture** (if you request it).
- **Completion / error screens** guide them to retry if possible, or stop if limits are exceeded.

See the ID Pass User Journey for more a complete walkthrough of the ID Pass process from start to finish.

Identified and Anonymous ID Passes

You can create an ID Pass **with or without Personally Identifiable Information (PII)**.

The **preferred option** is to use an **identified ID Pass**, in this case you send the name (and optionally the date of birth) of the customer you intend to identify in the `idpass/register` call. The ID Pass service will then compare the supplied name and DOB to the verified documents, and fail the verification if they don't match.

Note: The customer identity you supply is never displayed to the customer, it is only used for verification purposes.

The **alternative option** is to use an **anonymous ID Pass**, in this case you do not send any PII to the ID Pass service. After the customer has completed the verification, you will need to check the returned `verified_identity` field to confirm it matches the intended customer's identity.

These options exist to support use cases where you are not permitted to send any customer PII to the Global Data ID Pass service. Check with your legal team to confirm which option is permitted in your organisation.

Identified: With name and date of birth

You provide your customer's name and DOB in the `idpass/register` call inside the `requested_identity` object.

ID Pass will compare the supplied customer name and DOB to the verified documents, and fail the verification if they don't match.

Use this when you want the service to enforce identity matching automatically.

Example:

```
{
  "document_1_allowed_types": ["licence", "passport"],
  "document_2_allowed_types": ["licence", "passport"],
  "document_verification": "dvs",
  "requested_identity": {
    "first_name": "Sarah",
    "middle_name": "Jane",
    "last_name": "Smith",
    "date_of_birth": "1980-01-01"
  }
}
```

The middle name field is optional, see the API reference for more details.

The date of birth field is also optional. If you omit it (or send null), only the name is matched against the verified documents. In this case you should check the returned `verified_identity.date_of_birth` yourself to confirm it matches your customer.

See the [Name Matching](#) section for more details on how name matching works.

Note: The requested identity data you supply is encrypted with the cipher key and stored in the ID Pass record. It is never displayed to the customer, and is only used for verification purposes.

Anonymous: No PII sent to ID Pass service

You don't provide a name or date of birth in the `idpass/register` call.

After the ID Pass has completed, you check the returned `verified_identity` field to confirm that it matches the intended customer's identity.

Use this when you prefer not to send PII to Global Data.

Example:

```
{
  "document_1_allowed_types": ["licence", "passport"],
  "document_2_allowed_types": ["licence", "passport"],
  "document_verification": "dvs"
}
```

What you can configure

When creating an ID Pass, you can choose:

- **Liveness check:** on or off (must be enabled for `idsp` verification strategy)
- **Number of required documents:** 1, 2, or 3
- **Allowed document types per document:** licence, passport, medicare, visa, centrelink, birth_certificate, nz_licence
- **Optional ID photo step**
- **Link validity period** (1-14 days, default 7)
- **Image retention period** (how long captured images are stored)
- **Webhook URL + events**
- **Return URL** to send the customer back to your app after completion
- **Optional name + DOB matching** (see above)

Quick start integration

Create an ID Pass

Call the `idpass/register` endpoint with your preferred configuration.

You will receive a response containing:

- **id** (ID Pass identifier)
- **link** (the secure link to send to your customer)
- **cipher_key** (needed to decrypt sensitive fields later)

Send the link to your customer

Provide the `link` to your customer. If you are inlining the ID Pass process in your application flow then you can just redirect the customer to the link, otherwise you can send the link via SMS or email. The customer opens it on mobile (recommended) or desktop. If they start on desktop, they'll be prompted to scan a QR code to continue on mobile.

Track progress

When creating the ID Pass, you can subscribe to webhooks for real-time updates. When the status changes, you'll get a simple payload posted to your webhook URL.

```
{
  "id": "19517924-94f0-4000-8e02-afba96ad5101",
  "status": "complete"
}
```

You can use this information to update your system with the current status of the ID Pass or call the `idpass/details` endpoint to retrieve the full pending or completed results.

Retrieve results

Once the ID Pass has completed, you can call the `idpass/details` endpoint with the `id` to retrieve the completed ID Pass results.

If you included the `cipher_key` when creating the ID Pass, then the sensitive fields will be decrypted for you in the response. If you did not include the `cipher_key`, then the response will contain the encrypted values for you to decrypt locally.

The response will contain the following information:

- Overall ID Pass verification status and description
- Document validation results
- Biometric face match scores
- OCR extracted data with customer modifications
- Detailed verification logs
- Biometric images
- Document images

Using the results

See the API reference for full field-by-field definitions of the response fields.

The most important returned fields are:

- Verification status
- Verification description
- Verified identity
- Consent

Verification status

The `verification_status` field contains the final identification pass/fail decision:

- `passed` - identity verified successfully
- `failed` - identity could not be verified
- `null` - still in progress

Verification description

The `verification_description` field contains a human-readable reason for the verification status:

If verification fails (or includes important notes), you'll get a plain-English explanation.

Example:

```
{
  "verification_status": "failed",
  "verification_description": "
    The name on the Medicare Card does not match the name on the Australian Drivers Licence\n
    Your customers date of birth does not match the date of birth on the Australian Drivers Licence"
}
```

Verified identity

When verification passes, the `verified_identity` contains the name and DOB extracted from the verified documents. This is especially useful if you created the ID Pass anonymously and need to confirm the identity of the customer.

Example of the `verified_identity` field in the response:

```
{
  "validation_summary": {
    ...
    "verified_identity": {
      "first_name": "John",
      "middle_name": "Andrew",
      "last_name": "Johnson",
      "date_of_birth": "1980-01-01"
    }
    ...
  }
}
```

Consent

The consent fields contain the exact text of the consent that was displayed to the customer and the date and time when the customer gave consent to the verification process.

Example of the consent fields in the response:

```
{
  "consent_text": "I confirm that I am authorised to provide my personal details...",
  "consent_given_at": "2024-05-16T01:35:11+00:00"
}
```

Note: It is important for you to store the consent details for audit and compliance purposes in line with the DVS requirements.

Billing

Calls to the ID Pass register endpoint are charged per call based on the number of documents requested.

The fee differs depending on the number of documents requested:

- 1 document
- 2 documents
- 3 documents

Calls to the ID Pass details endpoint are not charged.

Please refer to your commercial agreement or pricing documentation for details.

Note: Calls to the ID Pass service in the sandbox environment are not charged.

Privacy and zero-knowledge encryption

ID Pass uses **zero-knowledge encryption** for sensitive data:

- Every ID Pass generates a unique `cipher_key`.
- Fields containing Personally Identifiable Information (PII) and all images are encrypted using that key.
- The key is returned to you in the create response.
- After the customer completes the check, the key is deleted from Global Data systems.

That means **only you can decrypt the sensitive parts of the result**, and you must store `cipher_key` securely. If it's lost, the encrypted data cannot be recovered.

Decrypting results

When calling the `idpass/details` endpoint to read results you can provide the `cipher_key` in the request. If you do, the ID Pass service will decrypt the sensitive fields and return the decrypted values over the HTTPS API response.

Note that this data is always encrypted at rest on the Global Data servers so you must provide the `cipher_key` with each request to decrypt the data.

Local decryption

If you prefer not to provide the `cipher_key` in the `idpass/details` request, then the response will contain the encrypted values for you to decrypt locally.

The data is encrypted using the AES-256-CBC cipher. Use the following pseudocode to decrypt the data locally:

```
function decryptData(encryptedData, cipherKey, iv):
    // Decode the cipher key and initialization vector (IV)
    decodedKey = base64Decode(cipherKey)
    decodedIV = base64Decode(iv)

    // Decrypt the data using AES-256-CBC
    decryptedData = AES256_CBC_Decrypt(encryptedData, decodedKey, decodedIV)

    return decryptedData
```

You can also validate the integrity of the data by validating the MAC.

```
function validateMAC(data, iv, cipherKey):
    // Concatenate the IV and encrypted data
    combinedData = iv + data

    // Generate a MAC using HMAC-SHA256
    mac = HMAC_SHA256(combinedData, base64Decode(cipherKey))

    return mac
```

Limits and retries (customer-visible behaviour)

These limits help protect against fraud and repeated guessing:

- **Face liveness attempts:** dynamically limited based on risk signals, with **at least 3 attempts** before the flow stops.
- **Document verification attempts:** 3 attempts per document.

If a customer hits one of these limits, the ID Pass will show the customer an error screen and return a failed status. You'll need to create a new ID Pass to allow the customer to try again.

Webhooks

Webhooks let you keep your system in sync as the customer progresses.

To subscribe to webhooks, pass the webhook URL and the list of events as part of the `idpass/register` API call.

Supported events

You can configure a webhook URL to receive notifications when specific events occur. The supported events are:

- `**opened**` – The ID Pass process has started.
- `**in_progress**` – Consent has been provided.
- `**complete**` – The ID Pass process is successfully completed.
- `**expired**` – The ID Pass has expired without being completed.
- `**failed**` – The ID Pass process failed.
- `**cancelled**` – The ID Pass was manually cancelled.

Example configuration

```
{
  "webhook_url": "https://example.com/your/webhook/path",
  "webhook_events": ["opened", "complete"]
}
```

We recommend subscribing to all events so you don't miss state changes.

Example webhook payload

When an event occurs, The ID Pass service will send a **POST** request to the configured webhook URL with a JSON payload.

```
{
  "id": "19517924-94f0-4000-8e02-afba96ad5101",
  "status": "complete"
}
```

Parameter	Type	Description
id	string	The unique identifier of the ID Pass. This corresponds to the ID received in the <code>idpass/register</code> API response.
status	string	The new status of the ID Pass, indicating the event that triggered the webhook.

Webhook response and retries

ID Pass expects a **200 OK** HTTP response from your webhook endpoint. If the request fails, the system will retry up to **3 times** before marking the webhook as failed.

Condition	Action
Success (200 OK)	Webhook is marked as delivered.
Failure (non-2xx response)	Webhook is retried up to 3 times.
All retries fail	The webhook is marked as failed, and no further attempts are made.

To ensure webhook requests originate from ID Pass, allow requests only from the IP addresses listed in the IP Whitelisting for Webhooks documentation.

ID Photo

The ID Pass service can optionally ask the customer to capture an ID photo of themselves.

Use this option if you are producing an ID card with the users photo or require a photo of the user for other purposes.

Note: Never use the liveness probe image as the ID photo! The probe image is optimised for biometric face verification and is not suitable for use as an ID photo.

To capture an ID photo, you can set the `capture_id_photo` parameter to `true` in the `idpass/register` request.

You will also need to set the `id_photo_purpose` parameter to specify the purpose of the ID photo. This text will be displayed to the customer on the page where they are asked to capture the ID photo. The `id_photo_purpose` value must be a string between 3 and 255 characters.

```
{
  "document_1_allowed_types": ["licence", "passport", "visa"],
  "document_2_allowed_types": ["licence", "passport", "visa"],
  "require_id_photo": true,
  "id_photo_purpose": "the SampleCo Membership Card"
}
```

The captured ID photo will be verified using a biometric face verification algorithm against the face in the liveness check probe image to ensure they are the same person.

The ID Photo is also checked for a number of different criteria to ensure the photo is valid.

Check	Message shown to the customer
Invalid image file	We could not process your ID photo. Please try again.
No face found	Could not find a face in the image. Please ensure your face is visible.
Multiple faces found	Multiple faces found in the image. Please ensure only your face is visible.
Face occluded	Please ensure your face is fully visible.
Pitch too high	Please tilt your head down slightly - your chin is too high.
Pitch too low	Please raise your chin slightly - you are looking too far down.
Yaw too high	Please turn your head slightly to the right - you are facing too far left.
Yaw too low	Please turn your head slightly to the left - you are facing too far right.
Roll too high	Please straighten your head - it is tilted too far to the left.

Check	Message shown to the customer
Roll too low	Please straighten your head - it is tilted too far to the right.
Brightness too low	Please ensure the image is well lit.
Sharpness too low	The image is too blurry.
Eyes closed	Please ensure your eyes are open.
Sunglasses	Please remove your sunglasses.
Biometric Check Failed	This does not appear to be a photo of you

The photo will only be accepted when all of the checks are passed.

The captured ID photo image and cropped face image are available in the `idpass/details` response in the `images` field.

The cropped face image is a passport style cropped image of the face in the ID photo.

```
{
  "images": {
    "id_photo": {
      "image": "base64 encoded JPEG image",
      "cropped_image": "base64 encoded JPEG image"
    }
  }
}
```

Logs

The ID Pass service logs the validation process and these logs are available to you in the `idpass/details` response.

To return the logs in the `idpass/details` response, you can set the `return_logs` parameter to `true`.

```
{
  "id": "19517924-94f0-4000-8e02-afba96ad5101",
  "return_logs": true
}
```

The logs are returned in the `logs` field of the `idpass/details` response.

```
{
  "logs": [
    "2024-05-16T01:31:23+00:00 - 203.22.251.3 - Starting IdPass flow",
    "2024-05-16T01:35:11+00:00 - 203.22.251.3 - Consent given"
    ...
  ]
}
```

Verification Notes

Name Matching

If a name is supplied when creating the ID Pass, then the ID Pass service will check that the supplied name matches the name on the identification documents.

When two or more documents are verified, the ID Pass service will also check to see if the names on the documents are the same.

Name matching allows for some difference in middle names, however first and last names must be the same.

Name 1	Name2	Name Match	Description
Jane Johnson	Jane Johnson	Pass	The names are the same
Jane Johnson	Jane Mary Johnson	Pass	Additional middle name is permitted
Jane M Johnson	Jane Mary Johnson	Pass	Middle name initials match
Jane Mary Susan Johnson	Jane Susan Mary Johnson	Pass	Middle names in different order
Robert Johnson	Mary Johnson	Fail	First name does not match
Mary Smith	Mary Johnson	Fail	Last name does not match
Mary Susan Smith	Mary Beverly Smith	Fail	Middle name does not match

When a name match between the supplied name and the names on the documents fails, or when multiple documents are verified and the names on the documents are different, then the verification status is set to `failed`.

Passport and Visa

Passport and Visa verification is based on the following fields:

- Given Name(s)
- Last Name
- Date of Birth
- Passport Number

Note that passports and visas use multiple given names instead of a first / middle name format.

Therefore data returned from a passport or visa verification will have the following structure:

```
{
  "first_name": "John Andrew",
  "middle_name": null,
  "last_name": "Johnson",
  ...
}
```

Note that the middle name is included in the first name field and the middle name field is set to null.

Licence

Drivers licence verification is based on the following fields:

- First Name
- Last Name
- Date of Birth
- Licence Number
- Card Number
- Licence State

Note that the middle name is not used in the validation process.

This is because some jurisdictions store only the initial of the middle name. This causes matching issues when the customer enters their correct full middle name but the verification service only has the initial. The DVS service recommends that the middle name is not used in the validation process.

For this reason the ID Pass service will only match the first and last name and date of birth.

New Zealand Driver Licence

The New Zealand Driver Licence (`nz_licence`) is captured front and back like an Australian licence, and the customer reviews the following fields:

- First Name
- Middle Name
- Last Name
- Date of Birth
- Licence Number (two letters followed by six digits, e.g. DB512036 ; the check digit is validated before submission)
- Version Number (exactly 3 digits, printed beside the licence number on the front of the card)

There is no licence state and no card number. The result is returned in the same shape as an Australian licence under the `dvs` strategy:

- Completed checks return `verification_result_code` `Y` or `N` . `D` is never returned for this document type. If the issuer's source is unavailable or the check cannot be completed, the code is null (no verdict) and the customer may retry with the same details.
- `originating_agency_code` is null.
- `verification_request_number` is the reference for the check and can be quoted in any query about the result.

Medicare

Medicare verification is based on the following fields:

- Full Name
- Date of Birth
- Card Number
- Individual Reference Number

Note that the Date of Birth is required for verification but is not printed on the Medicare card. Therefore manual entry is required for this field.

Data returned from a Medicare verification will have the following structure:

```
{
  "full_name": "John Andrew Johnson",
  "date_of_birth": "1980-01-01",
  ...
}
```

Centrelink

Centrelink verification is based on the following fields:

- Full Name

- Date of Birth
- CRN
- Card Type
- Card Expiry

Centrelink card details are entered manually in the ID Pass flow and are validated with DVS.

Note that some Health Care Cards print the name with the full middle name. However, the name should be entered with the middle name as an initial in order to get a successful match.

Data returned from a Centrelink verification will have the following structure:

```
{
  "full_name": "John Andrew Johnson",
  "date_of_birth": "1980-01-01",
  ...
}
```

Birth Certificate

Birth certificate verification is based on the following fields:

- Given Name/s
- Family Name
- Date of Birth
- State or Territory of Registration
- Registration Number, or Registration Date for Queensland and Tasmania
- Certificate Number

Birth certificate details are entered manually in the ID Pass flow and are validated with DVS. The certificate is verified against the registry for the state or territory the birth was **registered** in, which is not necessarily where the certificate was most recently printed.

Each registry identifies the record differently. Queensland and Tasmania are identified by the date the birth was registered; every other state and territory by a registration number. Where a registration number is printed in a form that is not what the DVS expects, ID Pass converts it before sending. Direct API callers are expected to send the value the DVS expects - see the Birth Certificate DVS endpoint for the per-state rules.

The certificate number and private sector callers

Private sector DVS users - which includes all Global Data API customers - must supply the certificate number for NT, SA and ACT certificates issued on or after these dates:

State	Certificate number required for certificates issued from
NT	12 July 1999
SA	1 November 1999
ACT	1 May 2002

This is a rule of the DVS, not of this API. Our validation deliberately does not enforce it: the base DVS rule accepts **either** a registration number or a certificate number, and tightening it here would reject requests that are legitimately valid for certificates issued before those dates.

The consequence is that a request can pass validation and still come back unverified. If you are checking an NT, SA or ACT certificate issued on or after the date above and you do not send `certificate_number`, expect a `D` result (no match on the data supplied) rather than a validation error. ID Pass handles this by asking the holder for the certificate number and letting them say their certificate does not have one.

Data returned from a birth certificate verification will have the following structure:

```
{
  "first_name": "John",
  "last_name": "Smith",
  "date_of_birth": "1980-01-01",
  "registration_state": "NSW",
  "registration_number": "123456",
  ...
}
```

OCR and Edits

The ID Pass service uses an Optical Character Recognition (OCR) engine to extract the data from most document images before verification. The OCR engine is very accurate, however there can sometimes be errors in how the information is read, especially if the document is worn, scratched or in poor condition.

Centrelink cards and birth certificates are manual-entry only and do not use OCR.

The customer is shown the result of the OCR reading and is given the option to edit the data if it is incorrect. This edited data is then used to verify the identity of the customer.

If the customer edits the data, then the changes are recorded in the `changes` field of the `validation_summary` for the document.

```
{
  "validation_summary": {
    "document_1_result": {
      ...
      "changes": [
        "first_name": [
          "from": "John",
          "to": "Jane"
        ]
      ]
    }
  }
}
```

The `verification_description` will also contain a message to indicate that the document had biographic identity edits before verification.

```
{
  "verification_description": "
    Document 1 (passport) had biographic identity edits before verification\n
    The identity was verified successfully"
  ...
}
```

Liveness check

The liveness check works best on mobile devices with a front-facing camera. If the customer is using a desktop computer, then they may receive a lower liveness score.

Device	Typical Liveness Score
Mobile	90 to 99%
Desktop	70 to 90%

The ID Pass service sets a liveness pass cut-off score of 70%. If the liveness score is below 70%, then the customer will be shown an error screen and asked to repeat the liveness check.

Presentation of a false face video during the liveness check will typically result in a liveness score below 20%, far below the 70% pass cut-off score.

Sandbox testing

Sandbox behaviour depends on the selected verification strategy (as set in the `document_verification` parameter when creating the ID Pass). In all strategies, no real DVS calls are made and no fees are charged.

The same set of DVS sample documents can be uploaded through ID Pass in sandbox; what the API surfaces back to you differs per strategy:

Strategy	Sample documents	Other data
<code>dvs</code>	Full simulated DVS result and codes, per the sample document	Follows normal DVS sandbox behaviour
<code>idsp</code>	Identity opinion only (valid / not valid)	Identity opinion only (valid / not valid)
<code>basic</code>	<code>passed</code>	Format pass/fail

DVS in sandbox

When using the `dvs` verification strategy, Australian documents flow through to the simulated DVS engine, which returns the same result codes and descriptions as a direct DVS sandbox call. Uploading a sample document produces its documented sandbox response. A New Zealand Driver Licence flows through a simulated issuer response instead; see [New Zealand Driver Licence in sandbox](#).

See the DVS sandbox responses and DVS sample documents for the full result matrix.

IDSP in sandbox

When using the `idsp` verification strategy, the API returns only Global Data's identity opinion - a valid / not valid assessment produced by the combined checks of Global Data's Document Validation System and DVS.

For testing, the DVS sample documents produce predictable identity opinions:

- Sample documents that pass all checks ? identity opinion is **valid**
- Sample documents that fail any check (document not found, data mismatch, lockouts, system errors, or any other failure) ? identity opinion is **not valid**

New Zealand Driver Licence in sandbox

This section applies to `document_verification: dvs` only. Under the `basic` strategy a New Zealand Driver Licence is format-checked locally and returns `basic_validation_passed`, so none of the simulated results below apply.

In sandbox with the `dvs` strategy, a New Zealand Driver Licence is verified against a simulated issuer response rather than the live source. The following details produce a verified (`Y`) result:

Field	Value
First Name	Dana
Last Name	Mitchell
Date of Birth	1965-09-13
Licence Number	DB512036
Version Number	001

Any other otherwise format-valid submission produces an `N` result with the `NZDL-101` code; licence number `DB111112` with any other details is a convenient deterministic no-match example. Licence number `DB000000` simulates a source outage (no result code; the customer may retry), and version number `999` simulates a rejected request. Details that fail the review-step rules (an invalid licence-number check digit, or a version number that is not exactly three digits) are rejected on the review page and never reach the simulated check.

Basic in sandbox

When using the `basic` verification strategy, no DVS call is made, live or simulated - only format validation is performed. Uploading a sample document returns `passed`. Any other input is validated against the normal document format rules and passes or fails on its own merits.

Cancel an ID Pass

It is possible to cancel an ID Pass after it has been created. This might be useful if, for example, the ID Pass link has been sent to the wrong person.

Call `idpass/cancel` with the ID Pass `id` to cancel when status is `new`, `opened`, or `in_progress`. The response includes `fee_refunded` (`true` or `false`) to indicate whether a refund was applied. A refund is only issued when no verification steps have been taken (typically status `new` or `opened`); if any steps have been taken, no refund is issued.

See the ID Pass API Reference for the full request and response specification.