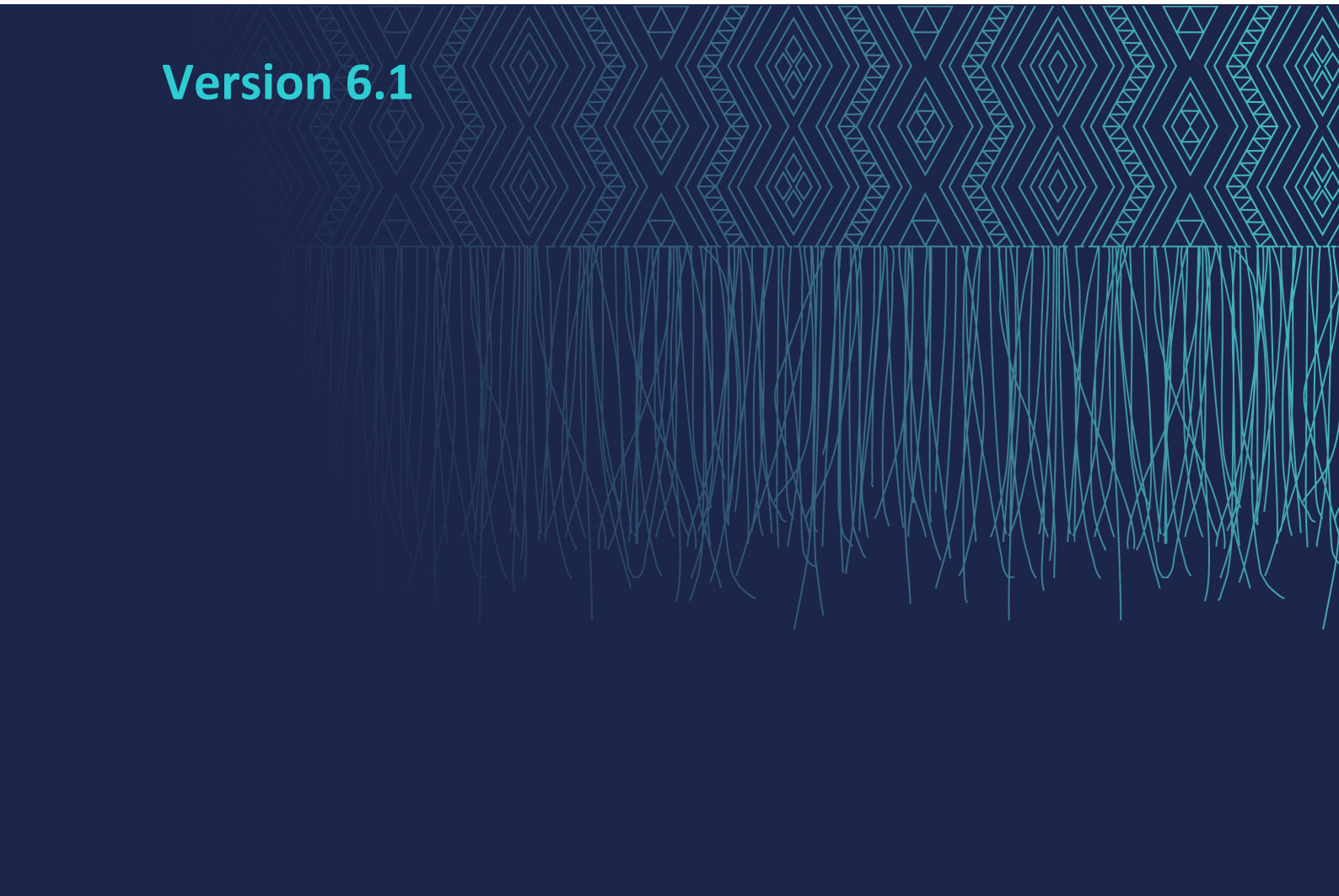
Te Whatu Ora
Health New Zealand

Digital Health Identity Service:
Onboarding & Integration Guide

Version 6.1



Contents

Intro & Getting Started

Welcome! Thank you for expressing interest in onboarding to our Digital Health Identity Service. Over three million people have created a **My Health Account** or **My Health Account Workforce**. Onboarding with the Digital Health Identity service will allow you to make your applications accessible to all our account holders.

Before starting your onboarding journey, please review this guide which provides useful information about our service and the steps required to onboard your application. You will also find pre-requisites, compliance and certification information and an overview of the support available once you are onboarded with the service.

This section provides an overview of the onboarding process and access to our Frequently asked Questions.

Onboarding Process Overview

Stage	Description	Related Information
Consider Stage	**About our Service** | Who we are and why you would want to use our service. **Ideal integrators for our Service** | What organisations are suited to integrating with our service. **Pre-requisites and considerations for utilising our Service** | An overview of what we need to know about you and your organisation, and your anticipated use of our service.	
Onboarding Stage	**Onboarding Process** | An overview of the end-to-end steps required to successfully onboard with our service. **Technical Integration Guide** | An overview of how to connect to our service.	Onboarding Request Form
Use Stage	**Operational & Product Support** | What support will be made available post onboarding to our service.	Who to contact for support
Extend Stage	**New Service Features & Enhancements** | An overview of how new service features and enhancements are requested, delivered and released. **Certification & Accreditation Renewals** | Terms of use and regular compliance reviews	

	may be undertaken and/or requested as and when required.	
Exit Stage	**Offboarding** | An overview of steps required to successfully offboard from our service.	Offboarding Request Form

Frequently Asked Questions

Question	Answer
What attributes can I have access to?	The attributes you can access will depend on your agreed use for them and who your application is targeted at. The core attributes available are: • Email address • First name • Middle name • Family name • Nickname • Birthdate • Mobile number • Confidence level In addition, the health *consumer* service (**My Health Account**) has: • NHI number • Linked Dependent Children The health *workforce* service (**My Health Account** Workforce) also has: • HPI number (CPN)
Are your email addresses verified?	Yes - We verify all email addresses by requiring all account holders to confirm their address using a One Time Passcode (OTP). Email verification occurs when first creating an account or when changing the email address associated with the account.
Are email addresses unique?	Yes - each **My Health Account** must have a unique email address.
Are your physical addresses verified?	**My Health Account** uses physical addresses to match a user to an NHI under certain circumstances only. As such **My Health Account** does not offer Address as an attribute.

What are Confidence Levels?	Confidence Levels are used to indicate to your application the degree to which a user has proven their identity. The confidence levels 1, 2 and 3 are based on the Levels of Assurance outlined in the Identification Management Standards 2020, with the 'N' suffix indicating if the user has linked their unique NHI number to their account. See the Level of Identification Guidance for Integrating Apps section for further guidance regarding Confidence Levels.
What Confidence Levels should I be using for access to my digital health service?	That determination should be made as a result of completing a Privacy Impact Assessment (PIA). There are a number of pieces of legislation that will need to be considered, including the Health Information Privacy Code (HIPC) 2020 and the Privacy Act 2020. The more sensitive the information being shared or updated, the higher the confidence level required. See the Level of Identification Guidance for Integrating Apps section for further guidance regarding Confidence Levels.
How will My Health Account work in a whanau setting, advanced care directives and are these recorded?	**My Health Account** currently supports the linking of dependent children's NHI number to a parent's NHI number in some circumstances. The capability is quite limited now but will be extended in the future to allow more parents and guardians to establish relationships and delegated access to their dependents.
What is your technical method of authentication?	Currently, the Digital Identity service supports Open ID Connect.
How do I sign up to use the service?	You can find out about the sign-up process for the Digital Identity service in our onboarding material. See Onboarding Stage.
Can I get technical support for integrating an application?	We provide a technical guide for the integration aspects of the onboarding process. You can also email any questions through to DHI.Integration@health.govt.nz If required, we can also arrange a group call with the support team to discuss any issues.

Is there a test environment available for development and testing work?	Yes - the integration (INT) environment is available for all development activities. You'll be setup with access as part of the onboarding process.

Consider Stage

The objective of the **Consider Stage** is to understand our service, identify your business benefit and your ability to meet our onboarding requirements. This stage will inform your decision to proceed to the next stage of onboarding.

About Our Service

What is a Digital Health Identity Service?

A Digital Health Identity Service is used by both health consumers and health professionals to confirm who they are digitally, so that they can gain access to online health services using a single verified account.

Why a Digital Health Identity Service?

People expect to engage with and control their health information the same way they do with other digital services – seamlessly and transparently across multiple channels, to help them Live Well, Stay Well, and Get Well. Digital Health Identity is central to the digital delivery of health services. It is an enabler for consumer, practitioner, and third-party access to national health records and systems.

Personally identifiable health information can be very sensitive, so we must ensure individuals are correctly identified, and that access is secure, before allowing them to interact with this information over the Internet.

If your service offering needs to provide secure access to health information, then a Digital Health Identity Service can help.

What is My Health Account?

My Health Account is our Digital Health Identity Service product for health consumers which delivers:

- A secure authentication service based on the OpenID Connect (OIDC) standard.
- A verified identity for over 3.4 million New Zealanders.
- Verified identity claims including name, birthdate, National Health Index (NHI) number and a level of confidence to indicate the strength of the identity verification.

What is My Health Account Workforce?

My Health Account Workforce is our new Digital Health Identity Service product for health professionals which delivers all the same benefits as **My Health Account** plus:

- A verified identity claim for their Health Provider Index Common Person Number, or HPI number (CPN).

While **My Health Account** and **My Health Account Workforce** are on the same underlying platform, there is no link between the two account types. This allows clear separation between personal and professional accounts.

Note: only the presence of an HPI number (CPN) on the **My Health Account Workforce** confirms that the account holder is a member of the health workforce. Where a HPI number

(CPN) is not available, integrating applications will need their own registration process in place to verify the individual is a member of the health workforce.

What are the benefits of integrating with our product and service?

Authentication & Account Management

- The OIDC standards-based approach to authentication means you can use off the shelf libraries to make integration simple, quick, and reliable.
- **My Health Account** and **My Health Account Workforce** provides account administration capability such as password resets.
- The self-service portal allows end-users to manage their account, including changing their email address, password, mobile number, preferred name and multi-factor authenticator.

Verification

- Email addresses and mobile numbers are validated as part of the signup and account creation process to ensure they are owned by the user, and that users can be reached with them.
- **My Health Account** and **My Health Account Workforce** offers a range of identity verification options for users to choose from including:
    - Document check (using 7 of the most common forms of identity documents).
    - Healthcare Provider check (using the details the user has registered with their enrolled General Practice).
    - In-person verification (by visiting a nominated professional to complete a liveness check).
- **My Health Account** and **My Health Account Workforce** users have the option to signup using their RealMe verified identity.
- For health *consumers*, **My Health Account** can find and bind their NHI number to their account, making it easy to match health information to their identity.
- For health *professionals*, **My Health Account Workforce** can find and bind their HPI number (CPN) to their account (if they have one), making it easy to match professional information (e.g. scopes of practice, annual practicing certificate) to their identity

Ideal Integrators for our Service

Our vision is to *enable New Zealand health consumers to better their health outcomes through access to digital health services*. Our ideal integrators are any agencies or entities, who share this vision.

This could include (but is not limited to):

- Primary Health Organisations (PHOs) with consumer portals.
- Private companies providing patient portals or other digital services to better the health outcomes of their customers.
- Health sector start-ups looking to leverage a large potential customer base.

- Other government agencies with an interest in the health outcomes of New Zealanders.

If you think you fit the bill, complete our onboarding request form to get started: Onboarding Request Form

Eligibility & Priority

To be suitable for onboarding with our service, an external application should:

1. Enable health consumers to digitally interact with the health sector and actively engage in their health journey.
2. Provide health related information that requires the unique identification of health consumers or providers.
3. Deliver services and outcomes for the health sector.

Onboarding priority will be given to integrators who meet one or more of the following criteria:

1. Support the National Public Health services
2. Be targeted at Māori and priority population groups including Pacific, disabled, elderly and people living in low socio-economic areas.
3. Enable increased engagement in the health sector to the benefit of the individual.
4. Support for New Zealand official languages.

Pre-requisites and Considerations for Utilising our Service

Before you are provided with access to the Digital Health Identity service, we need to find out more about you, your organisation or agency and the applications you intend to integrate with **My Health Account** or **My Health Account Workforce**.

In connecting with the Digital Health Identity service, we will be providing you with known information about the holder of the account. This includes information such as their name, email, date of birth and NHI number or HPI number (CPN).

While we won't share this information with you without the account holder's consent, we do need to confirm that you have effective measures in place to safeguard the privacy and security of the attributes being shared.

The onboarding process is designed to confirm your application is both designed and implemented with effective security and privacy controls in place.

Should you choose to integrate with the Digital Health Identity service you must be prepared to supply the following information during the onboarding process:

- An overview of the features and services your application will provide to **My Health Account** or **My Health Account Workforce** holders.
- A high-level design for how you plan to integrate with the Digital Health Identity service.
- A Privacy Impact Assessment that details how the **My Health Account** or **My Health Account Workforce** supplied data will be managed.
- Evidence of due diligence in terms of a security risk assessment or penetration test report for your integrated application.

- A test exit report with the findings of your end-to-end testing with our product and service.

We will work with you to collect and review your documentation as part of the onboarding process. We also provide a technical guide and support as you work through the steps to open your application to over three million New Zealand **My Health Account** and **My Health Account Workforce** holders.

Level of Identification Guidance for Integrating Apps

As part of the onboarding process, integrators must provide evidence that access to their application is restricted to those **My Health Account** or **My Health Account Workforce** users who meet the required Level of Identification (known as the Confidence Level claim). The below table provides guidance to integrators on the Levels of Identification and the types of information that would apply to each.

Note: this information is meant as a guide. For applications where there is an established identity risk, a full identity risk assessment should be conducted to help inform mitigation strategies. The Digital Government website has a comprehensive guide for identification risk and assessments: Assessing identification risk.

Level of Identification	Description	Use Cases	Guidance for Integrators **The types of information that can be viewed or collected must align with the level of identification**
Level 1	A user at this level of identification has validated that their email address is real and that they have access to it. At Level 1 no identity verification processes have been completed.	N/A	When a user presents with this level of identification, they should be directed back to **My Health Account** to complete account set-up.
Level 2	A user at this level of identification has provided information from an official document (such as a driver licence or passport) which has then been verified as a valid identity. Alternatively, the user has provided information related to their enrolment with a	Allow a user to view a limited range of self-determined information about themselves such as Preferred Name, Gender, Ethnicity. Allow a user to access non-public information (so long as it is non-personal) such as integration details or maintained data lists.	Personal information must not be collected. Any shared personal information must be self-determined only.

	GP, where a link to the person who supplied the identity has been confirmed. At Level 2 there is limited assurance that the person claiming the identity attributes is also the owner of the identity.		
Level 3	A user at this level of identification has both verified an official document and further substantiated that they are linked to that verified identity. There is strengthened assurance that the person claiming the identity attributes is the owner of the identity.	Allow a user to view and submit personal information about themselves such as physical address, contact details and other personal information.	Personal information can be collected (other than health information which requires Level 3N). Personal information can be shared (other than health information which requires Level 3N).
Level -N	A user with an “N” suffix has chosen to link their National Health Index (NHI) number to their **My Health Account**. An NHI number can only be linked to a single **My Health Account**. The NHI can be linked at Level 2 or Level 3 but can only be used to access or submit personal health information when at Level 3N. Level 3N provides additional assurance that the health information you share or collect belongs to the account owner.	Allow a user to view and submit personal health information about themselves. Allow a user to book an appointment (this may be available at 2N) or request a prescription.	Access to non-personal health information (such as requesting bookings and appointments) could be allowed at Level 2N. Access to personal health information is restricted to Level 3N.

Onboarding Stage

The objective of the **Onboarding Stage** is to obtain onboarding approval and successfully onboard with our service.

During this stage we will guide you through the end-to-end onboarding steps required to successfully onboard with the Digital Health Identity service.

Onboarding | Initiation

Applying for Access

To start the onboarding process, we need to know more about your organisation and the applications you will be developing that will integrate with the Digital Health Identity service.

You need to provide this information by completing the Onboarding Request Form

and submitting it to the Digital Identity team.

Describing your Application to the Consumer

As part of the onboarding request form, you will be asked to provide a description of your application.

The description should, in 200 characters or less, describe the following:

What your app does, how you intend to use someone's data if they agree to share their details with you, and/or how sharing their details with you benefits them.

The description must begin with the name of your application.

Some example descriptions can be found below:

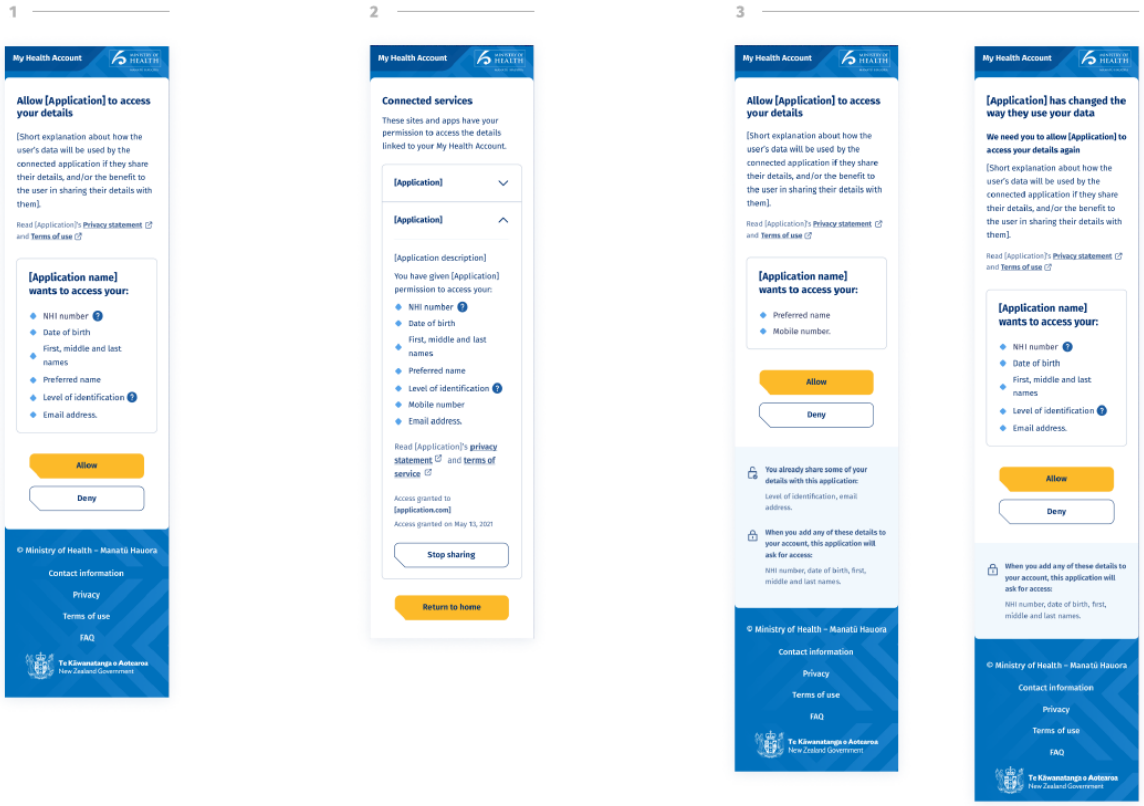
"[Application Name] uses your details to verify who you are, securely match you to your health records, and to communicate with you about your health."

"[Application Name] needs your information so that you can request and manage appointments with your healthcare provider and so you can receive reminders when you are due for a check-up."

This is intended to empower users to make informed choices when consenting to sharing their information with you.

The description will be used in 3 scenarios:

1. When someone first logs in or signs up to your application using their **My Health Account** or **My Health Account Workforce**.
2. When someone views the list of applications they have previously consented to sharing their details with. When your application is in the list, the text you supply will be used to remind them of what your application does.
3. When someone is renewing consent, after:
    a. They add new information to their account.
    b. The claims list requested by your application is updated.
    c. The description of how your application uses someone's data changes.



Onboarding Request Form

Below is a link to the onboarding form. You need to complete a form for each application that you intend to integrate with the Digital Health Identity Service.

Onboarding Request Form

The form requests information about you, your organisation, the application you wish to integrate, and how you intend to use the Digital Identity Service to support your application as well as some technical details needed to initiate the integration.

Once you submit your form it will be sent to DHI.integration@health.govt.nz for processing.

Processing Your Application

The onboarding team will review your application. During the review process the team may require further information and a short meeting maybe required to discuss your application. If required, the meeting will be held remotely over Microsoft Teams.

You can expect the approval process to take around 5 business days, but this may vary depending on further information required specific to your application.

Once your application has been processed and approved you will be provided with all the necessary information to start the next step of the process and commence your integration work.

Onboarding | Integrate your Application

When your onboarding request is approved, you can begin the development work to integrate your application with the Digital Health Identity service.

The integration, or INT, environment is provided for this purpose. In addition to using the INT environment for developing and testing your application, you will also use the environment for completing the compliance process. Once you have completed all the onboarding steps, the INT environment remains available to you for your ongoing development and testing needs.

Connecting your Application

Note: A detailed Technical Guide for developers is provided as part of the onboarding pack.

We will use the information you supplied in the onboarding request to create an app registration for your application. Once the app registration is in place you will receive the following details:

- ✓ Connection details for the INT environment.
- ✓ The client ID for your application.
- ✓ Shared secret.
- ✓ Details of available test accounts and data.

Developers can use this information to begin the process of integrating with the service.

Testing Access

To allow you to test your application's integration with the Digital Health Identity service, we provide details of pre-created test accounts that are available to all integrators.

These accounts allow you to perform your testing against each of the confidence level's the Digital Health Identity service supports. Namely:

- Level 1
- Level 2
- Level 2N
- Level 3
- Level 3N

My Health Accounts created from RealMe Verified accounts are also available in the test set that cover confidence levels 3 and 3N.

Getting Support

Any questions or problems can be submitted to the Digital Identity team by sending an email to dhi.integration@health.govt.nz.

The team will endeavour to respond to any support requests within 48 hours.

Please note support is only available during standard business hours.

Onboarding | Technical Integration Guide

Overview

This guide explains how to connect to the Digital Identity service, thereby making your applications accessible to over three million **My Health Account** holders. This guide is applicable to both the consumer and workforce versions of **My Health Account**.

The service supports Open ID Connect and is built on Microsoft's Azure AD B2C. While this guide will walk through the technical aspects of the authentication process, it is not intended as an OIDC/OAuth tutorial. Consequently, this guide assumes you are already familiar with the use of OIDC.

If further information is required, documentation on both OIDC and OAuth is available online. You can also find the OIDC specification on the OpenID site.

My Health Account and My Health Account Workforce

The Digital Identity service provides a common platform for both the *consumer* and *workforce* versions of the account. The integration approach is identical for each account type except for the use of a different endpoint and a variation in the claim set available to the relying application.

This guide identifies the integration differences where they exist. However, unless otherwise stated, you should assume the instructions provided are applicable to both account types.

You should note that while both accounts are served by the same identity platform, the accounts are not interchangeable, i.e. you cannot authenticate using a consumer account against a workforce endpoint and vice versa.

Getting Started

Before you start, you will need to have registered your application with the Digital Identity team and have the following information available:

- ✓ Client ID.
- ✓ Shared secret (unless using PKCE).
- ✓ Registered redirect URL.

Initially, you will receive this information for connecting to the integration (INT) environment. This is an environment where you can develop the integration for your application. You will also use this environment for completing the compliance process. Once we have confirmed your application is compliant, you will be set up with access to the Digital Identity production environment.

Recommended Grant Types

You will need to tell us your application type so we can create the appropriate registration. The application's type will determine the OAuth grant types the Digital Identity service integration will support.

There are two application types:

App Type	Grant Type	Description
Web application	Authorization Code	This is for classic web applications where the calls to the Digital Identity service can be orchestrated through a back channel.
Single page app or mobile app	Authorization Code with PKCE	Use this type where you have a single page application, in which the client is handling the authorization flow directly with the Digital Identity service.

Note: While implicit flow is available, we do not recommend or support its use.

Connection Details

My Health Account and **My Health Account Workforce** are accessed via separate endpoints. You can use the public endpoints below to pull down all the details needed to issue auth requests for the INT environment.

My Health Account:

```
1 https://b2c-int.login.health.nz/mohintb2cdir.onmicrosoft.com/b2c_1a_moh_digitalidentity_signuporsignin/v2.0/.well-known/openid-configuration
```

The **My Health Account** self-service portal for the INT environment is available at:

- https://app-int.identity.health.nz

My Health Account Workforce:

```
1 https://b2c-int.login.health.nz/mohintb2cdir.onmicrosoft.com/b2c_1a_moh_digitalidentity_signuporsignin_workforce/v2.0/.well-known/openid-configuration
```

The **My Health Account Workforce** self-service portal for the INT environment is available at:

- https://workforce-int.identity.health.nz

Authentication with the Digital Identity Service

The Digital Identity service is a standards-based identity provider that supports Open ID Connect. This adherence to standards means you can use your preferred OAuth library for integrating with the service.

The Digital Identity service is built on Microsoft's Azure Active Directory B2C platform. Some samples on integration can be found here: Azure Active Directory B2C integrate with app samples | Microsoft Docs.

While you will likely use your favourite library to handle the authentication process, this section of the guide provides an example of the authentication request, as well as describing the key parameters the Digital Identity service supports.

Issuing the Authentication Request

Below is an example of the requests involved in the authorization code flow. Please note this is an example only and you should consult the documentation of your chosen library.

The first step is to direct your user to the Digital Identity service where they can initiate the login process. This is achieved by your client application directing the **My Health Account** holder to the authorize endpoint:

```
1 https://b2c-int.login.health.nz/mohintb2cdir.onmicrosoft.com/b2c_1a_moh_digitalidentity_signuporsignin/oauth2/v2.0/authorize?
```

```
client_id=your-client-id
&response_type=code
&redirect_uri=http%3A%2F%2Fredirecturi%2Fyourapp%2F
&scope=openid%20%2000000000-0000-0000-0000-000000000000
&state=your-state-value
```

If the **My Health Account** holder is authenticated by the Digital Identity service, your application will receive a code in response to the above request. You can then exchange this code for an ID token and access token.

Note: In the above example, the scope value `00000000-0000-0000-0000-000000000000` represents the client ID for your app. The client ID must be supplied to receive an access token.

Obtaining the ID and Access Tokens

Here is an example request to complete the authentication flow by issuing a POST request to the `/token` endpoint. Note in this case the client secret (not shown) is supplied using the HTTP basic authentication scheme:

```
POST /token


code=the-authorization-code
&redirect_uri=http%3A%2F%2Fredirecturi%2Fyourapp%2F
&grant_type=authorization_code
```

Once you have obtained the `id_token` and `access_token` your application will have access to the claims the Digital Identity service assets on behalf of the **My Health Account** holder.

Requesting Access Tokens for FHIR Services

Health consumer applications that integrate with Hira FHIR services require the following for authorization:

- The API key issued for your application
- A Digital Identity issued access token containing the required scope values for the FHIR resources

The API key, which is added as a header to all requests to the FHIR service, and is obtained as part of the onboarding process. You must ensure this key is not exposed to the client and hence mandates that all FHIR calls from your application are made from a back channel.

The access token is obtained by including the required FHIR resources in the `scopes` parameter of the request submitted to the `/authorize` endpoint. The scope value in the request must be of the format:

```
<DI env domain>/fhir/<context>:<resource>.<permissions>
```

The format of the scope values as shown above are based on SMART on FHIR [1]and must include the domain of the authorization server as a prefix.

An example of scope values for the NHI Patient resource for the INT environment is:

```
https://b2c-int.login.health.nz/fhir/patient:Patient.r
https://b2c-int.login.health.nz/fhir/patient:Patient.u
```

You will be advised of the scope prefix for the production environment when your production credentials are issued.

The scope values for the required FHIR resources need to be included in the `/authorize` request along with the existing scope value, e.g., `openid`, `offline_access`.

A successful call to `/authorize` will return a code that can be exchanged for a token from the `/token` endpoint. Setting a scope value will result in an access token being returned to your application, along with the `id_token`.

You can confirm the success of the call by inspecting the claims within the access token. If access to the FHIR resource has been granted, the `scp` claim will contain a list of the entitled resources. Note the prefix for the scope value is stripped off in the access token, as shown in the example below:

```
"scp": "patient:Patient.r”
```

You should note that the content of the `aud` claim will differ between the `id_token` and the access token. The `aud` claim identifies the audience for the token. For the `id_token`, the claim will hold the client ID of your application. For the access token, the audience claim holds the client ID of the FHIR resource, as the FHIR service is the intended recipient of the token.

To call the FHIR resource you need to attach the access token to the call as a bearer token. You must also add your issued API key to the request as a header:

```
Authorization: Bearer xxxxxxxxxxxxxxx
x-api-key: xxxxxxxxxxxxxxx
```

The next section covers the supported set of claims.

Digital Health Identity Claim Set

The Digital Identity service provides a combination of standard and custom claims.

Claims are available to the application either through the `id_token` or through the `UserInfo` endpoint. The ID token includes the standard OIDC claims while applications can use the `/userinfo` endpoint to retrieve the full set of standard and custom claims.

The next section details the standard and custom claims and their sources.

---

[1] http://hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html

Standard Claims

The standard claims are shown in the table below:

Claim	Description	Source

sub	The unique identifier for the **My Health Account** holder.	`id_token`
		
		`UserInfo`

email	The verified email address for the **My Health Account** holder.	`id_token`
		
		`UserInfo`

given_name	The account holder's optional given name, as recorded on the official document they supplied as evidence of identity on sign up.
	
	Available on accounts at confidence level 2 and higher.
		`id_token`
		
		`UserInfo`

middle_name	The account holder's optional middle name, as recorded on the official document they supplied as evidence of identity on sign up.
	
	Available on accounts at confidence level 2 or higher.
		`id_token`
		
		`UserInfo`

family_name	The account holder's family name, as recorded on the official document they supplied as evidence of identity on sign up.
	
	Available on accounts at confidence level 2 or higher.
		`id_token`
		
		`UserInfo`

nickname	The nickname claim is an optional attribute that can be set by the **My Health Account** holder using the self-service portal. On the portal this is known as the preferred name.
	
	When set, the claim is available on accounts at confidence level 1 or higher.
		`id_token`
		
		`UserInfo`

birthdate	The date of birth as recorded on the account holder's official document used as evidence of identity. The format of the date is YYYY-MM-DD. Available on accounts at confidence level 2 or higher.	`UserInfo`

Custom Claims

In addition to the standard set of claims as defined by the Open ID Connect core specification, the Digital Identity service also provides a set of custom claims that are specific to a **My Health Account**.

All custom claims are identified by the prefix `urn:login:health:nz:claims:`

Claim	Description	Source
urn:login:health:nz:claims:mobile_number	Where available, contains the verified mobile number of the account holders. Available on accounts at confidence level 1 or higher.	`UserInfo`

urn:login:health:nz:claims:confidence_level	Asserts the confidence level of the account holder's identity.
	
	Available on all accounts. Value range:
	
	• 1
	• 2
	• 2N
	• 3
	• 3N
		`id_token`
		
		`UserInfo`

urn:login:health:nz:claims:nhi (Consumer only)	The NHI number bound to the account. Available on all accounts at confidence levels ending in N (2N or 3N).	`UserInfo`
urn:login:health:nz:claims:cpn (Workforce only)	The CPN/HPI number associated with a healthcare professional. Available on accounts at confidence level 2.	`UserInfo`
urn:login:health:nz:claims:relationships_parentchild_list (Consumer only)	List of children setup in a relationship. This claim is returned as a comma delimited string of NHIs. e.g. "ZZZ0032, ZJJ8114"	`UserInfo`

User Info Endpoint

The `/userinfo` endpoint is invoked using the request as shown below and by submitting either the `id_token` or the access token as a bearer token:

```
GET https://b2c-int.login.health.nz/mohintb2cdir.onmicrosoft.com/b2c_1a_moh_digitalidentity_signuporsignin/openid/v2.0/userinfo
```

The request will return the full set of claims that your application is entitled to view.

Note: certain claims available from the User Info endpoint are governed by the trust relationship between the application and Te Whatu Ora and a need to know, e.g., if an application does not need to know the account holder's NHI, mobile number or DOB, these will not be returned. The list of which claims an application can receive is configured during the application onboarding process.

Below is an example of the claims returned from the `/userinfo` endpoint for a **My Health Account:**

```
{
    "sub": "55601ea4-19ba-48ee-98e2-bf061e91cf0a",
    "email": "user_email@domain.com",
    "given_name": "Dennis",
    "middle_name": "The",
    "nickname": "Dean",
    "family_name": "Menace",
    "birthdate": "2000-05-25",
    "urn:login:health:nz:claims:mobile_number": "+64123456789",
    "urn:login:health:nz:claims:confidence_level": "3N",
    "urn:login:health:nz:claims:nhi": "ZZZ1234"
}
```

You should note that if the access token used is issued for requesting a FHIR resource, then the claims available from the `/userinfo` endpoint will be restricted to the minimal set available for the FHIR service, typically the confidence level and NHI number. If this is the case, then to obtain the full set of claims available to your application you must use the `id_token` in the `/userinfo` call.

Integration Details

This section contains information you must be aware of when integrating with the Digital Identity Service.

RealMe Error Requirements

The Digital Identity service integrates with RealMe to provide account holders with another option for signing up to **My Health Account**.

Most of the integration with RealMe is handled seamlessly by the Digital Identity service. However, due to the way both RealMe and Digital Identity technologies work, any errors that occur for account holders during the RealMe journeys are returned as errors to the application that triggered the request. Consequently, your application needs to be aware of these errors and ensure they are handled accordingly.

Integrating applications will need to handle these errors:
https://developers.realme.govt.nz/how-realme-works/realme-saml-exception-handling

Error Codes

In addition to the RealMe codes, you can find a full list of the possible error codes returned during the auth process from the Microsoft Azure AD B2C documentation. See https://learn.microsoft.com/en-us/azure/active-directory-b2c/error-codes

Token Expiry

The lifetime of Digital Identity tokens is:

Token	Expiry
ID Token	60 minutes
Access Token	10 minutes
Refresh Token	24 hours

Logout

When an end-user logs out of your application you may also wish to clear their session within Azure B2C. Doing so will cause **My Health Account** to request the user to authenticate should they attempt to sign back into your application. Without the logout, if the B2C session is still active than an `id_token` and `access token` will be issued without the need for the user to authenticate again.

The timeout on the B2C session is a rolling 30 minutes.

If this behaviour is not required for your app, then you will need to explicitly logout from B2C. This is achieved using the `logout` endpoint.

The logout endpoint can be found from the discovery URL under the `end_session_endpoint` key.

For the INT environment the logout URL is:

```
1 https://b2c-int.login.health.nz/mohintb2cdir.onmicrosoft.com/b2c_1a_moh_digitalidentity_signuporsignin/oauth2/v2.0/logout
```

The request parameters required for a successful call are:

Parameter	Description
id_token_hint	A previously issued `id_token`. This is a mandated parameter and enforces a check that the supplied URL in the `post_logout_redirect_uri` parameter is a registered URL.
post_logout_redirect_uri	Specifies the URL that the user will be redirected to after successfully signing out.

	This URL must be set as a redirect URI under the application's app registration.

Upgrading Accounts at Sign-In

Your application is responsible for checking the `confidence_level` claim of the signing-in account holder to confirm they meet the required level of identify assurance for access. When an account holder is not at the necessary confidence level, for example level 2N is required but the account is only at a level 1, you have the option to redirect the user to the My Health Account self-service portal to complete the necessary identity checks. Once the account holder has achieved the necessary confidence level, the self-service portal will redirect them back to your application, where they can continue with their sign-in journey.

Additionally, this mechanism can be used to navigate the healthcare consumer to the My Health Account self-service portal, where they can add one or more relationships to their account and then be returned to your application when they are complete.

The process for initiating the redirect to My Health Account, in order that the account holder can complete their identity checks or add new relationships, is explained in the next sections.

Prerequisites

When redirecting the account holder to the self-service portal, a return URL is required in the request. The return URL must be recorded against your application's app registration so that it can be whitelisted with the Digital Health Identity platform. You can provide this URL in the list of redirect URLs when requesting to onboard with the service.

Upgrade Request

The endpoint for requesting an account upgrade is:

```
GET
https://identity.health.nz/account/upgrade
```

The request parameters for the call are:

Parameter	Description
redirecturl	The URL that the account holder will be redirected to once they have achieved the requested confidence level. Note the use of deep links and query strings within the URL is not supported.
clientid	The client ID of your application.
levelrequired	The confidence level you require the account holder to achieve before they are redirected back to your application.
state	A URL encoded string that will be returned as a parameter in the redirect response once the upgrade on My Health Account is complete. You can use this parameter to drive the user experience when the account holder returns to your application. To guard against man-in-the-middle type

	attacks we strongly recommend that you do not provide sensitive information in this parameter. Instead, the guidance is to submit a nonce that can be used to correlate the response with session information held on the client side.

Add Relationship

The endpoint for requesting the account holder to add additional relationship information is:

```
GET
https://identity.health.nz/relationship/add
```

The request parameters for the call are as per the upgrade account request, except in this case the confidence-level required parameter is not supplied:

Parameter	Description
redirecturl	The URL that the account holder will be redirected to once they have completed adding relationships.
clientid	The client ID of your application.
state	A URL encoded string that will be returned as a parameter in the redirect response once the account holder has completed adding the additional relationships.

In redirecting the account holder to the My Health Account self-service portal, they must have a confidence level of 3N. If the account holder does not have the required confidence level, then an error code is returned - `incorrect_confidence_level`.

Response Error

If the response values are incorrect or missing, a 400 (Bad request) Http Status code will be returned with details of the incorrect values:

```
[
    "Redirect URL must be set.",
    "The confidence level required must be set.",
    "ClientId is required"
]
```

Response Parameters

At the end of the upgrade or add relationship process the user is redirected back to your application. The following optional parameters are returned in the redirect response:

Parameter	Description

reauthrequired	If set to “true”, indicates that the application needs to initiate a re-auth by calling the `/authorize` endpoint. This is typically required when the account holder is adding a new relationship. This could result in a new claim being added to the account that has not previously been consented. Initiating the authentication process will ensure the account holder is prompted to provide consent for the new claim.
error_code	Error code indicating an issue with the request. This is currently only used when adding a relationship and the account holder is not at the required confidence level. For other errors you must check the status of the http response.
state	Value passed in for the originating request. Note the security guidance to avoid passing sensitive information and to instead adopt the pattern of supplying a nonce that can be used to subsequently retrieve information stored on the client-side.

Onboarding | Testing & Signoff

Once your development work is complete, we require you to demonstrate that your application conforms to our standards, which will involve you working through a number of test cases which we will provide to you.

This step is simply for you to make sure you're happy with the integration and that everything is running as expected. Use this step as a chance to ask any questions, make sure you're getting the responses that you expect, and that you've met any Branding and RealMe Error requirements outlined in the Technical Integration Guide. We can also have our technical support engineers assist with onboarding if you find that you're struggling to get something working.

Once you think you're good to go, we'll work with you to validate your onboarding, ensure our integration requirements are met and provide you with a sign-off certificate to validate INT is functioning correctly.

Note: We won't do this for every environment you've integrated into our INT environment. Pick one that is late enough in your lifecycle to be a stable integration environment, but not so late you can't test yourself in your own higher environment if you have it (such as Pre-Production).

Testing your Integration

You will receive the test cases you need to execute as part of the materials we will supply when you start the onboarding process.

For the formal testing process, this will be run collaboratively, where we will step through the test cases with you as part of an extended demo. This session will be run remotely, and you will need to capture screenshots of each successful test to confirm your application's behaviour.

For your planning purposes, the table below provides a high-level view of the main test cases you'll need to execute during the testing and sign-off steps:

	Test Case	Objective
1	Branding - Compliance	Demonstrate your application complies with the **My Health Account** or **My Health Account Workforce** branding guide.
2	Login - Sign-in or sign-up success	Confirm your application is correctly integrated with the correct Digital Health Identity service (i.e. either **My Health Account** or **My Health Account Workforce**) and that an account holder can either login securely from your application or login by following the sign-up flow.
3	Login - Consent declined	Demonstrate how your application can handle the scenario where the account holder declines to give consent to share claim information.
4	Login - RealMe errors	In the case of a RealMe account holder failing to authenticate, demonstrate your application can successfully handle the errors returned by RealMe.

5	Login - email change	Confirm that a user of your application can still login after changing the email address associated with their **My Health Account** or **My Health Account Workforce** using the self-service portal.
6	Claims - Retrieval	Demonstrate your application can retrieve the account holder's confidence level from the Digital Health Identity service.
7	Claims - Confidence level	Show your application can prevent the account holder from accessing restricted information if their identity confidence level is not at the required level. You should also consider in your demonstration how you inform the account holder of the need to upgrade their confidence level and cover how your application will allow the account holder to sign up once they have increased their confidence level.
8	Logout - Success	An app can request the Digital Health Identity service to logout the user. If your application is calling the `logout` endpoint you need to demonstrate you can successfully initiate the logout without error.
9	Terms of Use and Privacy Statement	Confirm that the links to your Terms of Use and Privacy Statement are valid.

Please note these tests represent the minimum set. Based on how your application intends to use the Digital Health Identity service additional tests may be required to cover other scenarios. Where additional tests are required, we will endeavour to advise you of any new testing requirements in the early stages of the onboarding process.

Branding Guide

You can download a copy of the **My Health Account** and **My Health Account Workforce** branding guide here.

Test Account Data

To test the integration of your application with the Digital Health Identity service you will obviously need a set of test data. We have created a set of accounts for this purpose. The accounts are shared by all users of the INT environment and account data is reset monthly.

Test Account details will be provided once your Onboarding Request has been approved.

In addition to the shared accounts, we also encourage you to make use of RealMe linked accounts for creating your own test data.

Using RealMe for Testing in the INT Environment

The INT environment enables you to develop and test your application with the Digital Health Identity service. However, while the INT environment does provide a number of test accounts that you can use for the compliance test cases, if you have specific test data requirements then you will need to create your own accounts.

Due to the complexity of the data required to pass the identification checks for **My Health Accounts** at confidence level 2 or higher, you may find you are limited to the creation of basic

level one accounts. Fortunately, the use of RealMe will allow you to both establish accounts at confidence level 3 and set your own test data.

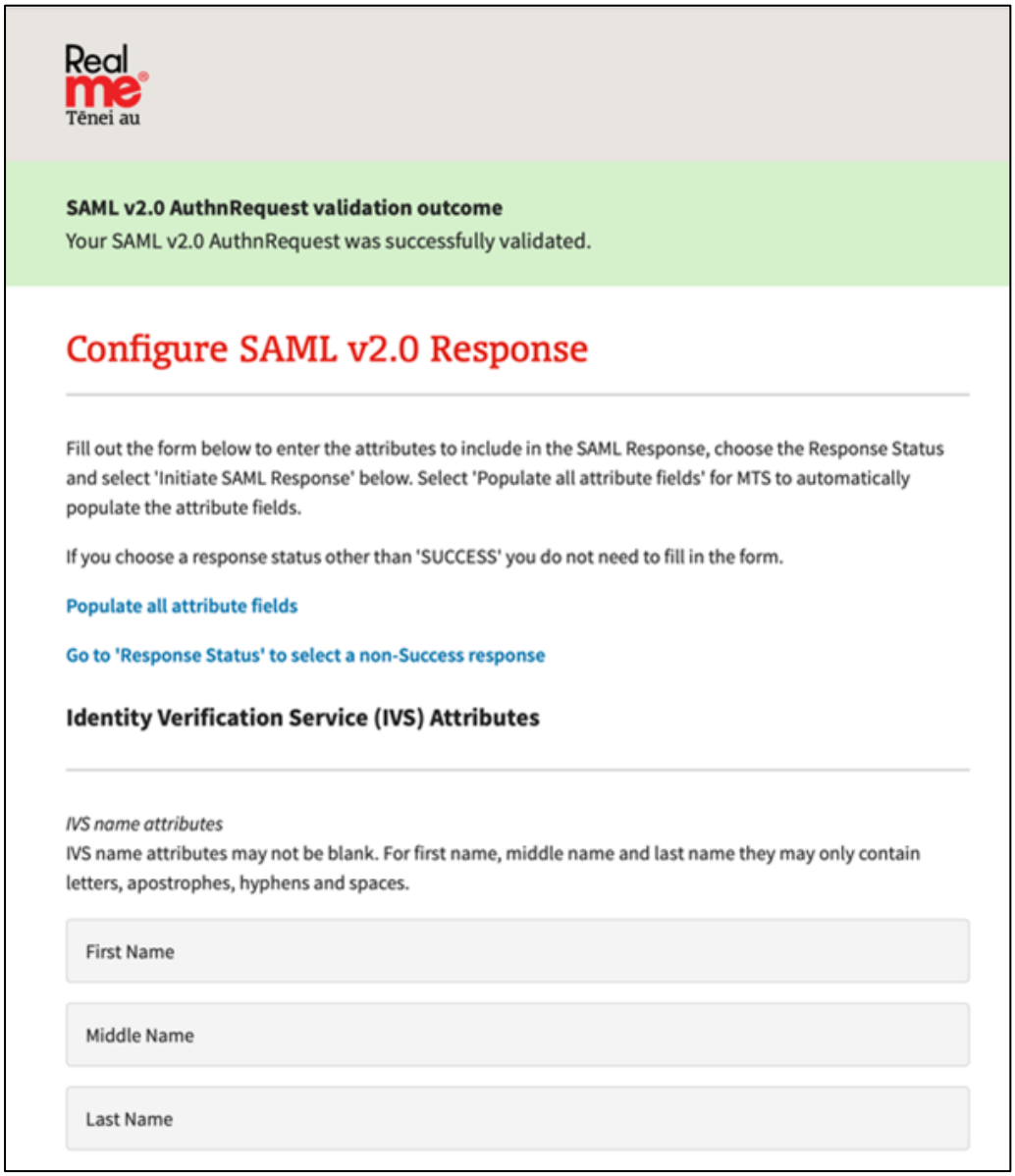
RealMe Message Test Environment (MTS)

RealMe provides their MTS environment to allow developers to both implement and test the integration of their applications with the RealMe services. Correspondingly, we have integrated the INT environment with MTS in order that anyone integrating with the Digital Health Identity service can easily test with RealMe linked accounts.

Using MTS allows you to test the sign-up and sign-in processes, as well as testing the various failure scenarios with your own self-generated data. You should note the main difference between RealMe MTS and RealMe Production is that some of the RealMe screens will look different, as MTS provides a more developer-centric view. However, the login functionality remains the same between production and non-production.

Creating Test Accounts

To create a new account in the INT environment with MTS, first select to sign-up with RealMe. You will be redirected to the following RealMe MTS site:

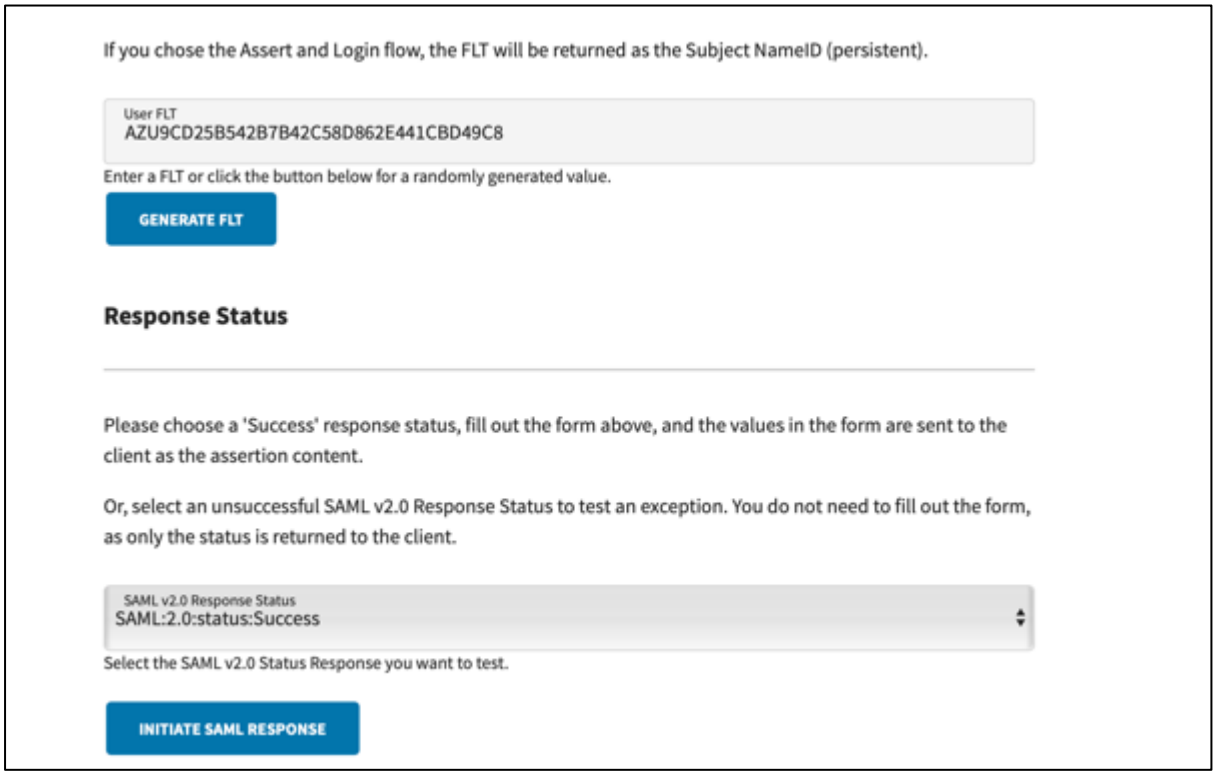


On this page, enter the details you require for the test account, such as the name, DOB and place of birth. Further down the page, the FLT that will be associated with the new account details is shown.

Note: You will need to generate and record the FLT to be able to log in with this account later.

The Digital Health Identity service's INT environment connects to the UAT system for the NHI. You can therefore enter test data that corresponds with a record in UAT if you want your account to bind to a specific NHI number.

Once you have entered your test data, you can record the FLT and initiate the response back from MTS.



The last part of the MTS page enables you to control the response status returned to your application. Typically, you will want a successful login, as shown in the screenshot above. However, you can also simulate a RealMe failure by selecting a response status from the dropdown on the page. This is ideal when testing login failures within your application.

Sign-in with RealMe

Once you have successfully created a RealMe account you can login to the newly created **My Health Account** or **My Health Account Workforce** by selecting the sign-in with RealMe option. This will take you through to the MTS login page as shown below.

Here, you can enter the previously saved FLT to complete the sign in process to your test account. Again, you have the option to set a different response status to simulate a RealMe login failure.

RealMe MTS Data Retention

You should note that MTS will not retain any of the information you enter, as MTS effectively echoes back whatever you enter in the form. You therefore cannot use a previously setup RealMe MTS account to create a new **My Health Account** or **Workforce** account, as the data attributes will not be available.

Where a new **My Health Account** or **My Health Account Workforce** is required, you must select to sign-up for a RealMe account as part of the process.

Onboarding | Compliance & Certification

Privacy Impact Assessment (PIA)

Applications that integrate with **My Health Account** are expected to undertake a privacy impact assessment that analyses their product and processes against the requirements of the Privacy Act 2020 and the Health Information Privacy Code 2020. The Office of the Privacy Commissioner has more information on completing a privacy impact assessment.

Elements we expect to see in an approved PIA:

1. How personal information will be stored and displayed.
2. How access to personal information and health information will be controlled using the attributes we provide such as NHI number, HPI number (CPN) and confidence level.
3. A privacy analysis that shows that your application conforms to the requirements of the Privacy Act 2020 and the Health Information Privacy Code 2020.

In accordance HISO 10046-2022 Te Whatu Ora requires all applications that read or write health information and/or personal information to have:

- Identified the user with reasonable care.
- Protected private information.
- Implemented application design in accordance with privacy by design.

Application Certification & Accreditation

Government Agency (Internal/External)

All government-held information requires appropriate protection. Government agencies must consider the nature and value of the information they're managing, and the measures needed to protect it. As such, Te Whatu Ora requires all integrating applications from a government agency to have gone through a Certification & Accreditation process.

Why?

Certification and Accreditation is a fundamental governance and assurance process, designed to provide the Board, Chief Executive and senior executives confidence that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met. It is essential for credible and effective information assurance governance.

The certification authority MUST accept that the controls are appropriate, effective and comply with the Protective Security Requirements (PSR) and, in particular, the relevant NZISM components, in order to award certification.

- Te Whatu Ora integrators should provide a snapshot of the recommendations from Defender for Cloud against their project/application resources.

Non-Government Agency

Security assurance is grounds for confidence that the three security goals (integrity, availability, confidentiality) have been adequately met by a specific implementation and are

effective in their application. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

We summarise the key processes that should be part of every security assurance program as follows:

1. Security Hardening – Design.
2. Security Testing – Test.
3. Vulnerability/Risk Management – Assess.

As a third party looking to integrate with Te Whatu Ora, we require evidence of security assurance activities carried out by the integrating party. In most cases, we will require evidence of an independent security test at minimum. The level of evidence and collateral required may vary depending on the nature of the information involved. As a government agency, Te Whatu Ora must consider the nature and value of the information being managed and so, the direction/decision relating to security assurance is ultimately at the discretion of Te Whatu Ora alone.

If you require guidance on the assurance process, you may refer to the following process developed by the Department of Internal Affairs. Agencies/organisations are free to use their own established risk assessment processes instead if preferred.

- Risk Assessment Process: Information Security
- Assurance for Low-Risk Sites

Baseline Questions

Security Questions
Have you completed a Security Risk assessment of your solution? If so, please provide details.
Have you completed a Privacy Impact Assessment of your solution? If so, please provide details.
Does your Software comply with the OWASP Top 10? If so, please provide details.
Has your code had an independent security review and penetration test conducted? If so, please provide details of the report.

If a security assessment is not available, and the solution is determined to carry a Low risk based on initial technical assessment and PIA, please complete the following:

Low Risk Solution
Do you have an Information Security Policy (Which includes the ongoing management and destruction of assets and media)?
What measures do you have in place to ensure the physical security of your environment? Please provide details.
Are you confident that any issues identified during testing of your solutions are addressed appropriately and in line with the risk that they present?
Do you understand and accept the residual risks associated with your solutions?
How do you sign-off on solutions that go into a live production environment using live data?
What type of Security controls do you have in place to protect your systems?
When dealing with PII information - how is this protected at rest and in transit?
How do you currently ensure testing demonstrates that security controls are effective, and vulnerabilities and defects are minimised?
Do you regularly patch and upgrade operating systems and application software?

If a security assessment is not available, and the solution is determined to carry a Medium risk based on initial technical assessment and PIA, please complete the following:

Medium Risk Solution
Does your organisation have a Governing Body that has established expected Security Guidelines, and do you comply with these guidelines?
Do all employees have security expectations and non-disclosure agreements in their contracts for employment and do they receive Security Awareness Training?
Are all new employees, temporary staff and contractors appropriately screened in relation to their appointed task?
Do you have a policy for the management of the access, management and sharing of sensitive information?
Do you use any Cloud Computing or outsourced processing?
Have you considered/identified any sovereignty issues associated with the location of the head office or the storage/processing site and the current health information security policy?
Can you confirm that any proposed provider protects New Zealand health information appropriately, such as the provision/enabling of NZISM approved encryption of data at rest and in transit?
Do you have appropriate backups, recovery and BCP plans for your systems?
What Anti-Malware and Anti-Virus software do you use (Including the version) and how often are scans activated? Please provide details (including what is used for user devices vs. Servers etc.).
Do you maintain sufficient separation between Development, Test and Production environments?
Are user's access rights regularly reviewed and amended according to changes of role and/or accountabilities within the organisation?
Do you use appropriate encryption standards when exchanging sensitive information?

Do you have up to date system documentation?
Which of the following controls do you apply when developing software (whether internal or outsourced)? □ Established code libraries, algorithms, and routines to implement security features and counter threats. □ Source code control. □ Technical reviews of code. □ Testing - unit, integration, compliance and user acceptance. □ Documentation - for user, business and technical audiences. □ Change control and version management. □ Deployment mechanisms, may include CI/CD. □ None of the above.
Do you have an incident management process and a way of learning from incidents? Do you complete post incident reviews?
Are users working to a security policy when working off-site, at home or in other public areas?

Privacy and Terms of Use Information for Consumers

Before you integrate with our production service you will be asked to provide a link to the published Privacy Statement and Terms of Use for your application.

Links to these documents will be presented to the user in 3 scenarios:

1. When someone first logs in or signs up to your application using their **My Health Account** or **My Health Account Workforce**.
2. When someone views the list of applications they have previously consented to sharing their details with. When your application is in the list, the links that you supply will be included should the user wish to read them.
3. When someone is renewing consent, after:
    a. They add new information to their account.
    b. The claims list requested by your application is updated.
    c. The description of how your application uses someone's data changes.

This is intended to empower users to make informed choices when consenting to sharing their information with you.

Onboarding | Commercials & Terms of Use

Before we provide access to our production service, commercial and Terms of Use agreements must be agreed and signed between both parties. This may vary depending on your organisation type.

Depending on your organisation type and the nature of the commercial engagement, a **Commercial Contract** and or a **Memorandum of Understanding (MOU)** (for government agencies) will be established and agreed between both parties.

A **Memorandum of Understanding (MOU)** will define the principles and objectives both parties aim to achieve, their ongoing relationship and, in general terms, how the parties intend to work jointly.

Or

A **Commercial Contract** will define the commercial relationship and terms and conditions between both parties and will incorporate a standard **Terms of Use** which will define the rules and guidelines regarding how the Digital Identity and **My Health Account** Service will be used.

Onboarding | Production Readiness

Once you have completed your testing and have compliance and accreditation approval, you are ready to integrate with the production service.

When you have a confirmed timeframe for your production release, we will schedule our support team to ensure your go-live goes smoothly.

To do this, we will need the following information from you:

- ✓ Planned time for your production release.
- ✓ The `redirect_uri` URL for your production app.
- ✓ Contact number for your helpdesk and their hours of operation.

Note: The helpdesk number is to ensure we can refer any queries received at our contact centre through to your team, in the event that the support call does not relate to the Digital Identity Service.

Once we have this information, we will provide you with the necessary details to connect through to production.

This includes:

- ✓ Production URL.
- ✓ Client ID.
- ✓ Client Secret.

During the initial days of your integration with the production service we will monitor your account activity closely, in order to alert you of any issues that may arise.

Use Stage

The objective of the **Use Stage** is to provision service support and continuity.

This section provides an overview of the support definitions, service levels, contacts, and processes for our service.

Post-Onboarding Implementation Support

Operational support will be provided postproduction onboarding of your application. Service level agreements will be defined in the commercial agreements established and agreed.

For support specific to the onboarding process please contact:
DHI.Integration@health.govt.nz.

Ongoing Operational Support

What support is provided for our product and service?

The Digital Health Identity team provides the following operational support:

- User Support | for users who are having issues with accessing or creating their **My Health Account** or **My Health Account Workforce**.
- Technical Support | for integrators who are experiencing technical issues that are impacting their application and user service.

While we do not provide support specific to your application, we do expect that users will mistakenly contact us when seeking support for your application and vice versa. Processes will be agreed and defined to manage this scenario.

Who to contact for User support?

If a **My Health Account** or **My Health Account Workforce** user has an issue during **business hours**, please direct them to contact the Contact Centre:

Who to contact	Hours	Contact Information
Contact Centre	Mon - Fri : 08:00 to 17:00 Sat - Sun : 10:00 to 15:00 (Closed on public holidays)	0800 222 478 support@identity.health.nz

Who to contact for Technical Support?

If you have a problem during **business hours**, please contact the Service Centre and the Digital Identity Operations Team.

If you have a problem **after hours** that relates to Production, please contact Solnet.

Any identified defect should be advised to the Operations Lead (di.operations@health.govt.nz) for immediate review and triage.

Who to contact	Hours	Contact Information
Service Centre	Mon - Fri : 07:30 to 17:30	IT_servicedesk@health.govt.nz 04 816 2011
Digital Identity Operations Team	Mon - Fri : 08:30 to 17:00 (Closed on public holidays)	di.operations@health.govt.nz
SOLNET	After Hours support only	support@solnet.co.nz 0800 765 638

When is Technical Support available?

The Digital Health Identity Service Production environment is supported 24/7 and the Integration Environment is supported during standard business hours for incidents. The resolution times for incidents are outlined in the table below:

SLAs / SLTs for Production Environment Incidents (Standard Business Hours):

Priority	Support Hours	Resolution
P1	Standard Business Hours	4 hours
P2		8 hours
P3		24 hours

SLAs / SLTs for Production Environment Incidents (After-Hours):

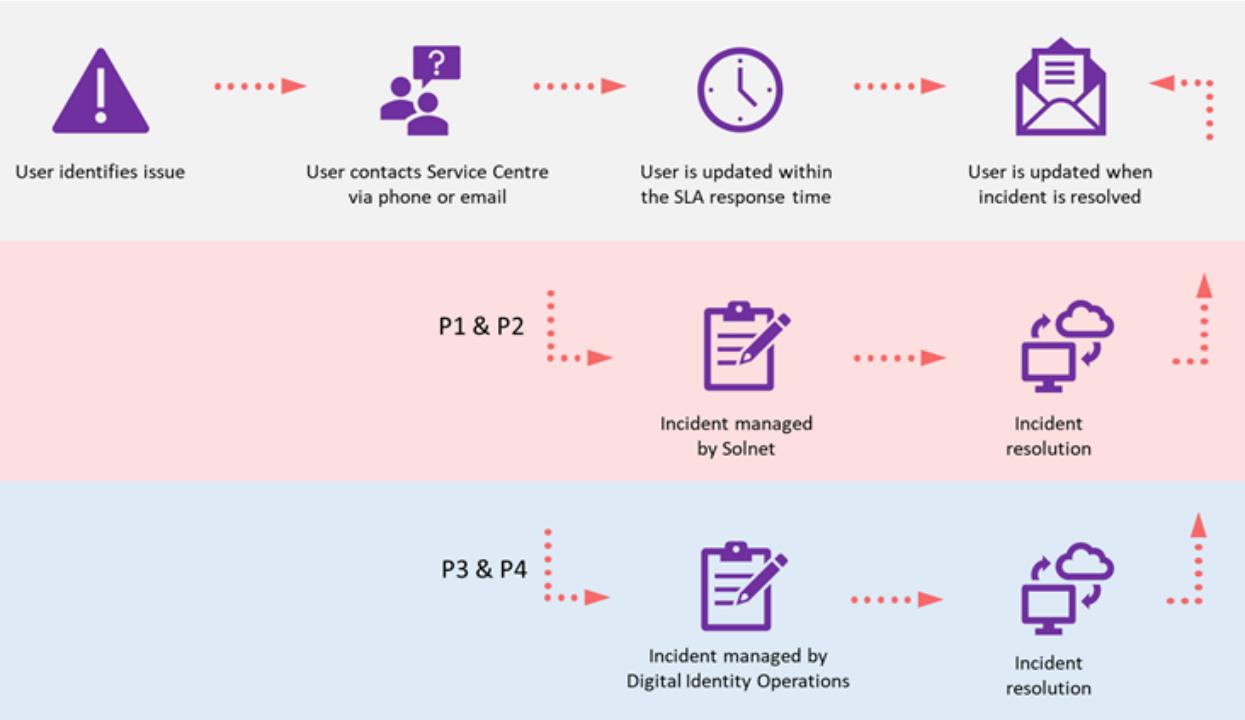
Priority	Support Hours	Resolution
P1	After Hours	Next Business Day
P2		Next Business Day

SLAs / SLTs for Integration Environment Incidents (Standard Business Hours Only):

Priority	Support Hours	Resolution
P1	Standard Business Hours	4 hours
P2		8 hours
P3		24 hours

How are incidents managed?

Once an incident has been identified, it will be triaged and managed by our Operations Manager and, where required, our primary incident response partner, Solnet. Our incidents response team are responsible for managing P1 and P2 incidents 24/7.



How are planned and unplanned service outages communicated?

In the event of a planned outage to our Integration or Production service, you will be notified in advance by our Operations team.

In the event of an unplanned outage to our service, you will be notified promptly by our Operations team with an overview of the service components impacted and the expected resolution time.

Priority definitions

Priority	Priority Definition
1	Critical. Daily business operations cannot take place. Major components of an agreed service (or services) cannot be delivered as required by the department.
	An outage resulting in an interruption to a business-critical service or services.
	Will affect an entire business unit, or multiple users across multiple business units, or multiple sector organisations.
	Any security issue which is likely to put daily business operations at risk.
2	Daily business operations are substantially slowed or reduced.
	An Outage resulting in an interruption to an agreed service.

	Multiple users will usually be affected.
	An individual user with an urgent problem likely to have a substantial negative impact on the business as a whole.
	Management escalation - urgent attention requested. Might otherwise be classified as a P3.
	Any security issue which has the potential to put daily business operations at risk.
3	Minor interruption to an agreed service.
	Some users (i.e., 2-3 users) are affected.
	Likely to have a significant impact on the user's ability to do their job, but unlikely to affect overall business operations.

Extend Stage

The objective of the **Extend Stage** is to support and enable service improvements and ongoing accreditation and compliance.

New Service Features & Enhancements

The Product Delivery team work on releasing new features and enhancements of **My Health Account** to ensure the Digital Health Identity Service is responding to the needs of its consumers.

How to provide feedback, suggestions, and enhancements

Product feedback, questions, or enhancement suggestions about the Digital Health Identity service are welcomed by the team. These should be directed to the Product Delivery team (DHI.Integration@health.govt.nz).

These will be reviewed, prioritised, and scheduled for delivery prior to each quarterly period. The Product Delivery team will communicate when features are planned for delivery to the relevant parties.

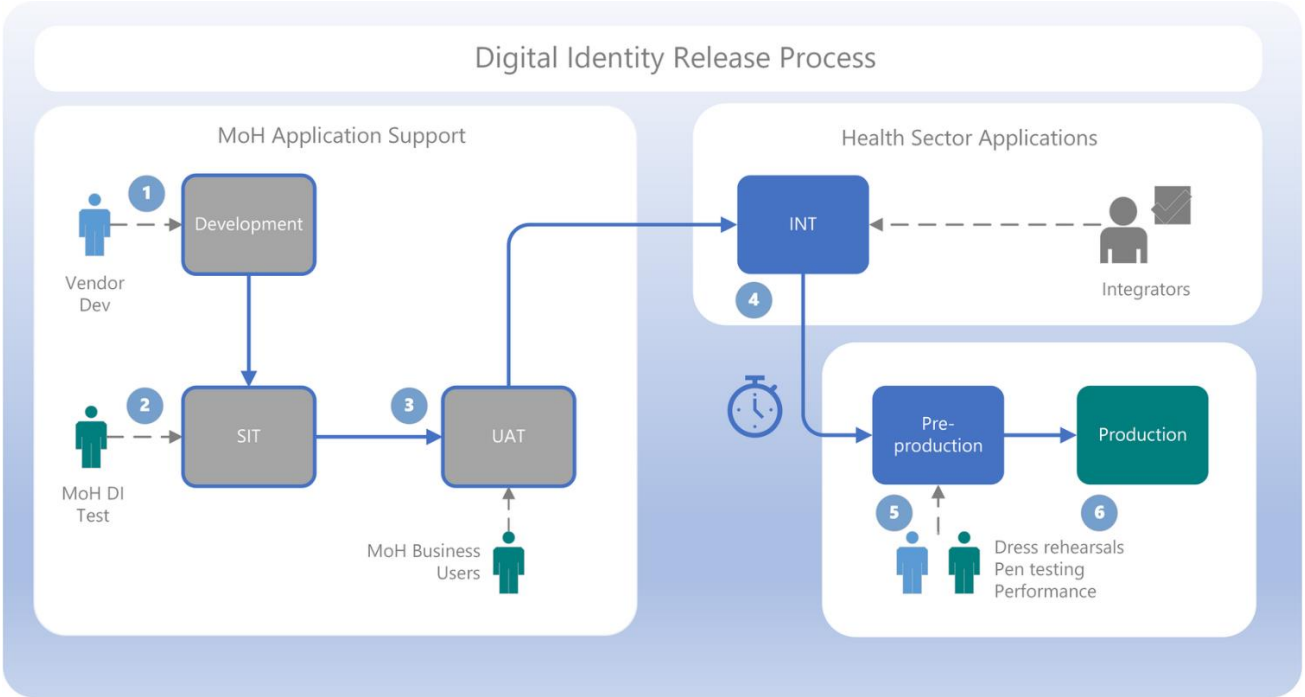
New Features and Enhancements

When a new feature or enhancement is developed it will follow the Standard release process as outlined below. Affected parties will be advised of up-and-coming feature releases when releases are available for testing within the Integration environment and the planned production implementation delivery dates.

Planned Releases

Standard Release Process

The diagram below illustrates the standard release path:



Release Cadence and Calendar

The current release cadence for changes is fortnightly. Thursday first and third week of each month. You will be notified of any upcoming releases.

Exit Stage

The objective of the **Exit Stage** is to support and enable a smooth transition when offboarding from our service.

This section provides an overview of the processes and steps required to successfully offboard from our service.

Offboarding Request Form

If you wish to stop using the Digital Health Identity Service, you will need to complete an offboarding form for each application that you intend to offboard from the Digital Identity Service.

Offboarding Request Form

The form requests the following information:

1.	**Company / Agency Name:**	
2.	**Application Name:**	
3.	**Contact Person:**	
4.	**Contact Details:** • Email address • Contact phone number	
5.	**Preferred date of offboarding from Service:**	
6.	**Reason for Offboarding:**	

Verify your Request

The offboarding team will be in contact to review and verify your request.

Once your request has been processed, your permissions to the service and all associated notification channels will cease.

Close out Commercial Agreements

Once offboarding is complete, commercial agreements will be terminated between both parties.