Services Australia

myGov User Guides

Digital Engagement Branch

myGov Member Service On-boarding
Technical Guide

Australian Government

Services Australia

Contents

1. Introduction

1.1 Purpose

The purpose of this document is to provide assistance to the prospective Member Service architects and technical experts in implementing solutions to enable Member Service integration with myGov.

The questionnaire provided to the onboarding Member Service which helps facilitate the onboarding process.

1.2 Audience

The target audience for this document is the technical lead or architect who is leading the onboarding process for the Member Service.

1.3 Scope

The scope of this document is to provide:

- An overview of the myGov capabilities and functions

- A questionnaire to onboarding Member Services to gain a high-level of understanding of some of the technical requirements to onboard.

- High-level technical activities required for integration

- A list of technical documentation available from myGov

1.4 Out of Scope

- This document does not include detailed technical information. Appendix 3 specifies available references. Further information may be made available on request.

1.5 Assumptions

It is assumed that:

- The prospective Member Service and myGov have agreed on the engagement scope; and

- The prospective Member Service is familiar with the OIDC and has the required enabling technologies.

- All staff working on the onboarding must;

o   Have security clearances

o   Be covered by appropriate contract / confidentiality agreements

1.6   Terms and Acronyms

This table provides a list of all acronyms and any terms used within this document that will require explanation or expansion

Term	Definition
Member Service	The Government Agency or Government Agency Program participating in the myGov program
myGov Capability	A myGov capability offered as a Service to Member Services
Engagement scope	List of myGov Capabilities the prospective Member Service plans to utilise
Account Linking	Process associating a customer's myGov and Member Service accounts
Pairwise Identifier	Shared common identifier allowing a Member Service and myGov to identify associated customer accounts without storing primary account identifiers from the other system. Other documents may refer to it as a Link ID or MBUN (Meaningless But Unique Number). Clarification by example: myGov identifies customer accounts by username or email. Member Service MS1 identifies customer's account by internally issued Customer Identification Number (CIN). myGov systems would not store CINs and/or other MS1 data and MS1 systems would not store myGov usernames and emails. Both parties would only store Member Service Link Identifier.

Term	Definition
Core Data	Customer's first name, last name and date of birth
Profile Member Service	A Member Service that is authorised to provide Core Data to myGov
OIDC	OpenID Connect
Service Consumer	In context of the current document, Service Consumer is a system component responsible for communicating data to externally exposed myGov Web Service and processing data returned by externally exposed myGov Web Service

1.7 Status

This document in draft

2.   Technical process for integrating with mygov

The process for a Member Service to implement integration with one or more myGov Business Services is as follows:

1.   Member Service and Service Australia collaborate to establish which capabilities the Member Service wants to onboard to. A written agreement is established to deliver those chosen capabilities.

2.   The Member Service provides the technical details and artefacts required by myGov in order to provision the Member Service (see Appendix 1 - Member Service on-boarding questionnaire).

3.   myGov provisions the Member Service in the test environment and provides the technical details and artefacts required by the Member Service (e.g. WSDLs, secret credentials, security keys, etc.) to integrate in the test environment (see Appendix 2 – myGov Details).

4.   The Member Service integrates with the myGov Business Service(s) in the test environment.

5.   myGov and the Member Service test the integration in the test environment.

6.   myGov provides the technical details and artefacts required by the Member Service (e.g. WSDLs, secret credentials, security keys, etc.) to integrate in the production environment.

7.   myGov provisions the Member Service in the production environment and the Member Service deploys the integration implementation in the production environment.

3.   myGov Capabilities

myGov Capabilities aim to make it easier for Member Service customers to access Member Services online, while allowing Member Services to leverage whole-of-government capabilities to interact with their customers. The table below provides a high-level description and list of detailed references for each of the myGov Capabilities.

Ref	Service/Function Name	Description	myGov references
1	OIDC Linking and Authentication	myGov implements a Federated Identity model and achieves account linking using pseudonymous identifiers. An Industry standard protocol (Open ID Connect (OIDC)) is used to authenticate users. The following functions may be performed by member services using the OIDC authentication protocol. 1. Account linking 2. Account unlinking 3. User Authentication – Single Sign-On (SSO) Further details can be found in the attached reference documents.	mygov-oidc-dev-guide.pdf

Ref	Service/Function Name	Description	myGov references

2	Update Your Contact Details	The myGov Update Your Contact Details Capability allows customers to update their contact details across participating linked Member Services with a single interaction. To integrate with this capability the following web services should be implemented or consumed by the Member Service. Further details can be found in the attached reference documents
		Web services to be consumed by the Member Service:
		    1. updateCustomerDetailsChangeStatus
		
		Web services to be provided by Member Service:
		    1. notifyCustomerDetailsChange
			myGov system Interface Spec Customer Details Change
			
			myGov TuO WS SIS Customer Details 2.3

3	myGov Inbox	The myGov Inbox Capability allows participating Member Services to send secure messages and electronic correspondence to their customers. To integrate with this capability the following	myGov System Interface Spec Digital Mail myGov Digital Mail v 3.3.pdf

Ref	Service/Function Name	Description	myGov references

		web services should be implemented or consumed by the Member Service. Further details can be found in the attached reference documents
		
		Web services to be consumed by the Member Service:
		   1. publishMessage
		Web services to be provided by Member Service:
		   1. retrieveAttachment
		   2. notifyReadReceipt	

4. Appendices

4.1 Appendix 1 - Member Service on-boarding questionnaire

4.1.1. General Information

The details collected in this section must be provided by any Member Service seeking to integrate with any myGov Capability.

Item	Description	Member Service Value
Member Service official name	myGov uses the Member Services official name for display and internal purposes. Please provide exact text. Note: The Member Service official name may be different from the Department / Agency official name. e.g. Medicare online	
Member Service abbreviation	A short acronym for the Member Service. Must be three to eight characters in length. This acronym will be used in web service interactions between myGov and the Member Service. e.g. MCA, CLK, ATO, DVA	
Member Service Name	myGov uses the Member Services name	

Item	Description	Member Service Value
preference for Publish Message Notification	preference for Publish Message Message Notification. Please provide exact text. Note: The Member Service Nname may be different from the Department / Agency official name. e.g. Medicare online	
Technical Lead's Contact Details	This will be contact details of the technical lead who is coordinating the onboarding.	Name: Email: Phone Number: Job Title:
Capability(ies) being integrated	The capability(ies)that the Member Service plans to integrate.	☐ OIDC Linking and Authentication ☐ Update Your Contact Details ☐ myGov Inbox

4.1.2. General Security Information

The details collected in this section relate to the security profile of the Member Service environments to be white-listed to access myGov services, and the users of those environments. These details must be provided by any Member Service seeking to integrate with any myGov Capability.

Item	Member Service Test Environment	Member Service Production Environment
Who will be accessing the environments?	☐ Staff from other Government Departments ☐ Staff from external companies ☐ Staff from external developers ☐ Other (specify) ………………………………………………	☐ Staff from other Government Departments ☐ Staff from external companies ☐ Staff from external developers ☐ Other (specify) ………………………………………………
What will the external users be doing?	☐ Development ☐ Testing ☐ Training ☐ Demonstrations ☐ Other (specify) ………………………………………………	☐ Development ☐ Testing ☐ Training ☐ Demonstrations ☐ Other (specify) ………………………………………………

Item	Member Service Test Environment	Member Service Production Environment
Do all staff members working on the onboarding have contract/confidentiality agreements?	☐ Yes ☐ No (answering no, prohibits staff from working on the onboarding) Specify ………………………………………………	☐ Yes ☐ No Specify …………………………………………………
Do users have security clearances?	☐ Yes ☐ No (answering no, prohibits staff from working on the onboarding) Specify…………………………………………	☐ Yes ☐ No Specify……………………………………………
Has external environment been accredited?	☐ No accreditation ☐ Meets Information Security Manual requirements ☐ Other (specify) ……………………………………..	☐ No Accreditation ☐ Meets Information Security Manual requirements ☐ Other (Specify) ……………………………………..
Will access be logged and monitored?	☐ Logged and monitored ☐ Logged only ☐ Other (specify) ……………………………………	☐ Logged and monitored ☐ Logged only ☐ Other (specify) ……………………………………

Item	Member Service Test Environment	Member Service Production Environment
How long is access required?	☐ 6 Months ☐ 12 Months	Specify...

4.1.3.   OIDC Authentication/Linking Member Service Details

The details collected in this section relate to the myGov OIDC Authentication/Linking Capability. These details must be provided by any Member Service seeking to integrate with that myGov Capability.

Item	Description	Member Service Test Environment	Member Service Production Environment Value
OIDC Redirect URI's	Per the OIDC Spec – the OIDC authorization_code will be redirected to this URL. myGov supports multiple redirect_uri's for a given client_id.	List of valid URLs:	List of valid URLs:
OIDC Initiation URL's	myGov has 3 URL's that it sends the customer to. At each one – myGov expects to initiate an OIDC SSO – but with different effects for each. These are the linking, unlinking and SSO endpoints. The "linking" endpoint will be presented on the services page, when the customer is not linked to the member service. When this URL is accessed – the member service should perform an	Linking URL: SSO URL: Unlinking URL:	Linking URL: SSO URL: Unlinking URL:

Item	Description	Member Service Test Environment	Member Service Production Environment Value
	IDP-initiated OIDC SSO and then funnel the customer into a "linking" flow. The "SSO" endpoint will only be shown when the member service is linked (on both the myGov dashboard and the Services page). When it is accessed – the member service should perform an IDP-initiated OIDC SSO. The "unlinking" endpoint will be presented as the "unlink" button on the services page. When this URL is accessed – the member service should perform an IDP-initiated OIDC SSO to identify the user. It should then remove the references to the link within the member service record, call the myGov Unlink API, and then return the customer to the return_uri.		

Item	Description	Member Service Test Environment	Member Service Production Environment Value
OIDC JWKS endpoint	If you are using private_key_jwt for security (which is recommended) – you need to supply the URL to myGov. Additionally – you need to allow myGov to access your JWK. And if you use a non-public CA for your TLS encryption – supply the relevant chain of trust.	☐ private_key_jwt ☐ client_secret (less secure) If JWKS – supply the URL:	☐ private_key_jwt ☐ client_secret (less secure) If JWKS – supply the URL:
Notify Account Change service Endpoint (Mandatory for mobile apps)	Endpoint for myGov to call the member service implementation of the Notify Account Change service.	Hostname: IP Address:	Hostname: IP Address:

4.1.4. Update Your Contact Details Member Service Details

The details collected in this section relate to the myGov Update Your Contact Details Business Service. These details must be provided by any Member Service seeking to integrate with that myGov Business Service.

Item	Description	Member Service Test Environment Value	Member Service Production Environment Value
Notify Customer Details Change service Endpoint	Endpoint for myGov to call the Member Service implementation of the notify customer details change service.	Hostname: IP Address:	Hostname: IP Address:
IP Addresses to be white-listed for consuming the Update Customer Details Change Status service	Member Service gateway / proxy IP address(es) for myGov to whitelist so that the Member Service system can call the required service.	IP Address(es):	IP Address(es):

4.1.5. Digital Mail Member Service Details

The details collected in this section relate to the myGov Digital Mail Business Service. These details must be provided by any Member Service seeking to integrate with that myGov Business Service.

Item	Description	Member Service Test Environment Value	Member Service Production Environment Value
Default Read Receipt Settings	A flag indicating a default value for whether a read receipt should be sent to the Member Service when a user reads a message sent by the Member Service. If this is "true" then by default a read receipt will be sent the first time a user reads each message sent by the Member Service. Otherwise by default a read receipt will not be sent. This default setting can be overridden by the	True/False	True/False

Item	Description	Member Service Test Environment Value	Member Service Production Environment Value
	Member Service on a per message basis.		
Retrieve Attachment service endpoint	Endpoint for myGov to call the Member Service implementation of the Retrieve Attachment service.	Hostname: IP Address:	Hostname: IP Address:
Notify Read Receipt service Endpoint	Endpoint for myGov to call the Member Service implementation of the Notify Read Receipt service.	Hostname: IP Address:	Hostname: IP Address:
IP Addresses to be	Member Service gateway / proxy IP address(es) for	IP Address(es):	IP Address(es):

Item	Description	Member Service Test Environment Value	Member Service Production Environment Value
white-listed for consuming the Publish Message service	myGov to whitelist so that the Member Service system can call the required service.		

4.2   Appendix 2 – myGov Details

After receiving the Member Service integration details from Appendix 1 - Member Service on-boarding questionnaire, myGov will generate a starting pack that includes the following information and artefacts.

Item	Description	Status
Test End points	Test Environment URLs for Authentication, Linking, and web services.	☐
Test Message Signing Certificate	DHS-issued X.509 certificate for Message Body signing	☐
Production End points	Production Environment URLs for Authentication, Linking, and web services.	☐
Production Message Signing Certificate	DHS-issued X.509 certificate for Message Body signing	☐

4.3   Appendix 3 - Technical documentation available from myGov

The table below presents detailed technical references available from myGov on request.

Ref.	Document Description	Document Name
[DHSEXTWSPROFv108]	DHS External Web Services Profile	references/standards/DHS.External.Web.Services.Profile.v1.08.pdf
[MGVAUTHPROTv14]	myGov Authentication Hub Protocol v1.4	references/standards/Reliance Framework Authentication Hub Protocol1.4.pdf
[MGVEXTWSPROFv09]	myGov External Web Services Profile v0.9	references/standards/Reliance Framework.Web.Services.Profile.v0.9.pdf
[MGVOIDCUGv10009]	myGov OIDC OAuth Developers Guide	references/OIDC/myGov Auth HUB - Developers Guide to OAuth OIDC v1.00.09.pdf
[MGVOIDCCLv10005]	myGov OIDC OAuth Metadata Client Checklist	references/OIDC/myGov Auth Hub Metadata for OAuth and OIDC clients v1.0.xlsx

Ref.	Document Description	Document Name
[MGVTUOSISv20]	myGov System Interface Spec Customer Details Change	references/TuO/myGov.TuO.System.Interface.Spec.v2.0.pdf
[MGVTUOWSDLv20150613]	myGov TuO Update Customer Details Change Status WSDL pack v20150613	references/TuO/v20150613.mygov.cd.ucdcs.memberservice.soap12.zip
[MGVTUOWSDLv20160305]	myGov TuO Notify Customer Details Change WSDL pack v20160305	references/TuO/v20160305.mygov.cd.ncdc.memberservice.soap12.zip9
[MGVDMISISv32]	myGov System Interface Spec Digital Mail	references/DigiMail/mygov.digitalmail.soap.sis.3.2 - External.pdf

Ref.	Document Description	Document Name
[MGVDMIWSDLv2013 0907]	myGov Digital Mail Publish Message WSDL pack v20130907	references/DigiMail/v20130907.mygov.inbox.publishmessage.virtual.soap12.zip
[MGVDMIWSDLv2013 0907]	myGov Digital Mail Retrieve Attachment WSDL pack v20130907	references/DigiMail/v20130907.mygov.inbox.retrieveattachment.memberservice.soap12.zip