PRESCRIPTION SEARCH SUPPORT

IAM Integration

This document is a manual for testing into the Prescription Search Support project. It provides guidelines and instructions to ensure seamless participation in the project.

Contact: integration-support@ehealth.fgov.be

Smals ICT for society

RIZIV - INAMI

eHealth

1. Contents

2. Document version

Version	Status	Date	Author	Description
1.0	Final	04/03/26	Smals	Initial version
1.1	Draft	20/03/26	Smals	Add M2M

3. Authenticate as an Individual Healthcare Provider using IAM Healthcare

This section covers the token exchange flow for individual healthcare providers accessing PSS. The scope used is iam:authz and the audience is nihdi-pss-fhir-hcp.

3.1. Scenario 1 — Token exchange request contains required audience

Description	
Description	Verify that a token exchange request with the correct audience parameter for an individual healthcare provider is accepted by IAM Healthcare without validation errors.

Specifications	
Given	I have a valid subject_token (access token) and a valid client_id
When	I perform a token exchange via POST https://api-acpt.ehealth.fgov.be/auth/realms/healthcare/protocol/openid-connect/token With parameters: • requested_token_type=urn:ietf:params:oauth:token-type:access_token • grant_type=urn:ietf:params:oauth:grant-type:token-exchange • subject_token={access_token} • subject_token_type=urn:ietf:params:oauth:token-type:access_token • client_id={client_id} • audience=nihdi-pss-fhir-hcp
Then	→ The request is accepted by IAM → No validation error occurs due to a missing or incorrect audience

3.2. Scenario 2 — Token exchange response contains correct access token claims

Description	
Description	Verify that the token returned by IAM after a successful exchange for an individual HCP contains the required claims: correct audience (nihdi-pss-fhir-hcp) and scope (iam:authz).

Specifications	
Given	I perform a token exchange with audience=nihdi-pss-fhir-hcp
When	IAM returns a response to the token exchange request
Then	→ HTTP status 200 OK is returned → Response contains a non-empty access_token → token_type = "bearer" → issued_token_type = "urn:ietf:params:oauth:token-type:access_token" → Decoded access_token contains aud including nihdi-pss-fhir-hcp → Decoded access_token contains scope including iam:authz

3.3. Scenario 3 — Get support parameters works with valid exchanged token

Description	
Description	Verify end-to-end that a valid exchanged access token (audience=nihdi-pss-fhir-hcp, scope= iam:authz) successfully authorizes access to the PSS 'Get Support Parameters' endpoint, confirming the complete IAM token exchange flow is operational for individual HCPs.

Specifications	
Given	I have a valid exchanged access_token containing aud=nihdi-pss-fhir-hcp and scope= iam:authz
When	I call the PSS endpoint Get support parameters I send a payload containing a clinical code (ICPC-2, code R21)
Then	→ The PSS service returns HTTP 200 OK → The IAM Token Exchange flow and audience configuration are confirmed correct → PSS is confirmed accessible for individual healthcare providers

4. Authenticate as an Organization using M2M

This section covers the M2M (Machine-to-Machine) client credentials flow for organizations integrating with PSS. The M2M client requests a token directly from the IAM M2M realm using a signed JWT client assertion (client credentials flow). Authentication is performed by signing a JWT with the client's private key, which is registered with the M2M realm.

4.1. Scenario 1 — Direct M2M token request is accepted by IAM M2M realm

Description	
Description	Verify that an M2M client credentials token request using the correct realm, scope, and a signed JWT client assertion is accepted by IAM and returns a valid PSS access token. No token exchange is involved.

Specifications	
Given	I have a valid M2M client_id and a signing certificate registered with the PSS M2M realm

When	I perform a token request via POST https://api-acpt.ehealth.fgov.be/auth/realms/M2M/protocol/openid-connect/token
	With parameters:
	• grant_type=client_credentials
	• client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer
	• client_assertion={signed JWT}, signed with the client's private key containing:
	  ○ iss = {client_id}
	  ○ sub = {client_id}
	  ○ aud = https://api-acpt.ehealth.fgov.be/auth/realms/M2M
	• scope=openid iam:authz nihdi:pss

Then	→ The request is accepted by IAM M2M realm → No authentication error occurs → A valid access token is returned

4.2. Scenario 2 — M2M token response contains correct claims

Description	
Description	Verify that the token returned by the IAM M2M realm contains the required claims: iss from M2M realm, aud including nihdi-pss-api, scope including nihdi:pss, role pss, and a userProfile with organization information.

Specifications	
Given	I have successfully obtained a token from the IAM M2M realm using client credentials
When	I decode the returned access_token JWT
Then	→ iss = https://api-acpt.ehealth.fgov.be/auth/realms/M2M → aud includes nihdi-pss-api → scope includes nihdi:pss → resource_access.nihdi-pss-api.roles contains pss → userProfile contains the organization nihdi and name → token_type = Bearer

4.3. Scenario 3 — Get support parameters works with valid M2M token

Description	
Description	Verify end-to-end that a valid M2M access token (aud: nihdi-pss-api, scope: nihdi:pss, roles: pss) successfully authorizes access to the PSS Get Support Parameters endpoint, confirming the complete M2M client credentials flow is operational.

Specifications	
Given	I have a valid M2M access_token issued from the M2M realm containing aud: nihdi-pss-api, scope: nihdi:pss, and roles: pss
When	I call the PSS endpoint Get support parameters from an M2M integration client I send a payload containing a clinical code (ICPC-2, code R21)
Then	→ The PSS service returns HTTP 200 OK → The M2M client credentials flow and audience configuration are confirmed correct → PSS is confirmed accessible for M2M organization-level integrations