Integration Guide for VITALINK

1. Recommendations and warning

- This document is only applicable for software clients.
- The healthcare actor has a eHealth Certificate in the Production environment.
- The certificate has to use the same identifier as the identifier for IAM Connect (ex hospital is identified by NIHII number and the eHealth Certificate has to be for this NIHII number)

User Group		Section in this document
Organisations	API, M2M realm, Client Credentials Flow	See 2.1.3
Individual Health Care actors (software)	API, Healthcare realm, Authorization code flow	See 2.1.1 or 2.1.2

To use Vitalink through the API, the health care provider must have medical software that has integrated this service.[1]

The Vitalink API is accessible through REST services cfr. cookbooks

https://www.vitalink.be/gebruikers/ik-ben-softwareleverancier

Contents

2. Onboarding client for REST services

2.1 General

In the case of the REST services, it is necessary to request integration using the I.AM Connect forms. [2]

- IAM Connect form:
  Particularity for the Vitalink API: TWO forms are available, you should fill in the one that, according to the explanations in this document, corresponds to your use case.
  - M2M for organisations
    https://www.ehealth.fgov.be/ehealthplatform/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/7398eab4ff8822da3fff64aa359e6ddb76951faa/iam-connect---m2m-client-registration-request-form.pdf
  - Healthcare Realm for individual healthcare actors
    https://www.ehealth.fgov.be/ehealthplatform/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/610181304e16b0afcad704e258d5e6b2f016315b/iam-connect---healthcare-client-registration-request-form.pdf

- Description of user groups:
  It is requested to clearly describe the different user groups and/or organizations that will use your service (e.g. doctors, nurses, group of doctors, proxy, hospitals, etc...). This description should be part of the application email, with the IAM Connect form attached.

---

https://www.ehealth.fgov.be/ehealthplatform/nl/service-i.am-identity-access-management#heading-0
https://www.ehealth.fgov.be/ehealthplatform/fr/service-i.am-identity-access-management

2.1.1 Case of a distributed application (and some webapps)

- The application runs 100% on a user-side client (it is not possible to manage private keys to authenticate the client application).
- The user authenticates himself directly through our IDP and FAS.
- Authorization code flow : PKCE integration.

Elements on the "***I.AM Connect – HealthCare Client registration***" [3] form to complete

- Section 4 General Information / information about your software
  - ***Client ID*** : Client's identifier which, by default, is the name of your company or software.
    - If an IAM Connect client for your company already exists in the healthcare realm, you should try to reuse the existing client (and therefore the client ID).
    - If an IAM Connect client for your company already exists in the healthcare realm, but it is not possible to reuse it, you need to get a new Client ID and add a suffix '-VITALINK' after the company or software name (e.g. softwarename-VITALINK)
  - ***Name***: Client's name
  - ***Description*** *(optional)*: VITALINK if dedicated client
- Section 5.1 URL
  - ***Redirect URI's*** for redirection after a successful log-in are essential.
  - The other fields are optional, see in case of web application.
- Section 5.3 Access Type
  - Tick « ***Public access type*** »
- Section 5.4 Credentials
  - N/A in this case
- Section 5.6 Scopes
  - Mention client scope : ***web-origins, profile, iam:authz, basic, pseudo:api:pseudonymize***

-

2.1.2 Case of a confidential healthcare client (some Web Apps for instance)

- Runs partly on the server side at recognized partner organizations (use of private keys for authentication of the client application itself).
- The user authenticates himself directly through our IDP and FAS.
- Authorization code flow : access token is sent from the client side to the server side of the client.

Elements on the "***I.AM Connect – HealthCare Client registration***" [4] form to complete

- Section 4 General Information / information about your software
  - ***Client ID*** : Client's identifier, which by default, is the name of your company or software.
    - If an IAM Connect client for your company already exists in the healthcare realm, you should try to reuse the existing client (and therefore the client ID).
    - If an IAM Connect client for your company already exists in the healthcare realm but it is not possible to reuse it, you need a new Client ID and add a suffix '-VITALINK' after the company or software name (e.g. softwarename-VITALINK).
  - ***Name***: Client's name
  - ***Description*** (optional): VITALINK if dedicated client
- Section 5.1 URL (of the Web App concerned)
  - ***Redirect URI's*** for redirection to your application after a successful log-in are essential.
  - The **Root / Base URL** of the Web App.
- - Section 5.3 Access Type
  - Tick « ***Confidential access type*** »

- Section 5.4 Credentials
  - JWKS information of the ETEE certificate for the JWKS URL :
    - ***Identifier*** : identifier of the client's identity (NIHII or CBE or EHP number)
    - ***Type*** : type of identifier(e.g.: EHP, CBE, NIHII-HOSPITAL,…)
    - ***Applicationidentifier*** (optional): Application ID for this identifier.

      Element to determine the institution's certificate used on the basis of the Application ID of the eHealth certificate. If your used certificate does not contain an application ID, leave this field blank. Only applicable if you have more than one set of certificats.
- Section 5.6 Scopes
  - Mention client scope : **web-origins, profile, iam:authz, basic, pseudo:api:pseudonymize**

[4] ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-iam-identity-access-management***

2.1.3 Case of a confidential client – Machine to machine (Organization)

- Runs 100% on the server side at recognised partner organizations.
- NO authentication of end-users.
- Client Credentials : access token is sent directly to the client after authentication (NOT an end-user).

Elements on the "***I.AM Connect – M2M Client registration***" [5] form to complete

- Section 4 General Information / information about your software
  - ***Client ID*** : Identifier of the organization, which is different depending on the type of organization:
    - For a company: cbe-XXXXXXXXXX where XXXXXXXXXX is the CBE identifier.
    - For a health care institution: nihdi-<type>-XXXXXXXX where the type is the type of institution (e.g. hospital, lab, guard post,…) and XXXXXXXX is the NIHII identifier.
    - For an eHealth institution: ehp-XXXXXXXXXX where XXXXXXXXXX is the EHP identifier.
    - *If an IAM Connect client for your organization already exists in the M2M realm, you should try to reuse the existing client (and therefore the client ID).*
    - *If an IAM Connect client for your organization already exists in the M2M realm, but it is not possible to reuse it, you need a new Client ID and add a suffix '-VITALINK' after the company or software name (e.g. softwarename-VITALINK).*
  - ***Name*** : name of the organization.
  - ***Description*** (optional): You can mention the software supplier.
- Section 5.1 Credentials
  - JWKS information of the ETEE certificate for the JWKS URL :
    - ***Identifier*** : identifier of the client's identity (NIHII or CBE or EHP number)
    - ***type*** : type of identifier(e.g.: EHP, CBE, NIHII-HOSPITAL,…).
    - ***applicationidentifier*** (optional): Application ID for this identifier.

      Element to determine the institution's certificate used on the basis of the Application ID of the eHealth certificate. If your used certificate does not contain an application ID, leave this field blank.
- Section 5.2 Scopes
  - Mention client scope : **web-origins, profile, iam:authz, basic, pseudo:api:pseudonymize**

[5] ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-iam-identity-access-management***

3. How to apply for Vitalink onboarding

3.1 REST

For a REST integration, please contact the Integration Support team

- Mail TO : ***integration-support@ehealth.fgov.be***
- Mail title : **Configure Client REST Vitalink for <Client's name> in realm <Name Realm>**
- Mail content : The email should explain the context of the use of the Vitalink services, the purpose, the methods you will use, as well as a volumetric estimate of your project
- Mail attachment : Ad-hoc form (see section 2.1) filled in accurately
- 1 mail per client

3.2 What are the requirements for activation of the VITALINK service in production?

- After configuration in the acceptance environment of the software product
- Perform the tests in the acceptance environment for each software product to demonstrate that the service has been correctly integrated into your software product
- Send a report with the results of these tests to the eHealth Integration Support team, and a copy to the project manager, who will validate your test report.
- If the tests are successfully completed in the acceptance environment, you can onboard your customers for VITALINK in the production environment.

4. Mandatory testing in ACC before onboarding your customers into production (to be carried out by the software supplier)

If, as a software supplier, you have multiple products on the market for which these onboarding processes must be carried out, you must perform theses test for each individual software product.

Which tests must be carried out as a minimum in the acceptance environment before you can onboard your individual customers in the production environment?

Step 1: As a software provider, are you already in production with an application that links to the Vitalink vault?

- If yes: specify which software product and which client ID.
- If no: see below.

Step 2: As a software provider, are you already in acceptance with an application that links to the Vitalink vault?

- If yes:
  - specify which software product and which client ID
  - have you already carried out tests: if yes, specify who carried out which tests and when
  - if no test battery but sporadic test moments, carry out all tests together and specify who carried out which tests and when
- If no: see below for which tests need to be carried out

Objective: to prove that the basic eHealth services used have been implemented correctly

1. Vitalink – test token
- The software supplier must be able to ask a token based on authentication information - The software supplier must be able to use the token delivered by eHealth **Institutions** A software supplier has to test 2 situations: ▪ an access token delivered by IAM Connect ▪ an access token consumed by the client **Individual Healthcare actors** A software supplier has to test 4 situations: ▪ an access token delivered by IAM Connect ▪ an access token consumed by the client ▪ a refresh token delivered by IAM Connect ▪ a refresh token consumed by the client
The software supplier must provide the following information in a document : (to be sent to Integration-support@eHealth.fgov.be) **Institutions** 1. The delivered access token for your client ID (with full query and response).

Individual Healthcare actors

1. The delivered access token for your client ID (with full query and response).
2. The refresh token delivered for your client ID (with full query and response).

Follow-up by integration support :

- for all tests: verify if the claim 'aud' corresponds with the identity of the client in the access token
- if the scope is "pseudo:api:pseudonymize" :

  a. verify the presence of the role "pseudonymize" for "ressource_access.ehealth-pseudo-api" in the access token.

  b. verify the presence of the scope "pseudo:api:pseudonymize" in the claim scope in the access token.

example :

```
"resource_access": {
"ehealth-pseudo-api": {
"roles": [
"pseudonymize"
]
}
"scope": "openid roles pseudo:api:pseudonymize",
```

1. Pseudonymization with “blinded pseudonymization” service

- The participant must be able to create a pseudonym
- Is the ‘multiple’ method applied where needed ?
- Is caching applied for the pseudonym in transit ?
- Use Domain: ehealth_v1 (pseudonym in transit)

If you test the service “blinded pseudonymization” you need to execute a “stand alone test” (1 testcase) and a “volume test” (multiple testcases) (to be able to test the use of the ‘multiple’ method and caching principle)

Cfr:
eHealth Pseudonymization v1 REST Richtlijnen en aanbevelingen v1.2
eHealth Pseudonymisation v1 REST Directives et recommandations v1.2

The software supplier must provide the following information in a document :
(to be sent to Integration-support@eHealth.fgov.be)

- The complete request sent to the Pseudo REST service and the complete response received.

Follow-up by integration support :

- Based on the "X-CorrelationID" retrieved from the response, verify via trafficLog that the call is concluded with a HTTP 200.