**Procédure on-boarding I.AM Connect en vue de l’intégration dans l’environnement FHIR d’un coffre-fort**

V2.0, avril 2024

# Introduction

Dans le cadre de l’échange de données médicales entre les prestataires de soins et les coffres-forts en Belgique (Vitalink en Flandre, RSW en Wallonie et RSB à Bruxelles), il a été opté pour l’usage de messages structurés en FHIR. L’API FHIR a recours au protocole REST comme base pour l’échange de données.

eHealth propose par conséquent d’utiliser I.AM Connect comme processus d’authentification des organisations partenaires qui souhaitent échanger des données avec l’environnement FHIR des coffres-forts dans REST. La procédure décrite dans le présent document doit être suivie par une organisation partenaire pour la configuration d’un client I.AM Connect.

# Procédure d’intégration (on-boarding) du partenaire en vue d’accéder à l’environnement FHIR d’un coffre-fort via I.AM Connect

Un partenaire qui souhaite accéder à un coffre-fort via I.AM. Connect est invité à contacter au préalable ce coffre-fort afin de s’informer sur les conditions particulières qui sont d’application. Ce n’est qu’après cette prise de contact préalable que le partenaire peut démarrer la procédure d’intégration (on-boarding) décrite dans le présent document.

**Le formulaire d’intégration (on-boarding)**

Pour accéder à l’environnement FHIR d’un coffre-fort, il y a lieu d’introduire une demande on-boarding I.AM Connect. Ceci se fait en complétant un des deux formulaires disponibles et en l’envoyant à eHealth Integration Support (voir ci-après dans le document).

Deux formulaires sont disponibles pour la demande d’intégration (on-boarding): un pour la configuration d’un client I.AM Connect dans le Healthcare realm et un autre pour la configuration d’un client I.AM Connect dans le M2M realm.

* [Formulaire pour la configuration d’un client I.AM Connect dans le **Healthcare realm**](https://www.ehealth.fgov.be/ehealthplatform/file/7927d1cb4d8b1f9654ed85a4c9285f9d6df44f47/429f5dbd17cdbcd8fadaac56c8ab4417993c48f8/240328-iam-connect-vault---healthcare-client-registration_form_2_0.docx)  : Utilisez ce formulaire lorsque l’application sera utilisée par des utilisateurs finaux humains qui s’authentifient individuellement. P. ex. : un citoyen ou un médecin qui se connecte à un portail pour consulter des données médicales
* [Formulaire pour la configuration d’un client I.AM Connect dans le **M2M realm**](https://www.ehealth.fgov.be/ehealthplatform/file/7927d1cb4d8b1f9654ed85a4c9285f9d6df44f47/c6593753c2f470d312666f325b1416be48261fba/240327-iam-connect-vault---m2m-client-registration_form_2_0.docx)  : Utilisez ce formulaire lorsque l’application s’annonce comme « application » auprès du coffre-fort (moyennant un certificat eHealth) et qu’aucune donnée relative aux utilisateurs finaux individuels n’est transmise.

Attention : quand un partnenaire souhaite donner accès à des organisations avec un numéro INAMI comme groupe cible (notamment des pharmacies, des hôpitaux ou des groupements d’infirmiers/infirmières), c’est possible uniquement en mode M2M, et donc le formulaire M2M doit être utilisé.

**Les prochaines étapes après avoir complété le formulaire on-boardin**g  
Dès que le partenaire a complété le formulaire d’intégration applicable (Healthcare realm ou M2M realm) et l’a dûment lu, les prochaines étapes sont les suivantes:

* Le partenaire envoie un e-mail à [integration-support@ehealth.fgov.be](mailto:integration-support@ehealth.fgov.be) et met les chefs de projet de eHealth pour I.AM en CC : [peter.laridon@ehealth.fgov.be](mailto:peter.laridon@ehealth.fgov.be) et [stijn.deblieck@ehealth.fgov.be](mailto:stijn.deblieck@ehealth.fgov.be)
* Titre du mail « **Configure I.AM Connect client REST for *<Nom du partenaire>*** »
* Document annexé: formulaire on-boarding dûment rempli de type exact (Healthcare realm ou M2M realm).

## À quelles conditions la configuration peut-elle être mise en production à l’issue des tests d’acceptation?

* Le client est d’abord configuré en acceptation.
* Exécuter les tests requis en acceptation afin de prouver que l’authentification de votre utilisateur se déroule de manière correcte.
* Communiquer les résultats de ces tests par écrit à l’équipe Integration Support et mettre le chef de projet en copie. Ce dernier contrôlera vos tests.

(fin de la procédure)