



I.AM (Identity & Access Management)



Qu'est-ce que le service « Gestion intégrée des utilisateurs et des accès » / I.AM (Identity & Access Management) ?

Le service « Gestion intégrée des utilisateurs et des accès de la plate-forme eHealth » a pour objectif de faciliter l'identification, l'authentification et l'autorisation d'acteurs de soins de santé.

Ce service est constitué de plusieurs composants qui travaillent ensemble pour permettre l'authentification (unique), l'autorisation et la propagation d'identité des utilisateurs de soins de santé, demandant l'accès aux services (hébergés par les organisations de soins de santé et la plate-forme eHealth).

Ces composants sont conformes aux normes internationales pour les communications interentreprises afin de garantir la sécurité et la stabilité et de faciliter l'intégration.

Quelles sont les fonctionnalités du service I.AM ?

Le service « Gestion intégrée des utilisateurs et des accès » offre les fonctionnalités suivantes :

- authentification de l'utilisateur :
 - via certificat eHealth,
 - via une clé numérique supportée par la plate-forme eHealth ;
- identification de l'utilisateur, choix de son profil selon :
 - sa qualité / le type de prestataire de soins individuels (sur base des informations contenues dans la base de données CoBRHA),
 - l'organisation au nom de laquelle il/elle peut agir,



- le mandant pour lequel il/elle peut agir,
- son/ses enfant(s) (sur base des données présentes au Registre national) ;
- authentification unique (single-sign-on) :
 - dans le cadre d'une application web, l'utilisateur ne devra pas se ré-authentifier (sauf si c'est explicitement demandé pour une application),
 - dans le cadre d'un service web, l'utilisateur se crée une session qui peut être utilisée dans le cadre de plusieurs services sur une durée déterminée (durée dépendant du profil de l'utilisateur) ;

Remarque : le single-sign-on IDP (voir [document Identity Provider \(IDP\) renseignant les spécifications techniques](#)) ne doit pas être confondu avec un comportement « isPassive » dans lequel les écrans de l'IDP proposés à l'utilisateur sont limités au strict minimum. Le « isPassive » est uniquement applicable entre les applications web supportant cette fonctionnalité. Cela permet notamment à l'utilisateur de sélectionner un profil dans une application et de ne plus devoir sélectionner de profil s'il passe vers une 2e application (supportant ce profil) protégée par notre I.AM IDP.

- délégation d'accès aux applications :
 - au sein d'une institution
 - il est possible de définir les utilisateurs qui peuvent agir au nom d'une institution pour certaines applications disponibles (voir la [page Comment accéder aux applications ? du portail eSanté](#) pour effectuer la délégation via UserManagement) ;
 - en complément de ces attributions d'application aux utilisateurs, il est possible de définir des fonctions au sein de cette institution (voir la [page Comment accéder aux applications ? du portail eSanté](#) pour effectuer la délégation via Management et Remaph). Cette fonctionnalité ne peut en principe pas être utilisée dans le cadre des services web. Si elle l'est, le projet doit demander à utiliser IDP ;
 - si une personne travaillant dans l'institution peut agir au nom d'un autre utilisateur de cette institution, il est possible de définir un lien hiérarchique entre ces 2 personnes (voir la [page Comment accéder aux applications ? du portail eSanté](#) pour effectuer la délégation via Management et Remaph). Cette fonctionnalité ne peut en principe pas être utilisée dans le cadre des services web. Si elle l'est, le projet doit demander à avoir accès à IDP et AttributeAuthority (qui permet à nos partenaires d'interroger les sources authentiques eHealth). Ce système a été défini afin de scinder les accès applicatifs des accès aux données. L'application est responsable de l'affichage pour le subordonné de la liste de ses supérieurs hiérarchiques, après que ce subordonné a reçu l'autorisation d'accéder à l'application (depuis notre IDP) ;



- d'une institution vers une autre institution (voir la [page Comment accéder aux applications ? du portail eSanté](#) pour effectuer la délégation via l'application web Mandats). Si les types de mandats présents dans l'application ne répondent pas aux attentes de l'application, il est nécessaire de demander la création d'un nouveau type de mandat par l'intermédiaire du [chef de projet eHealth responsable](#) ;
- d'une personne physique à une autre personne physique (voir [la page Comment accéder aux applications ? du portail eSanté](#) pour effectuer la délégation via l'application web Mandats) ;
- accès aux données :
 - certaines données (adresse de contact d'un prestataire de soins, dénomination d'une institution, liste de responsables hiérarchiques d'un subordonné au sein d'une institution...) présentes dans nos sources authentiques (dont [la base de données CoBRHA](#)) sont accessibles via le service web I.AM AA (AttributeAuthority, qui permet à nos partenaires d'interroger les sources authentiques eHealth) ;
 - l'accès à ces données est sécurisé ;
- sécurisation d'application via un mécanisme d'autorisation basée sur l'identité de l'utilisateur.

En pratique

Dépendances, recommandations & avertissements

L'intégration de ce service de base est étroitement liée aux architectures proposées par la plate-forme eHealth.

Dans le cadre du développement d'une application web (server side), nous vous recommandons d'utiliser [le logiciel Shibboleth SP](#) pour faciliter l'intégration de votre application avec notre I.AM IDP.

Si votre système nécessite l'accès à certains services REST (Representational State Transfert) de la plate-forme eHealth, une intégration avec notre I.AM Connect devra être réalisée.

Si votre application doit être capable d'utiliser notre token eXchange, certaines règles sont à respecter et un contrat doit être signé.

Pour pouvoir utiliser I.AM STS et I.AM AA, l'eID de l'acteur de soins de santé ou un [certificat délivré par la plate-forme eHealth](#) est requis.

I.AM ne peut être utilisé que pour des acteurs de soins reconnus par la plate-forme eHealth.



Quelles sont les conditions d'intégration du service I.AM de la plate-forme eHealth ?

- Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth, eHealthppkb@ehealth.fgov.be, en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet.
- A cette issue, si accord, fournir les documents nécessaires à la configuration des services souhaités :
 - CAB-I.AM / eDU à remplir en concertation avec votre chef de projet responsable au sein de la plate-forme eHealth ;
 - pour utiliser la fonctionnalité d'accès aux données :
 - obtenir un [certificat eHealth](#) par environnement souhaité,
 - compléter et soumettre le [formulaire I.AM Registration](#), par environnement, en y mentionnant le certificat obtenu ;
 - pour utiliser I.AM Connect :
 - remplir le bon formulaire client en fonction du realm, [formulaire Healthcare](#) ou [formulaire M2M](#) ;
 - pour utiliser l'I.AM IDP :
 - compléter et soumettre [le formulaire I.AM Registration](#), par environnement, en y mentionnant le certificat obtenu.

Afin de faciliter l'intégration de l'appel au service web STS, la plate-forme eHealth met à la disposition des acteurs des soins de santé des « [connecteurs](#) ».

Pour plus d'information, contactez support@ehealth.fgov.be.

Identity & Access management - Organisation technique

Introduction

Le système I.AM (Identity & Access Management) de la plate-forme eHealth intègre l'ensemble des services de base dont les fonctionnalités permettent d'assurer une gestion des accès, une gestion des utilisateurs et une gestion de l'accès aux données.

Selon les besoins applicatifs, il est possible de distinguer 4 contextes :

1. La sécurisation de Web App
2. La sécurisation de services web « Simple Object Access Protocol » (SOAP)
3. La sécurisation de services web « Representational State Transfert » (REST)
4. Le Data Access

L'authentification et l'autorisation sont des aspects importants pour chacun de ces contextes.



La sécurisation de Web App

Pour accéder à une application de type Web App sécurisée, il faut s'authentifier et obtenir une autorisation :

- pour les applications web classiques (typiquement des applications server-side HTML), via le composant « I.AM IDP » ;
- pour les applications web mobiles (applications utilisant du JavaScript pour appeler des services REST par exemple) ou applications natives, via le composant « I.AM Connect ».

Dans tous les cas, le système offre la possibilité aux utilisateurs d'avoir du « single sign-on » qui permet de s'identifier une seule fois pour accéder à plusieurs applications différentes.

Dans le cas d'applications web classiques, la gestion des autorisations est effectuée par notre IDP (Identity Provider), via User & Access Management (UAM).

Dans le cas d'applications web mobiles, la gestion des autorisations est effectuée par les différents services appelés.

Documentation utile pour les applications web classiques :

- [I.AM overview](#)
- [I.AM federation metadata](#)
- [I.AM IDP \(Identity Provider\)](#)
- [I.AM federation attributes](#)
- [I.AM logout](#)
- [I.AM SP Shibboleth](#)
- [I.AM SP Shibboleth upgrade](#)
- [I.AM registration](#)
- [UAM \(User Access Management\)](#)
- [Gestion intégrée des utilisateurs et des accès SLA](#)

Documentation utile pour les applications web mobiles ou applications natives :

- [I.AM Connect - Mobile integration - Technical specifications.](#)

La sécurisation de services web SOAP

SOAP (Simple Object Access Protocol) est un protocole orienté « objet » qui permet la transmission de messages structurés (format XML dans une Enveloppe SOAP) entre un WSC (Web Service Consumer) et un WSP (Web Service Provider).



Ce protocole est notamment utilisé dans le cadre d'architectures de type SOA (Service Oriented Architecture).

L'authentification des WSC s'effectue via le service « I.AM STS » (Secure Token Service) au moyen d'un certificat eHealth ou d'une carte d'identité électronique (eID). L'assertion obtenue par le WSC est ensuite évaluée dans le cadre de l'autorisation.

L'autorisation est principalement effectuée, pour chaque service appelé, par le service Bus de la plate-forme eHealth sur base de règles préalablement définies. Pour chaque service SOAP disponible et protégé sur l'[Enterprise Service Bus \(ESB\) de la plate-forme eHealth](#), les règles d'accès définies sont évaluées afin d'autoriser ou non l'accès au service.

Il est également possible, pour un utilisateur, de basculer d'une authentification/autorisation de type Web Service, vers une authentification/autorisation de type Web App, via le service « [I.AM STS to IDP](#) ».

Documentation utile :

- [Certificat eHealth](#)
- I.AM STS
- Coordination de processus
- [Sécurisation des services web](#)

La sécurisation de services web REST

Les services web REST (Representational State Transfert) sont utilisés dans le cadre d'architecture de type REST. Cette architecture se repose sur le protocole HTTP via ces différentes opérations : GET, POST, PUT, DELETE.

Le format des messages échangés ici n'est plus du XML mais du JSON.

Ce type de services s'adresse plus particulièrement aux applications mobiles.

L'authentification et l'autorisation des clients s'effectuent via le service « I.AM Connect » qui se base sur le standard OIDC (OpenID Connect).

I.AM Connect permet, entre autres, de délivrer un « Access token » au client qui peut l'envoyer ensuite vers le service REST.

Le service REST vérifie alors le contenu de cet « Access token » afin de traiter les contraintes de sécurité préalablement établies.

Documentation utile :

- [I.AM Connect - Mobile integration - Technical specifications](#)



Le Data Access

Ce système fait appel au composant « I.AM AA » dont la fonction est d'interroger différentes sources de données afin de vérifier si les conditions préétablies pour accéder aux données sont remplies et, le cas échéant, autoriser ou non l'accès.

I.AM AA (AttributeAuthority)

I.AM AA permet à nos partenaires d'interroger les sources authentiques eHealth. Ces sources contiennent des informations concernant les acteurs des soins de santé (CoBRHA), les mandats...

Ce système a été défini afin de scinder les accès applicatifs des accès aux données.

I.AM STS (Secure Token Service)

I.AM STS permet à un acteur de soins de santé de s'identifier via la génération d'un token (par opposition à l'identification par eID ou username). Il est dédié à l'identification pour les services web intégrés aux logiciels médecin et permet de s'identifier en tant que médecin, médecin spécialiste, infirmier, etc.

I.AM IDP (Identity Provider)

I.AM IDP est le service permettant de créer, de maintenir et de gérer les informations d'identité des utilisateurs pouvant s'authentifier dans un réseau distribué ou au sein d'une fédération.

Différentes méthodes d'authentification sont supportées par l'IDP afin de s'assurer que l'utilisateur puisse prouver qu'il est bien celui qu'il prétend être.

I.AM IDP permet de sécuriser l'accès aux applications web proposées et hostées par des fournisseurs de service (Service Providers) via [UAM](#).

I.AM Connect

I.AM Connect est une solution de gestion d'identité et d'accès pour les applications web et les services web RESTful basée sur OIDC (OpenID Connect).

Elle permet aux clients de demander et recevoir des informations sur les sessions authentifiées et les utilisateurs finaux. I.AM Connect permet également aux clients de vérifier l'identité de l'utilisateur final en fonction de l'authentification effectuée par notre serveur d'autorisation.

Les clients de tous types sont pris en charge : clients d'applications web, clients JavaScript, applications natives (clients « mobile »).

Documentation utile :



- [I.AM Connect - Mobile integration - Technical specifications](#)

UAM

UAM = User & Access Management

L'UAM est utilisé dans le cadre de Web Apps classiques, de Web services via le service Bus de la plate-forme eHealth et permet d'autoriser ou non l'accès d'un utilisateur à une ressource protégée.

L'UAM fonctionne sur base du Policy Enforcement Model générique, comprenant le Policy Enforcement Point (PEP), le Policy Decision Point (PDP), le Policy Administration Point (PAP) et le Policy Information Points (PIP).

Plus d'information sur [UAM](#).

