Welcome Pack

La plate-forme eHealth met à la disposition des partenaires un inventaire détaillé des informations nécessaires pour l'intégration de ses différents services. Ce catalogue comprend l'ensemble de 'ce qu'il faut savoir', 'ce qu'il faut comprendre' et 'ce qu'il faut prévoir' avant de démarrer un projet ainsi que les adresses de contact utiles.

Process des projets

1. Prise de connaissance par le partenaire des informations contenues dans notre Welcome Pack
2. A cette issué, prise de contact par le partenaire avec notre cellule projets avec un résumé du projet comprenant la finalité du projet, les flux déterminés, les services sollicités etc..
3. Examen du projet en interne > Attribution si accord à un chef de projet
4. Introduction si nécessaire par le partenaire d’un dossier unique
5. Examen juridique du projet par la plate-forme eHealth (le projet nécessite-t-il une délibération ou un avis du comité sectoriel ?)
6. Proposition de planning en accord avec la cellule IT – introduction du projet dans le release calendar
7. Contact si nécessaire avec la cellule IT (soutien à l’intégration des composants utiles)
8. Mise à disposition si nécessaire des documents techniques par le partenaire

Un projet doit répondre au minimum aux contraintes suivantes – la mise en production est soumise strictement au respect de ces contraintes

1. Prise de connaissance par le partenaire des informations contenues dans notre Welcome Pack
2. Rédaction et approbation d'un dossier unique
3. Approbation du Comité sectoriel (si nécessaire)
4. Rédaction et approbation d'un planning
5. Rédaction et mise à disposition de la documentation technique (si nécessaire)

Services de base

1. Codage, anonymisation et TTP
2. Datation électronique (timestamping)
3. Système de cryptage end-to-end
4. Portail
5. Data Attribute Service - service web
6. Répertoire des références (Hubs & Metahub)
7. Webservices ConsultRN
8. Coordination de processus partiels électroniques
9. IAM (Identity & Access Management)
10. Certificats eHealth
11. Boîte aux lettres électronique sécurisée (eHealthBox)

Application LiveCycle

1. eHealth Business Continuity Plan
2. Niveaux de service
3. Releases Management

Standards

1. Standards

Connectors

1. eHealth platform services connectors

Sécurité de l'information & GDPR

1. Sécurité de l'information & General Data Protection Regulation

Architectures

1. Architectures

Important

La plate-forme eHealth rappelle à ses partenaires l'importance de toujours reprendre contact avec ses services s'ils souhaitent développer un nouveau projet ou étendre un projet existant. En l'absence de cette diligence, la plate-forme eHealth peut être impactée à différents niveaux.

En effet, en ce qui concerne le suivi des projets, la plate-forme eHealth risque de ne plus disposer de vue globale sur l'ensemble des projets utilisant ses services de base. Des incohérences sur le plan de l'architecture pourraient par ce biais être générées. Une telle façon de procéder pourrait également surcharger la capacité technique de la plate-forme eHealth en cas d'envois massifs et simultanés de messages, ayant pour conséquence d'impacter la disponibilité du service de base pour l'ensemble des partenaires.

Les conditions générales relatives à l'octroi du certificat eHealth (acceptation et production) énoncent à cette fin depuis le mois de septembre 2013 que « toute utilisation du certificat eHealth se limite, le cas échéant, au champ d'application des délibérations juridiques existantes. En cas d'extension, adaptation ou évolution de la finalité ou portée de cette utilisation, il faut obligatoirement contacter la plate-forme eHealth ».

La plate-forme eHealth invite donc ses partenaires à tenir compte des responsabilités qui leur incombent et de l'obligation qui est la leur de respecter les termes du dossier unique.

Services de base

1. Codage, anonymisation et TTP

Que sont le codage et l'anonymisation (Trusted Third Parties) de la plate-forme eHealth?

Ces outils permettent de dissimuler derrière un code l'identité d'une personne ou des données à caractère médicale la concernant afin de respecter sa vie privée et le secret médicale. Le codage se présente sous la forme d'un service web synchrone tandis que l'anonymisation TTP se présente sous la forme d'un batch complémentaire à l'eHealthBox et fonctionne de façon asynchrone.

Quelles sont les fonctionnalités du codage et de l'anonymisation TTP ?

Codage

Le service web de codage (WS Seals) offre les fonctionnalités suivantes :

- 'Encode': cette méthode permet de soumettre des données en input et de retourner en output ces données encodées. Différents algorithmes sont disponibles afin de réaliser l'encodage
- 'Decode': cette méthode permet de soumettre des données encodées en input et de retourner en output les données en clair (décodées)

Anonymisation TTP

L'anonymisation TTP également appelée « Batch TTP Codage » permet à une institution ou à professionnel de soins de santé, en possession de données médicales, d'envoyer ses données vers un destinataire connu en les anonymisant, c'est-à-dire en encodant les informations permettant d'identifier les personnes liées à ces données médicales. L'anonymisation se fait également au niveau de l'émetteur du message afin que le destinataire ignore de qui proviennent les données médicales qu'il a reçu et éviter de cette manière toute déduction qui lui permettrait de lier une personne précise à ces données.

Le TTP permet également au destinataire d'enrichir les données médicales qu'il a reçues et de les retourner vers l'émetteur initial (en ignorant toujours l'identité de ce dernier). Dans ce cas, les données seront « désanonymisées » de façon à ce que l'émetteur initial puisse lire toutes les informations en clair.

Concrètement, l'envoi et la réception des messages se fait via l'eHealthBox tandis que le batch TTP Codage traite ces derniers de façon à les anonymiser/désanonymiser et les envoyer vers l'institution ou personne correctes. Une fois qu'un message est traité et délivré, un accusé de réception est envoyé à l'émetteur afin de l'en avertir ou au contraire pour lui transmettre la raison qui rend impossible son traitement. Un message est au maximum traité et transmis au destinataire final dans les 2h après son envoi.

En pratique

Quelles sont les conditions d'intégration du service de codage et du TTP de la plate-forme eHealth ?

- Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth

  Wolf.Wauters@ehealth.fgov.be

  en détaillant clairement le contexte et la finalité de votre projet

- Dans le cadre de l'utilisation du batch TTP codage, trois éléments sont prérequis :
  - Accord du comité sectoriel
    - rédaction d'une demande d'autorisation d'utilisation du batch codage auprès du Comité Sectoriel. Vous trouverez la liste des différents Comités Sectoriels ainsi que les informations concernant la demande d'autorisation via le lien suivant
    - toute question supplémentaire concernant la demande peut être envoyée à TTP@ehealth.fgov.be
  - Signature électronique du document TTP_GlobalDoc
    - une fois que le Comité Sectoriel a rendu son accord, un document nommé « TTP_GlobalDoc » doit être rédigé par l'équipe TTP Service de la plate-forme eHealth (contact : TTP@ehealth.fgov.be). Ce document résume la procédure d'échange de données médicales (émetteurs, destinataires, détails de la transmission,…) en accord avec la délibération du Comité Sectoriel. Ce document doit être signé électroniquement par toutes les parties en lien avec le projet
    - suite à la signature de ce document, l'équipe TTP Service de la plate-forme eHealth fournira aux émetteurs les informations nécessaires à l'utilisation du batch TTP (par exemple le nom du projet TTP à utiliser dans les messages)
  - Accès à l'eHealthBox
    - comme expliqué précédemment, l'utilisation du batch TTP codage implique l'utilisation de l'eHealthBox. Dès lors, cela implique que les émetteurs et les destinataires doivent posséder un certificat eHealth.
- Dans le cadre de l'utilisation du service de codage

- Disposer d'un certificat eHealth afin de pouvoir utiliser le service web
- Accord du Comité Sectoriel dans le cas de l'utilisation de la méthode « Decode »

  L'utilisation de la méthode « Decode » permettant de décoder les données, elle doit être approuvée par le Comité Sectoriel. Vous trouverez la liste des différents Comités Sectoriels ainsi que les informations concernant la demande d'autorisation via le lien suivant

  Toute question supplémentaire concernant la demande peut être envoyée à Wolf.Wauters@ehealth.fgov.be

2. Datation électronique (timestamping)

Qu'est-ce que le timestamping ?

La plate-forme eHealth offre un service de timestamping (datation électronique ou horodatage certifié) à ses partenaires.

Le timestamping est un système qui permet de conserver la preuve de l'existence d'un document et de son contenu à une date donnée. Le terme 'preuve' indique le fait que personne, pas même le propriétaire du document, ne peut modifier le certificat de timestamping.

Quelles sont les fonctionnalités du timestamping ?

Ce service propose plusieurs fonctionnalités :

- un service web d'horodatage classique (TimeStampAuthority) qui procède à la certification du document et si besoin à son archivage (facultatif);
- un service web de consultation (TimeStampConsult) des documents horodatés qui assure le contrôle des documents horodatés au cours d'une période donnée.

En pratique

Dépendances, recommandations & avertissements

Le service de timestamping de la plate-forme eHealth est aujourd'hui utilisé dans le cadre de

- la prescription électronique dans les hôpitaux (majoritairement)
- la prescription électronique ambulatoire (Recip-e)

- MyCareNet
- RCT

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

- prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth

  Emmanuel de Hemricourt de Grunne en détaillant clairement le contexte et la finalité de votre projet

- à cette issue, si accord, disposer d'un certificat eHealth

Prescription électronique dans les hôpitaux - Cadre spécifique

Concrètement, un médecin hospitalier émet une prescription électronique (le document à certifier) laquelle est envoyée à la pharmacie de son hôpital. Cette prescription est 'hachée' c'est-à-dire qu'elle est transformée en un code chiffré unique n'ayant aucune signification logique.

Toutes les 5 minutes, les codes chiffrés sont rassemblés au sein d'un package appelé 'TimeStampBag'. Ce package est envoyé à la plate-forme eHealth afin que son service de 'Timestamping' puisse y apposer une date et une heure précise. Muni de sa datation, ce 'package' est alors renvoyé à l'hôpital pour conservation au sein de ses archives. Quant à la plate-forme eHealth, elle conserve une copie du 'package' et de sa datation. En d'autres termes, la plate-forme eHealth fournit la preuve que des prescriptions électroniques ont été créées à une heure et une date précise sans pouvoir connaître leur contenu puisqu'elles sont codées. En cas de contrôle, on applique à nouveau le système de haching sur la prescription. Le code obtenu est comparé avec celui stocké au sein de la plate-forme eHealth. Si les codes sont identiques cela signifie que la prescription n'a pas été modifiée.

Comment un hôpital peut-il utiliser la datation des prescriptions électroniques ?

- La plate-forme eHealth met à la disposition des hôpitaux un outil nommé TimeStamping Client et faisant office d'implémentation de référence.
- La documentation détaillant l'installation et le fonctionnement de cet outil se trouve ci dessous.
- Néanmoins, l'hôpital qui le souhaite peut développer sa propre solution ou installer celle proposée par un fournisseur de logiciel du moment que celle-ci suit les mêmes spécifications que l'implémentation de référence.

- Dans tous les cas, cette solution devra interagir avec la plate-forme eHealth via les services TimeStamping Authority et TimeStamping Consultation afin d'horodater les prescriptions et d'effectuer des vérifications entre les archives de l'hôpital et les archives de la plate-forme eHealth.

Conditions légales à l'utilisation du service Timestamping

En ce qui concerne le timestamping et les prescriptions hospitalières, l'utilisation de ce service est réglée par la loi (voir le règlement du 5 décembre 2016 relatif à la prescription électronique intra hospitalière).

Plus d'info: support@ehealth.fgov.be

3. Système de cryptage end-to-end

Qu'est-ce que le service End to End Encryption de la plate-forme eHealth?

Les service End to End Encryption (ETEE) (également appelé service de chiffrement ou de cryptage) de la plate-forme eHealth est un ensemble de services permettant de chiffrer des messages à destination de prestataires de soins (individuels ou institutions). Ces services sont accessibles aux prestataires de soins individuels et aux institutions et dans certains cas aux patients.

Les services de chiffrement sont utilisés, entre autres, dans le cadre de l'utilisation du service eHealthBox ou de prescriptions électroniques (Recip-e).

Les services ETEE sont les suivants :

- ETKDepot, pour le chiffrement vers un destinataire connu
- KGSS, pour le chiffrement vers un destinataire inconnu

Les services ETEE sont disponibles comme services web (accessibles via un logiciel médical ou via une application tierce).

Quelles sont les fonctionnalités du service End to End Encryption?

Le service web EKDepot est accessible à tous les publics et offre les fonctionnalités suivantes :

- la recherche d'un ETK, qui est la clé publique associée au certificat eHealth d'un prestataire de soins ou d'une institution dont les identifiants (NISS, numéro INAMI, numéro BCE) sont connus

- une fois obtenu, cet ETK permettra de chiffrer un message pour un destinataire connu (le prestataire de soin ou l'institution)

Le service web KGSS (Key Generation and Storage System) est accessible à tous les publics et offre les fonctionnalités suivantes :

- la création d'une clé de chiffrement symétrique qui sera stockée par la plate-forme eHealth et sera accessible sous certaines conditions définies par le créateur de la clé
- la récupération d'une clé existante, à condition de connaitre l'identifiant de la clé et de satisfaire aux conditions d'accès définies lors de la création de la clé (exemple : être authentifié en tant que pharmacie reconnue par la plate-forme eHealth)

Ces fonctionnalités permettent d'utiliser le service KGSS lorsque l'identité du destinataire du message chiffré n'est pas connue à l'avance, mais que certaines conditions doivent être remplies pour l'obtention de la clé de chiffrement.

En pratique

Dépendances, recommandations & avertissements

Pour utiliser le service web ETKDepot ou le service web KGSS, le prestataire de soins ou le patient devra disposer d'un logiciel médical ayant intégré ce service. Ces deux services sont également intégrés au sein de solutions plus globales comme Recip-e, Chapitre IV, eHealthBox.

Afin de faciliter vos opérations de cryptage, une librairie technique est mise à votre disposition.

Quelles sont les conditions d'intégration du service End to End Encryption de la plate-forme eHealth?

- prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth

  Kris Van Aken

  en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet.

Plus d'info: support@ehealth.fgov.be

4. Portail

Qu'est-ce que le service 'Portail' ?

Le portail www.ehealth.fgov.be est historiquement un point d'entrée sécurisé et coordonné pour les acteurs des soins de santé aux différentes applications et informations disponibles en matière de santé en ligne (eSanté). Il offre également toute l'information disponible en matière de support technique aux développeurs ICT pour l'intégration de nos services de base (plate-forme eHealth: www.ehealth.fgov.be/ehealthplatform). La gestion du contenu du portail est assurée par un 'Content Management System' (CMS) qui permet de concevoir et de mettre à jour de manière dynamique les différents contenus utiles (textes, FAQ's, outils de support en ligne, documents divers, structures de menus etc.)

Quelles sont les fonctionnalités d'un CMS?

L'intégration d'un CMS pour gérer un site web ou une application offre les fonctionnalités suivantes (liste non-exhaustive):

- Gestion de contenus génériques: actualités, FAQs, support, …caractéristiques d'un type de contenu
  - champs obligatoires ou optionnels
  - possibilité de créer des liens entre les contenus
  - plus de 30 types de données possibles (dates, données numériques, textes libres, couleurs)
  - plusieurs langues possibles
- Gestion des droits d'accès et de publication selon le profil de l'utilisateur (auteur, publisher, admin, …)
- Gestion de la chaîne de publication (workflow) pour l'approbation et la publication du contenu
- Gestion des différentes versions
- Historique des modifications selon la date et l'auteur
- Possibilité de gérer différents formats de publication: JSON, XML, HTML, …

En pratique

Dépendances, recommandations & avertissements

Il est préférable que l'application ou le site web dispose de sa propre mémoire cache afin de

- disposer d'un scénario de fall back en cas d'indisponibilité du CMS

- de ne pas avoir à faire appel au CMS à chaque requête (éviter les reports de charge) par exemple en ne faisant appel au CMS qu'au maximum une fois toutes les minutes

Quelles sont les conditions d'intégration du service au sein 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 de votre projet

5. Data Attribute Service - service web

En exécution de l'article 5, 4°, a) de la loi organique de la Plate-forme eHealth du 21 août 2008, la Plate-forme eHealth a reçu comme mission d'être une plate-forme de collaboration pour l'échange électronique de données sécurisé.

De nouveaux projets, entre autres dans le cadre de la simplification administrative, exigent en vue d'un routage adéquat des messages, l'utilisation d'un annuaire. L'objectif poursuivi est de pouvoir déterminer à quelle(s) instance(s) un message relatif à un patient doit être envoyé (par exemple : service de prévention, médecin-contrôle, employeur...).

DAAS est donc un service générique développé par la Plate-forme eHealth pour répondre à différentes questions permettant d'identifier le ou les destinaire(s) d'un message dans le secteur de la santé.

Ce service générique s'inspire de Attribute Authority (AA).

Pour identifier le destinataire d'un message, ce service va opérer des consultations soit de sources authentiques soit de l'annuaire de routage résiduaire et transmettre le résultat de la recherche au softprovider du prestataire de soins.

Selon le projet, l'utilisation de ce service sera soumise à l'approbation par le Comité de gestion de la plate-forme eHealth et par le Comité sectoriel de la sécurité sociale et de la santé.

Pour qui ?

Dans un premier temps, dans le cadre du projet "back to work", ce service est appelé par les fournisseurs de logiciels des médecins généralistes, ainsi que par la solution utilisée par les organismes assureurs et services de prévention et protection au travail.

« Back to work » vise à la réintégration de malades de longue durée qui ne sont plus en mesure d'exécuter le travail convenu

- en leur offrant temporairement du travail adapté ou un autre travail en attendant qu'il puisse à nouveau exercer le travail convenu,
- en lui donnant définitivement du travail adapté ou un autre travail.

Ce trajet de réintégration est établi en concertation entre les différents médecins (médecin traitant, service médical gérant les incapacités de travail et médecin du travail).

A cet effet, il y a notamment lieu de réaliser la communication électronique entre les différentes parties. Le présent projet vise en particulier à réaliser l'échange de données médicales entre le médecin traitant, le médecin-contrôle de la mutualité et le médecin du travail.

DAAS est utilisé dans le cadre du présent projet pour un routage correct des messages eHealthBox aux divers médecins concernés.

Ce service générique sera également plus tard utilisé dans le cadre du projet Mult-emediatt (Informatisation des certificats d'incapacité de travail).

Besoin d'aide ?

Le centre de contact peut aider les producteurs de logiciels en cas de questions à ce sujet.

Tél : 02 788 51 55

Mail : support@ehealth.fgov.be

6. Répertoire des références (Hubs & Metahub)

Le système « hubs & metahub », dans sa globalité, a pour objectif de réaliser l'interconnexion des systèmes régionaux et locaux d'échange d'information médicale, dénommés "hubs", afin de permettre à un prestataire de soins de retrouver et de consulter les documents médicaux électroniques disponibles au sujet d'un patient et ce indépendamment, d'une part, du lieu effectif de stockage des documents et, d'autre part, du point d'entrée du prestataire dans le système.

7. Webservices ConsultRN

Qu'est-ce que ConsultRN?

ConsultRN regroupe un ensemble de services qui permet de rechercher et consulter des données d'une personne au sein du registre national et du registre de la banque carrefour.

Ces services sont accessibles aux institutions et aux professionnels de la santé (reconnus par l'arrêté royal AR78), qui ont obtenu préalablement reçu l'autorisation du Comité de sécurité de l'information (anciennement « Comité sectoriel ») de la sécurité sociale et de la santé.

Les autorisations obtenues par le passé auprès du Comité sectoriel du Registre national ou du Comité sectoriel de la sécurité sociale et de la santé restent valables.

Ces autorisations sont obtenues en fonction :

- du type d'institution et/ou de prestations effectuées (hôpitaux, laboratoires agréés, médecins généralistes)
- de la finalité de la demande (ex. : d'utiliser le numéro de ce registre en vue de la vérification et de l'actualisation des données d'identification des patients, vérification et de l'actualisation des données d'identification de leurs patients, de leur identification univoque au sein du dossier médical, …)
- du type de données auxquelles il est demandé d'accéder (nom, date de naissance, sexe, résidence, ….

Pour le détail des délibérations, nous vous invitons à consulter l'onglet « Comité de Sécurité de l'Information ».

Quels sont les services proposés par ConsultRN ?

IdentifyPerson

permet de consulter certaines données du registre national et des registres Banque Carrefour d'un patient à partir d'un NISS (Numéro d'Identification de la Sécurité Sociale) et d'inscrire celui-ci au registre de suivi de ses mutations.

PhoneticSearch

permet de retrouver l'identifiant unique actif d'un patient au sein du registre national et des registres Banque Carrefour sur base de critères phonétiques (ex : nom et date de naissance).

PersonHistory

permet de consulter l'historique (nom, date et lieu de naissance, sexe, adresse) des données du registre national et des registres Banque Carrefour d'un patient à partir d'un NISS (Numéro d'Identification de la Sécurité Sociale

ManageInscription

permet à une organisation de gérer l'enregistrement d'un patient au service d'abonnement des mutations afin d'être informée des modifications des données de celui-ci (ex : changement d'adresse).

MutationSender

permet de recevoir les modifications (adaptation, ajout ou suppression) des données (ex : changement d'adresses) du patient. Au préalable, le patient devra être inscrit au service d'abonnement des mutations (ManageInscription)

SsinHistory

permet de recevoir l'historique des identifiants uniques (NISS/BISS) pour un patient à partir du dernier NISS connu par le prestataire

ManagePerson

permet, de créer des numéros NISS-bis et, dans le cadre des tests d'intégration du service ConsultRN, de créer un patient avec des données fictives au niveau du registre national.

En pratique

A qui s'adresse ConsultRN ?

Les services web de ConsultRN ont été développés à l'attention des institutions de soins et des prestataires de soins.

Les institutions suivantes ont déjà été autorisées via des délibérations générales à utiliser ces services:

Hôpital

- Délibération RN n° 21/2009 du 25 mars 2009
- Délibération RN n° 60/2009 du 7 octobre 2009
- Délibération n°9/039 du 7 juillet 2009

Laboratoire agréé de biologie clinique

- Délibération RN n° 35 du 6 octobre 2010
- Délibération n°10/078 du 9 novembre 2010

Maison de repos ou maison de soins agréée

- Délibération RN n°41/2011 du 20 juillet 2011
- Délibération n° 11/084 du 8 novembre 2011

Maison de soins psychiatriques ou initiatives d'habitation protégée

- Délibération RN n° 40/2011du 20 juillet 2011
- Délibération n° 11/083 du 8 novembre 2011

D'autres organisations ayant introduit un dossier justifiant la finalité et la proportionnalité ont également reçu une délibération spécifique.

Les professionnels des soins de santé (AR78) ont été autorisés sur le plan juridique à utiliser le numéro de registre national dans le cadre de l'utilisation des applications utilisant les services de base de la plate-forme eHealth et à enregistrer à cette fin le numéro de registre national dans le dossier du patient. Dans un premier temps, cette faculté est ouverte aux médecins généralistes.

- Délibération RN n° 77/2009 du 23 décembre 2009, n°11/2018 du 21 février 2018 et n° 20/2018 du 28 mars 2018
- Délibération n° 18/039 du 6 mars 2018

Pour tout renseignement complémentaire ou pour connaître les étapes à entreprendre en vue de l'obtention de toute nouvelle délibération, nous vous invitons à contacter la Plate-forme eHealth : valerie.forton@ehealth.fgov.be

Comment accéder à Consult RN ?

a) Préalables

Pour utiliser les services de eHealth ConsultRN, l'institution ou le prestataire de soins devra :

- disposer d'un logiciel médical qui aura intégré ce service ;
- disposer d'un certificat eHealth (pour obtenir un certificat en acceptance et en production)

b) Procédure d'intégration à suivre si votre organisme est un hôpital, un laboratoire, une maison de soins psychiatriques, une initiative d'habitation protégée, une maison de repos ou une maison de soins

Etape 1 : Les instances visées ci-dessus souhaitant intégrer le webservice au sein d'une de ses applications doivent tout d'abord transmettre (de préférence par mail) l'ensemble des documents ci-dessous à l'adresse suivante :

Comité de sécurité de l'information, chambre sécurité sociale et santé

A l'attention de Madame Joke Vanderpoorten

E-mail : ivc@mail.fgov.be

Adresse postale: Quai de Willebroeck, 38 à 1000 Bruxelles

1. un engagement dans lequel l'institution déclare respecter les conditions décrites dans la délibération. Vous devez choisir le formulaire adéquat en fonction du type de votre institution :

    - formulaire pour un hôpital
    - formulaire pour un laboratoire
    - formulaire pour une maison de soins psychiatriques ou une initiative d'habitation protégée
    - formulaire pour une maison de repos ou une maison de soins

2. un acte de reconnaissance de votre institution (preuve du statut ou de l'agrément)
3. un formulaire d'évaluation du DPO de votre organisation
4. un formulaire de déclaration de conformité portant sur les mesures de référence en matière de sécurité
5. une demande d'autorisation d'utilisation des webservices eHealth

Pour toute question relative sur les formulaires à remplir, n'hésitez pas à prendre contact avec Valérie Forton, chef de projet responsable pour la Plate-forme eHealth à l'adresse suivante : valerie.forton@ehealth.fgov.be

Etape 2 : Le Comité de sécurité de l'information, chambre Sécurité sociale et Santé, vous communiquera sa décision (et en cas d'accord, votre APPLICATIONID) et informera en même temps le Registre National.

Etape 3 : Vous devez ensuite entamer la partie technique (voir les cookbooks ci-dessous) et envoyer à l'adresse suivante : integration-support@ehealth.fgov.be vos cas de tests en acceptation.

Le document à compléter à cet effet est disponible ici.

Etape 4 : En cas de validation des cas de tests, la Plate-forme eHealth fera le nécessaire pour la configuration de vos accès en production.

c) Procédure d'intégration à suivre si votre organisme ne relève pas de la catégorie visée ci-dessus

Nous vous invitons à prendre contact avec le chef de projet responsable pour la Plate-forme eHealth en détaillant clairement le contexte, la finalité de votre demande ainsi qu'une estimation volumétrique de votre projet. Un examen de votre demande sera réalisé avec vous.

Pour les médecins généralistes, l'appel à certains services de « eHealth Consult RN » sera intégré dans les critères d'enregistrement des software de médecine générale.

d) Points d'attention importants

Si votre organisation évolue sur le plan juridique ou administratif (fusion, retrait d'agrément,..) ou en cas de changement de DPO, il vous est demandé de directement prendre contact avec la Plate-forme eHealth : valerie.forton@ehealth.fgov.be

Ces évolutions peuvent en effet avoir des impacts tant sur le plan juridique que sur le plan technique (par exemple accès aux services de la Plate-forme eHealth via les certificats eHealth).

8. Coordination de processus partiels électroniques

Qu'est-ce que le service 'Coordination des processus'?

Ce service vise à permettre l'intégration, harmonieuse et flexible, des différents services (services de base et applications) au sein d'un système d'échange de données déterminé.

Il veille à la structuration des messages, qu'ils soient compréhensibles par les différents systèmes, il s'assure que les fonctionnalités soient compatibles et respectent certains standards et qu'il n'y ait pas de variation des niveaux de sécurité selon les étapes de la procédure.

Cette coordination est transparente pour l'utilisateur et s'effectue notamment au moyen de ce qu'on appelle un Entreprise Service Bus (ESB).

Quelles sont les fonctionnalités du service?

Le service de coordination des processus offre les fonctionnalités suivantes :

- Standardisation des messages et erreurs
- Vérification et propagation de l'identité de l'utilisateur
    - la vérification effectuée dépend du service appelé par l'utilisateur
- Gestion de loggings de sécurité
- Orchestration des appels
    - transformation des messages
    - enrichissement des messages
    - transport des messages vers les services web des partenaires ou de la plate-forme eHealth
- Registre de services (Registry)
    - le registre reprend l'ensemble des services offerts par la plate-forme eHealth et ses partenaires, les informations techniques et fonctionnelles y sont mentionnées
    - le registre est accessible en acceptation et production

En pratique

Dépendances, recommandations & avertissements

Recommandations :

- les services des partenaires doivent prendre les mesures nécessaires pour garantir la stabilité et la conformité des services appelés par notre ESB
- les services des partenaires doivent être en mesure d'investiguer les incidents

Avertissements :

- les services échangeant des données de manière asynchrone ne peuvent pas utiliser ce service

Quelles sont les conditions d'intégration d'un service au sein 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

Afin de faciliter l'intégration de l'appel aux services, la plate-forme eHealth peut inclure ces services dans les 'connecteurs'.

Plus d'info: support@ehealth.fgov.be

9. IAM (Identity & Access Management)

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

Le service de gestion 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 composé 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 plateforme eHealth).

Ces composants sont conformes aux normes internationales pour les communications inter-entreprises 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 individuel (sur base des informations contenues dans la base de données Cobrha)
  - son 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 un durée déterminée (durée dépendant du profil de l'utilisateur)

Remarque: le single-sign-on IDP 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 2ème application (supportant ce profil) protégée par notre IAM 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
      - la délégation s'effectue via le UserManagement
    - en complément de ces attributions d'application aux utilisateurs, il est possible de définir des fonctions au sein de cette institution
      - la délégation s'effectue via le UserManagement et Remaph
      - cette fonctionnalité ne peut en principe pas être utilisée dans le cadre des services web > si cette fonctionnalité est utilisée, 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.
      - la délégation se fait via UserManagement et Remaph
      - cette fonctionnalité ne peut en principe pas être utilisée dans le cadre des web services > si cette fonctionnalité est utilisée, 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
    - la délégation se fait 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
        - la délégation se fait 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 CoBRHA) peuvent être accédées 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 IAM 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

- à cette issue, si accord, fournir les documents nécessaires à la configuration des services souhaités
  - CAB-IAM / 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 IAM Registration, par environnement, en y mentionnant le certificat obtenu
  - pour utiliser IAM Connect
    - désigner le realm à utiliser ou compléter le formulaire de création de realm
    - remplir et soumettre le formulaire d'enregistrement de client
  - pour utiliser l'IAM IDP
    - compléter et soumettre le formulaire IAM 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'.

Plus d'info: support@ehealth.fgov.be

Identity & Access management - Organisation technique

Introduction

Le système IAM (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 Web Service 'Simple Object Access Protocol' (SOAP)
3. La sécurisation de Web Service 'Representational State Transfert' (REST)
4. Le Data Access

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

La sécurisation 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 'IAM IDP'
- pour les applications web 'mobile' (applications utilisant du JavaScript pour appeler des services REST par exemple) ou applications natives, via le composant 'IAM 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.

Il est également possible, pour un utilisateur, de basculer d'une authentification/autorisation de type Web App, vers une authentification/autorisation de type Web Service au moyen de la fonctionnalité 'SSO IDP to fat client'.

Dans le cas de Web Apps classiques, la gestion des autorisations est effectuée par notre IDP (Identity Provider) (via User & Acces Management - UAM).

Dans le cas de Web Apps 'mobile', la gestion des autorisations est effectuée par les différents services appelés.

Documentation utile pour les Web Apps classiques :

- IAM overview
- IAM federation metadata
- IAM IDP
- IAM federation attributes
- IAM logout
- IAM SP Shibboleth
- I.AM SP Shibboleth upgrade
- I.AM registration
- Gestion intégrée des utilisateurs et des accès SLA
- UAM

Documentation utile pour les Web Apps 'mobile' ou applications natives :

- I.AM Connect Technical specifications
- I.AM Connect - Client registration
- I.AM Connect - Realm registration

La sécurisation Web Service 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 IAM 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'ESB de la plate-forme eHealth, les règles d'accès définies sont évaluées afin d'autoriser ou non l'accès au service.

Tout comme il est possible de basculer d'une authentification/autorisation de type Web App vers une authentification/autorisation de type Web Service, l'exercice inverse est possible, via le service 'IAM STS to IDP'.

Documentation utile :

- Certificat eHealth
- IAM STS
- Coordination de processus

La sécurisation Web Service REST

Les web services 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 'IAM Connect' qui se base sur le standard OIDC (OpenID Connect).

'IAM 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 Technical specifications
- I.AM Connect - Client registration
- I.AM Connect - Realm registration

Le Data Access

Ce système fait appel au composant 'IAM 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.

IAM AA (AttributeAuthority)

IAM 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.

IAM STS (Secure Token Service)

IAM 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 web services intégrés aux logiciels médecin, et permet de s'identifier en tant que médecin, médecin spécialiste, infirmier, etc.

IAM IDP (IDentity Provider)

IAM 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.

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

IAM 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 Technical specifications
- Définition de realm
- Définition de clients

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).

Informations sur UAM.

10. Certificats eHealth

Qu'est-ce qu’un certificat eHealth?

Les certificats délivrés par la plate-forme eHealth permettent à un individu ou une organisation de s’authentifier en tant que prestataire de soins ou institution reconnue.

Lorsqu'un prestataire de soins souhaite avoir accès à certains services de base de la plate-forme eHealth en utilisant une connexion de système à système et non une application web, il doit disposer d'un certificat eHealth. Ce certificat permet d'identifier et d'authentifier le partenaire “système” tandis que l'eID ou le token permet d'identifier et d'authentifier l'utilisateur (la personne).

Ceci est valable tant pour l'utilisation de services de base que pour l'utilisation d'applications proposées sous forme de services web.

Le certificat, une fois configuré dans le logiciel du prestataire ou de l'institution, permet d'utiliser les services mis à disposition par la plate-forme eHealth et requérant une authentification.

Un certificat eHealth peut être demandé et installé grâce à une application téléchargeable.

Les intégrateurs de logiciels (et non les prestataires de soins) peuvent par ailleurs demander des certificats de test. Ces certificats permettent aux collaborateurs IT de ces intégrateurs de logiciels qui sont actifs dans le secteur belge des soins de santé, de tester l'intégration de nos services de base. Plus d'informations sur les certificats d'acceptation.

Quelles sont les fonctionnalités d'un certificat eHealth?

Le certificat offre les fonctionnalités suivantes :

- la possibilité pour le prestataire ou l'institution de s'authentifier lors de l'utilisation des services web eHealth, notamment en demandant un jeton d'accès permettant l'accès à ces services
- la possibilité de chiffrer des messages, par exemple dans le cadre de l'utilisation d'une eHealthBox
    - le certificat et le mot de passe associé servent alors de clé privée de chiffrement
- la possibilité pour un prestataire ou une institution de recevoir des messages chiffrés
    - une clé publique est en effet créée en même temps que le certificat et mise à disposition du public grâce à un web service dédié (ETEE ETKDepot)

En pratique

Dépendances, recommandations & avertissements

Pour un prestataire de soins individuel, il faut

- que son profil soit enregistré dans une source authentique validée
- disposer d'un moyen d'authentification considéré comme fort (eID)
    - pour les prestataires non-Belges, qui ne disposent de facto pas d'une eID, mais qui, exerçant sur le territoire belge, ont besoin d'un accès aux services en ligne et dès lors d'un certificat, il existe une solution hybride

Pour les institutions de soins, il faut

- que son profil soit enregistré dans une source authentique validée en ce compris le titulaire du certificat autorisé au nom de l'institution

- le détenteur du certificat doit disposer d'un moyen d'authentification considéré comme fort
- respecter les normes minimales de la sécurité sociale
- le fonctionnement interne de l'institution de soins doit garantir que seules les personnes autorisées ont accès au système
- une autorisation contenant les conditions de partage des données relatives aux soins de santé entre les institutions de soins de santé

Afin d'utiliser un certificat eHealth pour s'authentifier dans un service web, le prestataire ou l'institution devra disposer d'un logiciel médical intégrant l'utilisation des certificats eHealth (ce qui est le cas de l'ensemble des logiciels enregistrés par la plate-forme eHealth).

Avant de procéder à la demande / l'utilisation d'un certificat eHealth, veillez à prendre connaissance des informations disponibles dans le «Welcome Pack», du règlement d'utilisation, ainsi que des directives pour un usage des certificats eHealth en toute sécurité dans un contexte médical.

Demande de certificat - Mode d'emploi

Qui peut demander un certificat ?

- les prestataires de soins actifs dans le secteur des soins de santé belge

Important :

- il y a lieu d'opérer une distinction entre un certificat individuel (personnel) et un certificat pour une organisation (pour un établissement de soins)
    - dans le cas d'un certificat pour une organisation ou un établissement, un titulaire de certificat mandataire est responsable, au nom de la personne morale, de la gestion et de l'utilisation correctes du certificat. Ceci signifie que ce titulaire du certificat est responsable du respect rigoureux des conditions d'utilisation
- un certificat eHealth est valide 36 mois (peut être renouvelé à partir de 90 jours avant la fin de la période des 36 mois/3 ans)

Processus de demande

Introduisez votre demande via l'application eHealth Certificate Manager

Cette application permet les opérations suivantes:

- demander un certificat eHealth et des clés d'encryption (voir cryptage end-to-end pour les clés);
- renouveler un certificat (endéans la période de renouvellement de trois mois);

- révoquer un certificat;
- modifier le mot de passe des clés d'encryption

11. Boîte aux lettres électronique sécurisée (eHealthBox)

Qu'est-ce que le service eHealthBox?

Le service eHealthBox de la plate-forme eHealth est une boîte aux lettres électronique sécurisée, développée spécifiquement pour les prestataires de soins et les institutions. Son objectif est d'assurer une communication électronique sécurisée des données médicales et confidentielles utiles entre les acteurs des soins de santé belges.
Le service eHealthBox est disponible comme service web (accessible via un logiciel médical) et comme application web (accessible via un ordinateur et une eID/ITSME ou TOTP).

Quelles sont les fonctionnalités du service eHealthBox?

Le service eHealthBox offre les fonctionnalités suivantes :

- sous forme d'application web, un package comprenant
  - un service de consultation des messages
  - un service de publication des messages
  - le service 'eHealth update info', qui est une application permettant d'être averti, via une adresse mail (par exemple l'adresse d'une simple messagerie web choisie par le prestataire de soins) de l'arrivée de nouveaux messages dans l'eHealthBox
  - un service qui permet de consulter les informations générales relatives à la capacité de sa messagerie (taille actuelle, taille maximale autorisée, nombre de messages non reçus lorsque la boite est pleine…)
  - un service de notification qui offre un aperçu du statut des accusés de réception et/ou de lecture des messages
  - la possibilité d'organiser, de déplacer les messages dans les différents dossiers
- sous forme de service web :
  - un service de publication qui permet d'envoyer des messages , qui comprend
    - un service 'out of office' qui permet de référencer un prestataire de soins remplaçant
    - une fonctionnalité de messagerie groupée qui permet d'envoyer un ou plusieurs messages à un groupe de prestataires (par exemple un message à l'ensemble du personnel infirmier d'un hôpital)

- un service d'encryption qui permet de garantir l'intégrité des données transmises
- la possibilité d'envoyer des pièces jointes (la taille du message ne peut dépasser 10 MB)
- la possibilité d'envoyer des messages de type 'news' qui sont des messages que l'on peut mettre à jour de manière illimitée

- un service de consultation des messages qui comprend
  - un service qui permet de consulter les informations générales relatives à la capacité de sa messagerie (taille actuelle, taille maximale autorisée, nombre de messages non reçus lorsque la boite est pleine…)
  - un service de notification qui offre un aperçu du statut des accusés de réception et/ou de lecture des messages
  - un service permettant de consulter un récapitulatif des messages (triés selon la date)
  - la possibilité de consulter simultanément plusieurs messageries (par exemple la messagerie d'un prestataire de soins en sa qualité de prestataire privé simultanément avec sa messagerie en sa qualité de prestataire au sein d'un hôpital)
  - la possibilité d'organiser, de déplacer les messages dans les différents dossiers
- un service dénommé 'eHealth Addressbook' qui
  - permet de rechercher un prestataire de soins sur base de
    - son numéro de registre national (et optionnellement sa profession)
    - son numéro INAMI (et optionnellement sa profession)
    - sa profession et son nom (et optionnellement son prénom)
    - sa profession et son code postal
    - sa profession et sa ville
    - son adresse mail
  - permet de rechercher une institution de soins sur base de
    - son numéro EHP (et optionnellement le type de l'institution)
    - son numéro INAMI (et optionnellement le type de l'institution)
    - son numéro d'entreprise BCE ((et optionnellement le type de l'institution)
    - son nom et son type d'institution
    - son type d'institution et son code postal
    - son type d'institution et sa ville
  - permet de consulter les données de contact les plus actuelles (enregistrées dans les sources authentiques) d'un acteur de soins de

santé ou d'une institution de soins

- pour un acteur de soins de santé : numéro de registre national / nom / prénom(s) / langue / genre / date de naissance / date de décès éventuelle / adresse postale / informations de contact / numéro INAMI / nom de la profession / code de la profession / nom de la spécialisation / code de la spécialisation / adresse(s) professionnelle(s) / eHealthBox
- pour une institution de soins : identifiant (avec son type EHP/CBE/NIHII) de l'institution / description de l'institution / type d'institution / nom / adresses / autres informations de contacts / eHealthBox
- les données eHeathBox retournées contiennent : l'identifiant de la boite et le type d'identifiant (NISS, NIHI, CBE), éventuellement le sous-type (hôpital par exemple), la qualité de l'acteur de soins de santé ou de l'institution

En pratique

Dépendances, recommandations & avertissements

Le service eHealthBox a été développé à l'attention des institutions de soins et des prestataires de soins détenteurs d'un numéro INAMI.

Pour utiliser eHealthBox sous forme d'application web, le prestataire de soins devra se connecter sur l'application via un ordinateur, avec une eID, ITSME ou un TOTP. Il est également essentiel d'utiliser un navigateur web (browser) testé par la plate-forme eHealth.

Pour utiliser eHealthBox, sous forme de service web, le prestataire de soins devra disposer d'un logiciel médical ayant intégré ce service (ce qui est le cas de l'ensemble des logiciels enregistrés par la plate-forme eHealth).

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

- prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth

  Wolf WAUTERS en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet

- à cette issue, si accord, disposer d'un certificat eHealth et prévoir l'intégration d'un service d'encryption

Afin de faciliter l'intégration de l'appel au service web de publication et de consultation de l'eHealthBox, la plate-forme eHealth met à la disposition des acteurs des soins de santé des 'connecteurs'.

Plus d'info: support@ehealth.fgov.be

Application LiveCycle

1. eHealth Business Continuity Plan

Le Business Continuity Plan de la plate-forme eHealth a pour but de garantir la maintenance de nos services après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données tout en conservant un certain niveau de sécurité. Ce plan est l'un des points essentiels de notre politique de sécurité informatique.

Quel que soit le niveau de responsabilité ou la source de l'incident, si un impact est constaté au niveau de la disponibilité des services de la plate-forme eHealth et/ou des services eSanté, l'objectif est de mettre à disposition une solution de secours afin d'assurer la disponibilité des fonctionnalités les plus importantes.

La détermination des fonctionnalités prioritaires, leur niveau de priorité ainsi que l'implémentation technique des solutions sont réalisées en étroite collaboration avec les partenaires institutionnels et fournisseurs de logiciels. En ce qui concerne la communication des informations et étant donné la complexité des attentes des différents groupes-cibles (utilisateurs finaux/prestataires et intégrateurs ICT/fournisseurs de logiciels), l'ensemble des informations directement utiles aux prestataires est communiquée via le site web https://www.status.ehealth.fgov.be/, lequel propose un aperçu détaillé des procédures mises en place et des logiciels qui les ont intégrées. Les informations et procédures spécifiquement dédiées aux intégrateurs ICT sont consolidées sur cette page du site web de la plate-forme eHealth, particulièrement consacrée à cette mission.

La mise en place d'un BCP, l'intégration des différentes interfaces ainsi que les exercices indispensables de tests nécessitent du temps et des adaptions continues. La priorité a été donnée dans un premier temps aux médecins généralistes et aux pharmaciens. L'implémentation des solutions est d'ores et déjà documentée sur le site https://www.status.ehealth.fgov.be/.

La poursuite des différents processus verra simultanément:

- la participation consolidée de nouveaux partenaires selon leurs responsabilités
- la continuité et validation des processus en cours d'intégration chez les partenaires

selon les standards imposés
- l'amélioration continue des outils et solutions sur base des observations de terrain
- la mise en place graduelle de nouvelles solutions pour l'ensemble des utilisateurs finaux

La plate-forme eHealth met à la disposition des intégrateurs ICT les informations utiles pour l'intégration de sa solution BCP au sein de leur système. Pour ce faire, différents supports de documentation sont proposés :

- un cookbook d'implémentation générique de la solution BCP
- un document récapitulatif présentant une application concrète et déjà fonctionnelle du BCP dans le cadre du service assurabilité destiné aux pharmaciens
- les cookbooks de certains services (STS et ETK depot) contiennent des procédures BCP spécifiques à leur utilisation et complémentaires de la solution BCP décrite dans le cookbook BCP
- les connecteurs constituent également des support à l'intégration

2. Niveaux de service

Les niveaux de service de la plate-forme eHealth sont formalisés au sein de deux types de documents :

- Le « MSA » (Master Service Agreement) qui fournit un cadre global ;
- Le « SLA » (Service Level Agreement) qui est spécifique à chaque service.

Le « MSA »

Le MSA propose, aux utilisateurs des services de la plate-forme eHealth, un cadre global traitant principalement de la gestion des incidents, problèmes et changements. Ce document décrit les engagements pris par la plate-forme, les diverses procédures applicables et les descriptions de services.

Le « SLA »

Le SLA clarifie les engagements plus spécifiques à chaque service de la plate-forme eHealth. Ce document contient notamment les objectifs de performance et/ou de disponibilité propres à chaque service, appelés aussi les « KPI » (Key Performance Indicators). Les différents SLA sont accessibles, sur le portail, au niveau des différents chapitres traitant des services proposés par la plate-forme eHealth.

3. Releases Management

Le tableau ci-dessous reprend les dates des prochaines MR (Major Releases) prévues, ainsi que les dates de début des tests en acceptance.

Nom Release	Type de release	Content freeze	Code Freeze	Début tests ACC	Release
R.2018.2.2	Minor	28/11/2018	03/01/2019	15/01/2019	03/02/2019
R.2019.1	Major	04/10/2018	03/01/2019	18/03/2019	05/05/2019
R.2019.1.1	Minor	03/04/2019	09/05/2019	21/05/2019	16/06/2019
R2019.1.2	Minor	30/05/2019	27/06/2019	09/07/2019	28/07/2019
R.2019.2	Major	03/04/2019	27/06/2019	02/09/2019	20/10/2019
R.2019.2.1	Minor	25/09/2019	31/10/2019	12/11/2019	08/12/2019
R.2019.2.2	Minor	28/11/2019	19/12/2019	04/02/2019	23/02/2020
R.2020.1	Major	03/10/2019	19/12/2019	09/03/2020	26/04/2020
R.2020.1.1	Minor	22/04/2020	21/05/2020	02/06/2020	28/06/2020
R.2020.1.2	Minor	28/05/2020	25/06/2020	04/08/2020	23/08/2020
R.2020.2	Major	06/05/2020	25/06/2020	31/08/2020	18/10/2020
R.2020.2.1	Minor	23/09/2020	21/10/2020	03/11/2020	13/12/2020

La dénomination des releases suit la logique suivante : R.2015.x.y, où x est le numéro du Major Release (MR), y le numéro du minor Release (mR). Par exemple, R.2015.1.2 est la 2e minor Release suivant la première Major Release de l'année 2015.

Une MR est planifiée un an avant sa mise en place. Ci-dessous vous verrez les étapes importantes du processus avec X = jour de la release majeure

X - 1 an :	un an avant la release, on décide de ce en quoi consisteront les changements apportés à la nouvelle release par rapport à la précédente;
X - 6 mois :	« content freeze » : plus aucune modification n'est apportée quant aux changements par rapport à la release précédente ;
X - 3 mois :	« code freeze »: plus aucune modification n'est apportée au code ; les cookbooks sont publiés.
X - 5 semaines :	début des tests dans l'environnement d'acceptation ;
X - 2 semaines :	« acceptation freeze »;
X - 1 semaine :	évaluation de la nouvelle version c.à.d. le Go/noGo ;
X	passage en production.

L'environnement d'acceptation bascule avant l'environnement de production ce qui permet de réaliser les tests nécessaires à la mise en place de la release dans l'environnement de production.

Lors du basculement, il est important que votre DNS et votre firewall soient correctement configurés. Vous trouverez ici un document expliquant comment les configurer.

Veuillez noter qu'il est indispensable d'utiliser des données fictives lors des processus de tests, l'utilisation de données à caractère personnel réelles est strictement interdite.

Il est conseillé de procéder à des tests dans le but, à chaque release ou à chaque intégration d'un nouveau composant, de vous assurer que vos composants sont compatibles avec les (nouvelles) versions mises en ligne de nos services. Il est d'autre part possible d'obtenir une démonstration de nos services dans l'environnement d'acceptation. Il suffit dans les deux cas de remplir le formulaire ad hoc et de nous le faire parvenir deux semaines à l'avance par mail à ehealth_service_management@ehealth.fgov.be.

Les eHealth Release Notes sont des documents dans lesquels figurent les nouveaux développements principaux, les adaptations des services de base de la plate-forme eHealth, la fin de vie de services et les problèmes éventuels connus.

Les Release Notes font toujours référence à une eHealth Major Release et sont publiées au portail de la plateforme eHealth trois mois avant une Major Release.

Standards

L'interopérabilité entre les divers acteurs du secteur des soins de santé ne peut être réalisée que si des accords clairs ont été conclus. En fonction du degré d'interopérabilité visé, il faut se mettre d'accord sur les règles régissant les échanges de données, l'architecture générale du système d'échange, les messages échangés, la structure des documents médicaux et sur la codification de l'information.

Depuis de nombreuses années déjà, des initiatives de standardisation sont prises et Belgique et des projets sont mis sur pied. Ci-dessous figure un aperçu non exhaustif des standards utilisés, dans une mesure plus ou moins large, dans les soins de santé en Belgique.

Le législateur a confié à la plate-forme eHealth la mission de définir des standards techniques et fonctionnels utiles en matière d'ICT à l'appui de l'échange électronique de données dans les soins de santé. Les standards existants, énumérés ci-après, serviront de point de départ pour les standards à définir en étroite concertation avec les divers acteurs des soins de santé. Les standards définis par la plate-forme eHealth porteront uniquement sur les aspects ICT et non sur les aspects de contenu des soins de santé.

1. Standards

L'interopérabilité entre les divers acteurs du secteur des soins de santé ne peut être réalisée que si des accords clairs ont été conclus. En fonction du degré d'interopérabilité visé, il faut se mettre d'accord sur les règles régissant les échanges de données, l'architecture générale du système d'échange, les messages échangés, la structure des documents médicaux et sur la codification de l'information.

Depuis de nombreuses années déjà, des initiatives de standardisation sont prises et Belgique et des projets sont mis sur pied. Ci-dessous figure un aperçu non exhaustif des standards utilisés, dans une mesure plus ou moins large, dans les soins de santé en Belgique.

Le législateur a confié à la plate-forme eHealth la mission de définir des standards techniques et fonctionnels utiles en matière d'ICT à l'appui de l'échange électronique de données dans les soins de santé. Les standards existants, énumérés ci-après, serviront de point de départ pour les standards à définir en étroite concertation avec les divers acteurs des soins de santé. Les standards définis par la plate-forme eHealth porteront uniquement sur les aspects ICT et non sur les aspects de contenu des soins de santé.

Standards de communication

En ce qui concerne la communication entre les systèmes de soins et la définition de messages de communication, on utilise le standard de communication Kmehr, développé en Belgique (Kind messages for Electronic Healthcare Record).

Vers le site dédié à ce standard

Patientsummary - Sumehr

En Belgique, lors de la rédaction d'un patient summary, le standard belge Sumehr est utilisé (Summarized Electronic Health Record). Sumehr est un standard basé Kmehr dans lequel est défini l'ensemble minimum de données dont un médecin a besoin pour avoir une vue de la situation médicale d'un patient.

Standards de codification

Les standards de codification utilisés dépendent fortement des divers domaines d'application. En Belgique, on utilise surtout le système de codific ation international WHO ICD (International Classification of Diseases) pour la rédaction de rapports et de statistiques. En fonction des données à rapporter, on utilise tant la version ICD-9 que ICD-10. Un certain nombre de domaines du secteur des soins ou de groupes d'utili sateurs travaillent avec des systèmes de codification dérivés de ICD-10. Des exemples sont ICD-O (International Classification of Diseases for Oncology), utilisé par le registre cancer et ICPC-2 (International Classification of Primary Care), qui est une codification spécifique à la médecine générale. Le cadre de concepts belge IBUI (Identificateur Belge Unique / Belgische Unieke Identificator) se base également sur ICD-10 et ICPC-2. Les standards cités ci-dessus ont une composition assez générique.

Standards spécifiques

Certains domaines spécifiques dans le secteur des soins de santé disposent de leurs propres standards (techniques) et systèmes de codification. DICOM (Digital Imaging and Communications in Medicine) constitue un exemple d'un standard technique développé pour la sauvegarde, la gestion et la communication d'images médicales. Des exemples de standards de codification spécifiques aux domaines sont entre autres ICF (International Classification of Functioning, Disability and Health) pour la kinésithérapie notamment ou Loinc (Logical Observation Identifiers Names and Codes) pour la codification de résultats de laboratoire.

Connectors

Aperçu des différents standards utilisés par la plate-forme eHealth

1. eHealth platform services connectors

Les « eHealth platform services connectors » sont des librairies locales (et légères) dont l'objectif est d'aider les développeurs de software à destination des prestataires de soins individuels et des pharmacies de soins à intégrer les services de base de la plate-forme eHealth qui sont proposés au travers d'interfaces « webservices ». Ces librairies visent également, plus généralement, à supporter les connexions aux services à valeur ajoutée accessibles via la plate-forme eHealth ou qui souscrivent aux standards ICT mis en place par la plate-forme eHealth (comme, par exemple, les « hubs »). Le développement de ces librairies s'inscrit donc dans une logique de standardisation et de support à l'utilisation des services de base de la plate-forme eHealth. Ces connecteurs sont structurés en deux « couches »:

- La première couche, dénommée « **connecteur technique** » offre une API générique de support à l'utilisation des services de base purement techniques (principalement afférents à la sécurité : authentification, cryptage, etc.).
- La seconde couche, dénommée « **connecteurs business** », exploite le connecteur technique pour faciliter les connexions à un ensemble de services associés à un public cible donné au sein d'une même session.

Les connecteurs sont évidemment tributaires des interfaces des services qu'ils intègrent. Les mises à jour des connecteurs inhérentes aux changements de ces interfaces seront mises à disposition dans la mesure des possibilités de la plate-forme eHealth au travers de cette page web.

Ces connecteurs sont disponibles en JAVA et .NET mais sont uniquement développés en JAVA. Le code .NET n'est donc pas un code natif. Cette génération est effectuée via une version de l'outil IKVM légèrement adaptée pour nos besoins. Si vous entendez développer vos propres librairies sur base des nôtres dans la même philosophie, nous vous recommandons d'utiliser cette même version de l'outil et de respecter les « directives d'intégration » proposées avec celle-ci.

Les connecteurs sont des librairies distribuées sous licence libre. Elles sont disponibles pour tous ceux qui souhaitent les utiliser. Pour bénéficier de support dans l'utilisation de ces librairies, il faut, par contre, avoir préalablement introduit une demande auprès de la plate-forme eHealth. Vous pouvez introduire cette demande via l'adresse mail info@ehealth.fgov.be (avec la mention « eHealth platform services connectors » au niveau du sujet du mail).

Modification pour octobre 2019 par rapport aux versions précédentes

Dans les connecteurs business, les fonctionnalités suivantes ont été modifiées:

- Mise à disposition, dans le connecteur business MemberData v2, du service

MemberData pour les nouveaux groupes cibles (voir tableau). Les packages médecins existants peuvent continuer à utiliser le connecteur business MemberData v1.

- Ajout d'un nouveau service MemberData Async (asynchrone) pour les infirmiers, sages-femmes, bandagistes et orthopédistes.
- Ajout de nouvelles opérations MOHM dans le connecteur business VSBnet Async (consultSupportAndRepairList, getConsultSupportAndRepairList, cancelApplication, getCancelApplication).
- Mise à disposition du service Mediprima Consult v2 pour les médecins et pharmacies.
- Mise à disposition du service Therlink pour les nouveaux groupes cibles (voir tableau).
- Modification des XSD MyCareNet pour le service MedAdmin.
- Les utilisateurs du connecteur business eAttest v2 doivent migrer vers la version 3.18.0 (voir les bugfixs et améliorations dans les release notes du package connecteur).

Les « Release notes » contiennent plus d'informations.

Services couverts au niveau des couches « business »

- eHealth-platform services connectors

Un connecteur générique est aussi mis à disposition, sur demande, pour les autres professions, fournissant le service eHealthBox v3.

Compatibilité du connecteur technique

La compatibilité du connecteur technique version 3.18 avec les connecteurs Vitalink et Recip-e est validée. Attention, dans le cadre de l'intégration du connecteur technique de la plate-forme eHealth au sein du connecteur « business » Recip-e, nous vous recommandons l'utilisation des API disponibles au sein de ce connecteur pour les services Recip-e. Les API Recip-e disponibles au sein de notre package « physician » ont été retirées.

Download

Les connecteurs « java » et un fichier d'archive aves les connecteurs « .net » sont disponibles par un maven repository (repo.ehealth.fgov.be). La liste suivante contient des liens vers les connecteurs business des differentes catégories professionnelles et le connecteur technique.

- Physician
- Physiotherapist
- Nurse

- Pharmacy
- Dentist
- Midwife
- Practical Nurse
- Audiologist
- Dietician
- Occupational Therapist
- Logopedist
- Orthoptist
- Podologist
- Trussmaker
- Connecteur technique

Sécurité de l'information & GDPR

Nos réglementations, nos service en matière de sécurité et l'information relative au RGPD

1. Sécurité de l'information & General Data Protection Regulation

Conseiller en sécurité – Formations

Objectif de la formation de base en sécurité de l'information, organisée par la Plate-forme eHealth

La Plate-forme eHealth propose chaque année une formation de base sur le thème de la sécurité de l'information. Cette formation de base vise principalement à acquérir de larges connaissances dans les divers domaines de la protection de l'information.

Le programme comprend différents modules indépendants, c'est à dire qu'il est possible de s'inscrire à certains cours au choix sans obligatoirement suivre toute la formation. Au total, la formation complète représentent 7 jours.

Les cours sont donnés en néerlandais et en français (sessions différentes)

- Programme et modalités d'inscription

General Data Protection Regulation

Le Règlement général européen sur la protection des données (« European General Data Protection Regulation », en abrégé « EU GDPR ») introduit de nouvelles règles en matière de gestion et de protection de données à caractère personnel. La Commission européenne a voulu avec ce Règlement rendre aux citoyens le contrôle de leurs données à caractère personnel et simplifier le cadre réglementaire pour les entreprises internationales en uniformisant les règles au sein de l'Union européenne.

Ce règlement est entré en vigueur le 24 mai 2016. Une période de transition de deux ans a cependant été prévue. Les organisations ont ainsi le temps jusqu'au 25 mai 2018 pour se conformer aux nouvelles exigences du règlement EU GDPR. Contrairement à une directive, il n'y a pas de transposition dans la législation belge.

A travers cette page web, la Plate-forme eHealth se propose de rassembler les informations correctes concernant ce nouveau règlement.

Vous trouverez ci-après les liens vers les sources pertinentes:

- Le texte original du règlement EU GDPR
- Circulaire GDPR

Autres informations de la Commission européenne concernant le règlement EU GDPR

- EU GDPR factsheets
- Informations relatives à la portabilité des données
- Informations relatives au délégué à la protection des données (DPO)
- Informations relatives à l'identification du « responsable du traitement » ou de "l'autorité de contrôle chef de file"
- Publication de données à caractère personnel à des fins de transparence dans le secteur public
- Informations concernant l'analyse d'impact relative à la protection des données
- Toolkit de l'EDPS en ce qui concerne les restrictions en matière de protection de données à caractère personnel
- DPO corner

L'Autorité de Protection des Données (APD) a consacré une page web spécifique au règlement EU GDPR et élaboré un plan par étapes pour la mise en œuvre du règlement EU GDPR.

L'Autorité de Protection des Données (APD) a également rédigé d'initiative une recommandation concernant l'analyse d'impact relative à la protection des données (« data protection impact assessment » ou « DPIA »).

La BCSS a élaboré une roadmap en vue de l'implémentation du règlement EU GDPR.

La BCSS a adapté les normes minimales de sécurité de l'information afin de les rendre conformes au règlement EU GDPR.

Cette page web sera régulièrement mise à jour avec de nouveaux textes et adaptée en fonction des évolutions.

Architectures

Dans le cadre du développement et de la maintenance de ses projets et services, la plate-forme eHealth propose différentes structures et organisations des systèmes informatiques, appelés 'architectures'.

1. Architectures

1. Introduction
2. Développement d'un projet dans le cadre de la santé en ligne : Ce qu'il faut prévoir, comprendre et définir
    1. Contraintes en matière d'identification et de gestion des accès
        1. Enregistrement
        2. Authentification
        3. Autorisation
    2. Contraintes en matière d 'identification et de sécurité de l'information
        1. Confidentialité
        2. Intégrité
    3. Définition des standards de communication (langages/protocoles)
    4. Définition d'un ou plusieurs types de flux
        1. Volet 'identification et gestion des Accès' > distinction entre
            1. une application destinée à fonctionner sur le dispositif mobile de l'utilisateur (native app/public client)
            2. une application 'server based, hébergée par un partenaire et 'appelée' par l'utilisateur pour utilisation sur son outil mobile (confidential client)

1. Introduction

Dans le cadre du développement et de la maintenance de ses projets et services, la plate-forme eHealth propose différentes structures et organisations des systèmes informatiques, appelés 'architectures'.

Ces modèles sont élaborés sur base des besoins des partenaires mais sont tenus de respecter certaines normes de qualité et de sécurité et sont soumis à de constantes évolutions, en relation directe avec le secteur.

Lors du démarrage d'un projet, il importe donc de comprendre les différents systèmes proposés afin d'assurer une mise en place optimale des différents composants mais également d'anticiper les évolutions futures possibles.

La plate-forme eHealth propose principalement 2 types d'architectures :

- Une architecture de type SOA (Service oriented Architecture), destinée aux applications et services dont l'objectif est de fonctionner sur un seul dispositif, un seul ordinateur
- Une architecture de type REST (Representational State Transfert) destinée aux applications et services dont l'objectif est de fonctionner sur plusieurs dispositifs (simultanément un ordinateur, un smartphone, une tablette..)

Comme mentionné préalablement, l'informatique est un domaine en constante évolution. Au démarrage de la plate-forme eHealth, l'utilisation de dispositifs mobiles tels que les tablettes et smartphones n'en était qu'à ses débuts, raison pour laquelle l'architecture de type SOAP a majoritairement été développée et structure aujourd'hui encore de nombreux systèmes mis en place avec nos partenaires. La maintenance et le support pour ce modèle demeurent aujourd'hui parmi nos missions et responsabilités, néanmoins, parce qu'il n'est pas recommandé pour le développement de projets de type mobiles (elle ne permet notamment pas l'encryption des messages), la priorité est logiquement donnée à la promotion de l'architecture de type REST.

2. Développement d'un projet dans le cadre de la santé en ligne : Ce qu'il faut prévoir, comprendre et définir

2.1. Le projet doit intégrer des contraintes en matière d'identification et de gestion des accès

Afin de permettre l'accès mobile aux services eHealth, nous devons être en mesure d'authentifier TOUS les utilisateurs qui ont besoin d'utiliser les services de la plate-forme eHealth, quel que soit l'appareil ou le système utilisé pour se connecter.

Dans l'ensemble, nous distinguons deux catégories d'utilisateurs de nos services:

- les personnes (citoyens belges ou étrangers, professionnels, membres d'une organisation, mandataires)
- les systèmes

Il doit être possible de construire une identité numérique pour chacun d'entre eux.

2.1.1. Enregistrement

Tous les utilisateurs doivent être enregistrés dans une source authentique accessible à la plate-forme eHealth (directement ou indirectement)

- les personnes présentes dans le registre national avec un NISS (citoyens belges) ou NISS BIS (étrangers) (les groupes cibles de la plate-forme eHealth incluent les citoyens belges et les étrangers qui vivent ici ou à l'étranger)
- les systèmes doivent appartenir à une organisation qui peut être identifiée de manière univoque dans une source authentique pour le type spécifique d'organisation

Tout utilisateur doit être en mesure de prouver son identité en ligne avec une clé numérique. Au moins une clé doit lui être remise lors de l'enregistrement.

2.1.2. Authentification

L'authentification doit être supportée pour tous les types de clients : web (navigateur), natif (application mobile), desktop, serveur (backend, batch).

Pour s'authentifier, l'utilisateur doit utiliser l'une de ses clés numériques pour prouver qu'il est bien celui qu'il prétend être. Le modèle d'identité fédérée de la plate-forme eHealth doit être réutilisable pour tous les utilisateurs.

Toutes les clés numériques doivent répondre à des exigences minimales de sécurité.

Une personne doit pouvoir utiliser plusieurs dispositifs pour s'authentifier vis-à-vis nos services.

Une personne doit être en mesure de choisir un profil d'utilisateur applicable (c.-à-d. citoyen, qualité, appartenance à une organisation, mandat) qui sera utilisé pour l'authentification vis-à-vis de nos services.

Il doit être possible de transmettre l'identité choisie aux ressources demandées ou celles-ci doivent pouvoir la récupérer.

2.1.3. Autorisation

Les autorisations doivent être basées sur l'identité numérique choisie pour chacune des ressources demandées.

Il doit être possible de propager les autorisations aux ressources demandées ou celles-ci doivent pouvoir les obtenir.

Il doit être possible de laisser l'utilisateur décider s'il souhaite ou non donner des autorisations à l'application cliente qui utilisera ces autorisations en son nom.

Les utilisateurs doivent pouvoir révoquer les autorisations accordées.

2.2. Le projet doit intégrer des contraintes en matière d 'identification et de sécurité de l'information

2.2.1. Confidentialité

Toute communication entre le client et le serveur doit être considérée comme confidentielle et doit être protégée contre toute interception, au moins lorsqu'elle transite par un support non sécurisé, comme Internet.

Les données médicales doivent être protégées au niveau du message afin d'empêcher la divulgation des données lorsqu'on passe d'un point à un autre sur le réseau. Si le cryptage de bout en bout entre l'expéditeur d'origine et le destinataire final n'est pas nécessaire, il doit au moins être configuré point à point entre ces deux parties de sorte que les données médicales ne soient jamais envoyées sans protection entre deux points. La question de savoir si le point à point est suffisant est à décider par projet.

Les utilisateurs doivent pouvoir signer et chiffrer des messages sur différents appareils (ordinateur portable, smartphone et tablette) sans devoir transférer et exposer des clés numériques entre ces appareils.

2.2.2. Intégrité

Lorsque des données médicales sont envoyées du client au serveur, elles doivent être signées au niveau du message pour assurer l'intégrité du contenu.

2.3. Le projet doit définir les standards de communication parmi ceux proposés

`Identity & Access Management`

Voici la liste des langages/protocoles proposés

- SAML 2.0
- Oauth 2.0
- OIDC 1.0
- JWT
- Signed JWT Assertion
- PKCE

`Information Security`

Voici la liste des langages/protocoles proposés

- TLS
- JWS
- JWE
- JWK
- WebAuthn

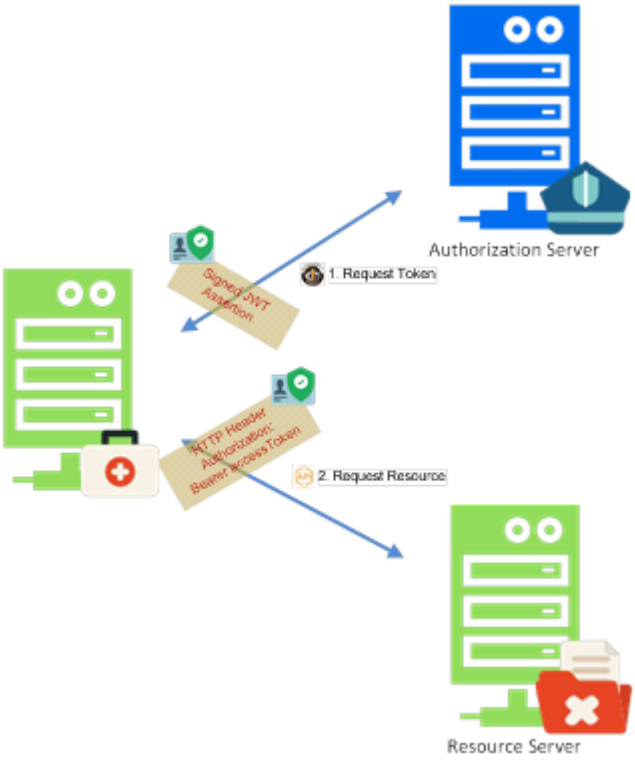
2.4. Le projet doit définir un ou plusieurs types de flux parmi ceux proposés

2.4.1. En ce qui concerne le volet ‘identification et gestion des Accès', il y a lieu de faire la distinction entre

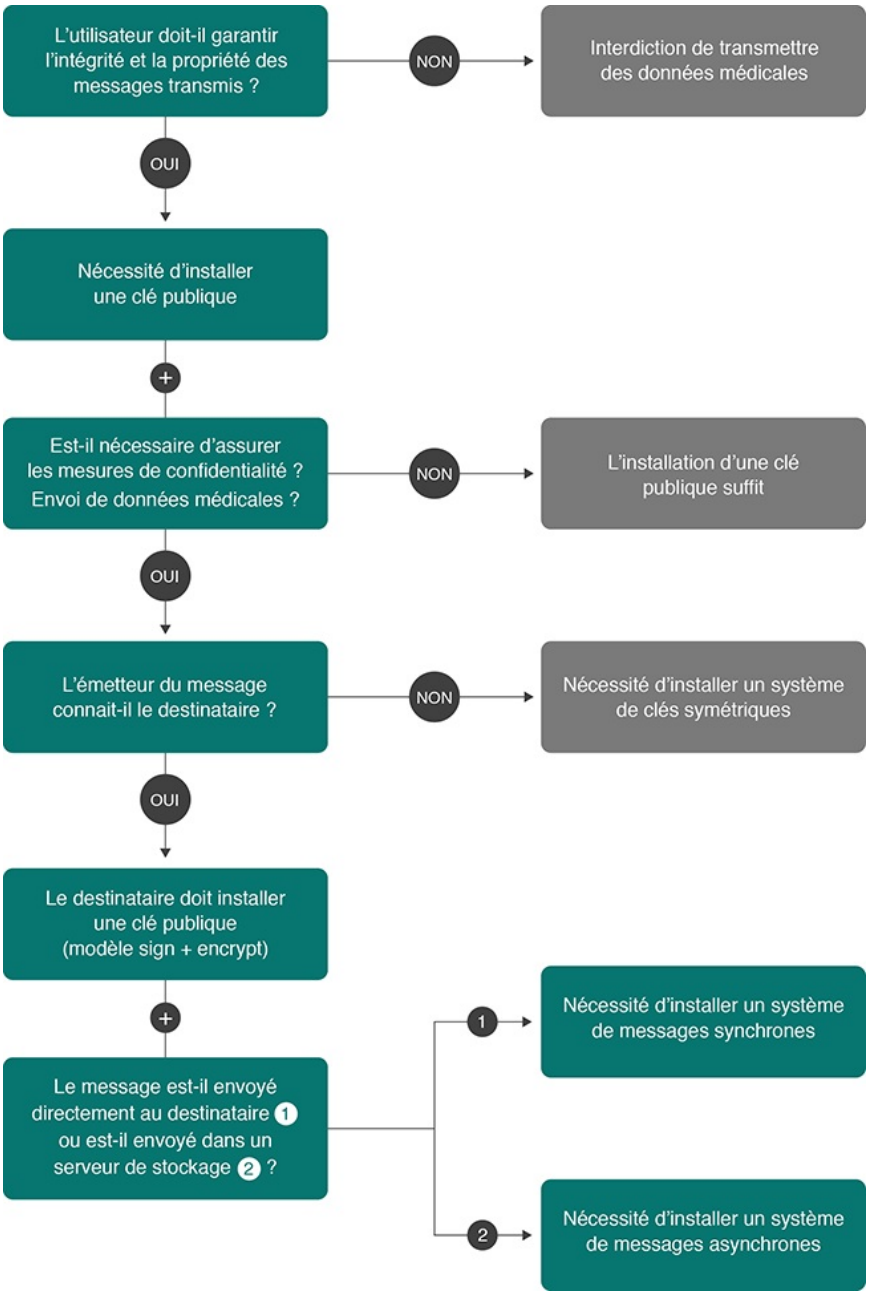
2.4.1.1. Une application destinée à fonctionner sur le dispositif mobile de l’utilisateur (native app/public client)

2.4.1.2. Une application ‘server based, hébergée par un partenaire et ‘appelée’ par l’utilisateur pour utilisation sur son outil mobile (confidential client)

2.4.1.3. Une application ne nécessitant pas d'intervention humaine, destinée à fonctionner automatiquement de serveur à serveur, pour la mise à jour automatique de banques de données par exemple (system client)

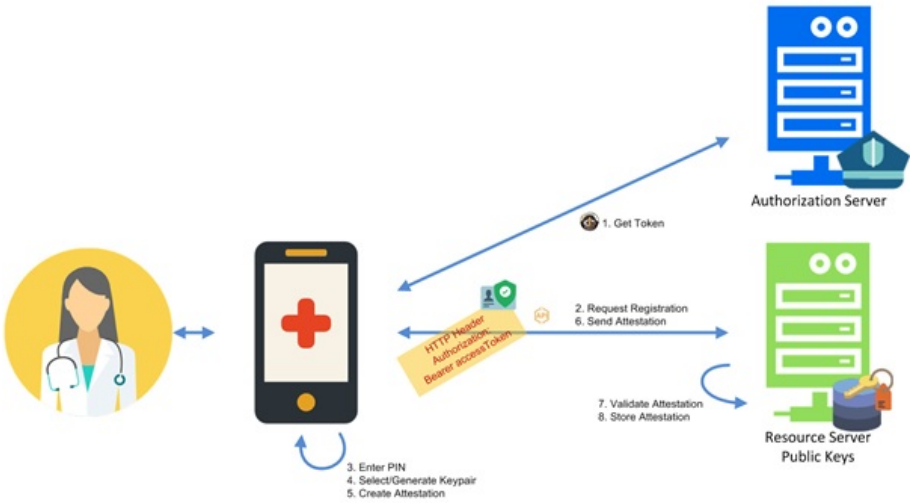


2.4.2. En ce qui concerne le volet 'Sécurité de l'information', il y a lieu de s'interroger sur plusieurs aspects

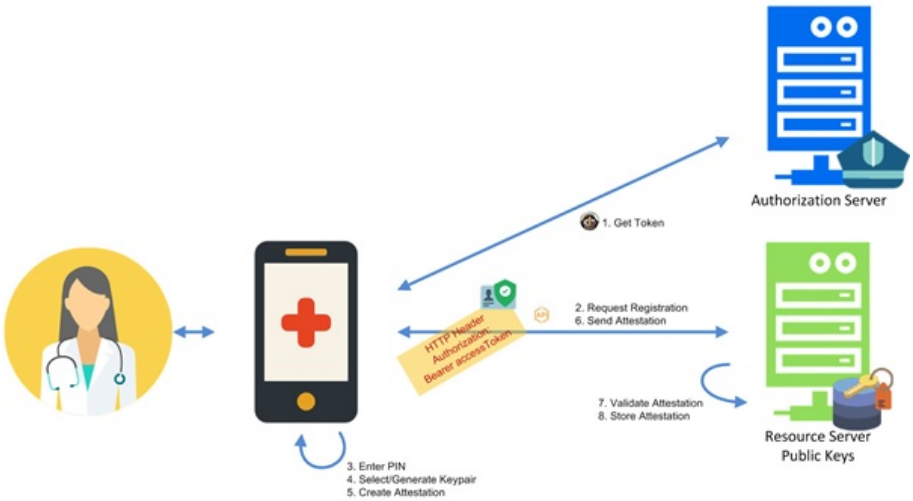


3. Cas pratiques schématisés

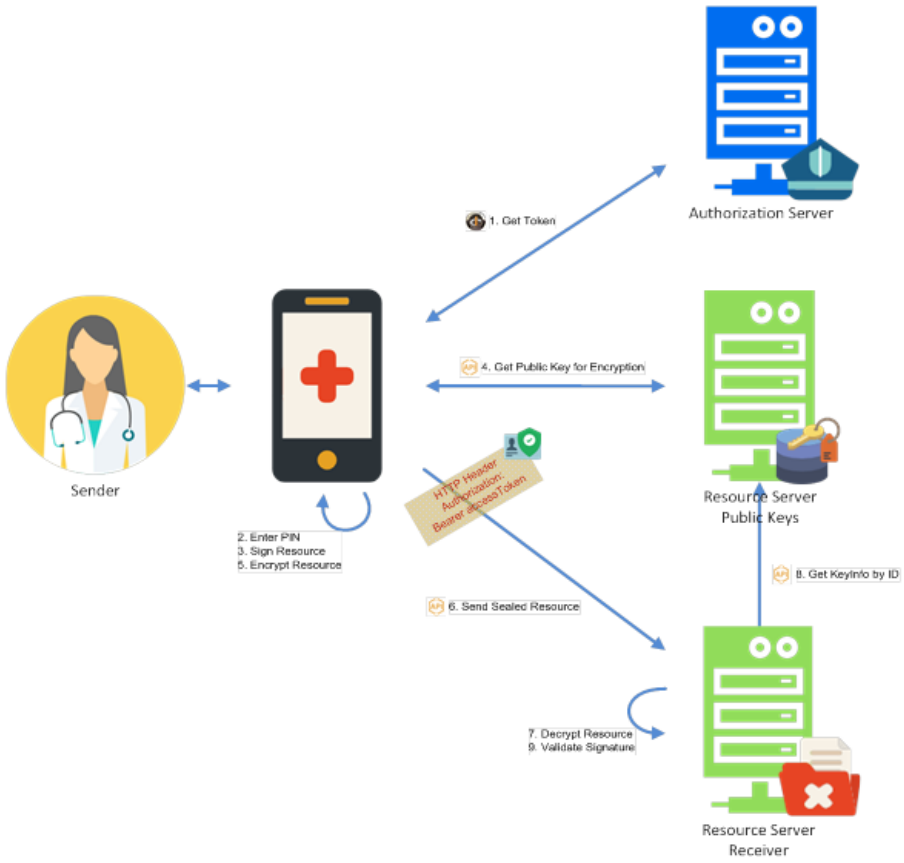
3.1. Enregistrement d'une clé publique (use case :enregistrement d'une clé dans le cadre de la demande d'un certificat eHealth au sein d'une architecture de type SOAP)



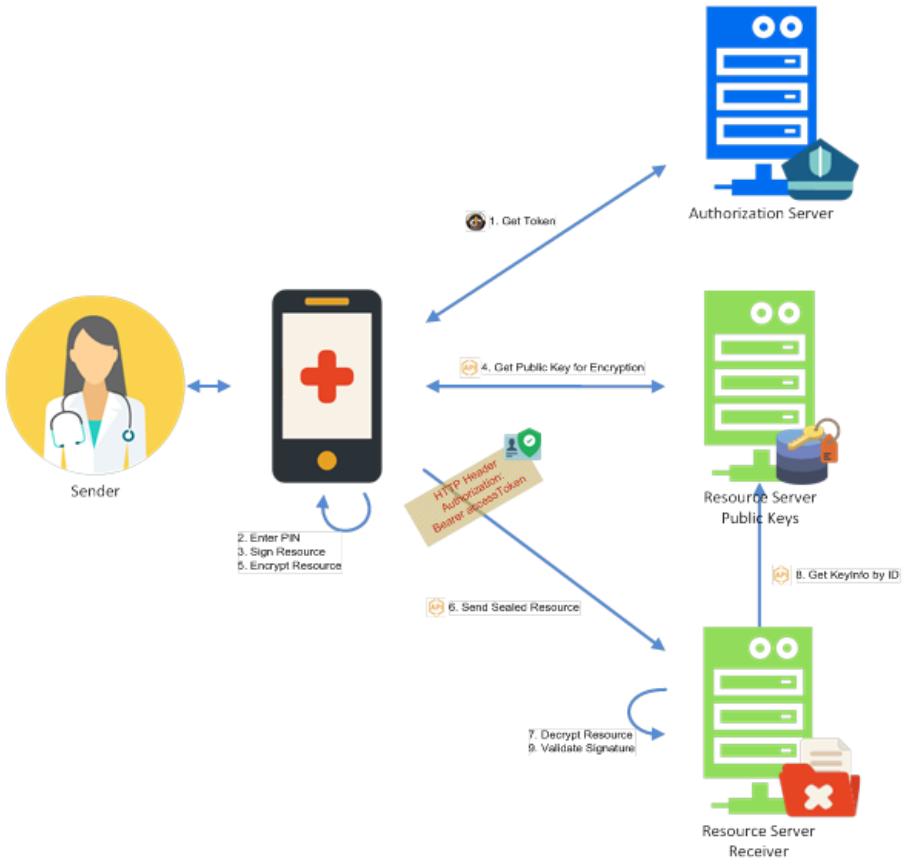
3.2. Enregistrement d'une clé symétrique (use case : enregistrement d'une clé dans le cadre de Recip-e)



3.3. Destinataire connu, communication synchrone (use case le plus fréquent : lorsqu'un client doit contacter directement un service de plate-forme eHealth qui impose le système d'encryption)



3.4. Destinataire connu, communication asynchrone (use case: eHealthBox)



3.5. Destinataire inconnu (use case : Recip-e)