Système de cryptage end-to-end

Que sont les services End-to-End Encryption de la plate-forme eHealth ?

Les services End-to-End Encryption (ETEE) (également appelés services de chiffrement ou de cryptage) de la plate-forme eHealth sont 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 (SOAP & REST) et KeyDepot (REST) pour le chiffrement vers un destinataire connu ;
- KGSS (SOAP & REST) 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 des services End-to-End Encryption ?

Le service web ETKDepot 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. Le service REST permet également de rechercher le détenteur d'un certificat ;

- 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) ;
- le service REST permet également de supprimer une clé existante par son détenteur.

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.

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

- la création d'une paire de clés (la clé publique sera stockée par la plate-forme eHealth et sera accessible à tous les publics) ;
- l'ajout, par son détenteur, d'informations pour une clé publique déjà existante ;
- la recherche d'une clé publique ;
- la suppression, par son détenteur, de clés publiques ;
- la recherche de toutes les clés publiques liées à une personne ;
- la recherche de l'attestation object liée à une clé publique ;
- la recherche d'informations sur le détenteur d'une clé.

En pratique

Dépendances, recommandations & avertissements

Pour utiliser le service web ETKDepot, le service web KGSS ou le service web KeyDepot, le prestataire de soins ou le patient devra disposer d'un logiciel médical ayant intégré ce service. Les deux services web KGSS et ETKDepot 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 des services 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.

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