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.

Si vous disposez d'une version Java plus récente que Java 8, le lien ci-dessus **ne peut plus** être utilisé pour démarrer l'application. C'est pourquoi l'application est également proposée via un fichier ZIP téléchargeable. Dans ce cas, vous pouvez extraire le fichier dans un dossier sur votre ordinateur et démarrer le programme via le fichier .cmd (Windows) ou .sh (MacOS, Linux).

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 actifs dans le secteur belge des soins de santé, de tester l'intégration de nos services de base. Pour plus d'information, consultez les pages dédiées aux environnements de test et 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 de session (session token) permettant l'accès à ces services ;
- la possibilité de chiffrer des messages, par exemple dans le cadre de l'utilisation d'une eHealthBox (certificat et 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 service web dédié, ETEE ETKDepot).

En pratique

Dépendances, recommandations et 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 pas de facto 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 méthode hybride pour la demande d'un certificat eHealth.

Pour les institutions de soins, il faut :

- que leur profil soit enregistré dans une source authentique validée, en ce compris le titulaire du certificat autorisé au nom de l'institution ;
- que le détenteur du certificat dispose d'un moyen d'authentification considéré comme fort ;
- que les normes minimales de la sécurité sociale soient respectées ;
- que le fonctionnement interne de l'institution de soins garantisse que seules les personnes autorisées ont accès au système ;

- qu'elles disposent d'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 ;
  - le titulaire du certificat est donc 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.

Evolution du ETEE Certificate Manager (RSA - ECC)

Pour rappel ou information, un changement de méthode cryptographique pour les certificats eHealth est en cours.

Une nouvelle méthode cryptographique a été choisie pour améliorer la sécurité et les performances, à savoir la cryptographie à courbe elliptique (ECC).

ECC 384 remplacera prochainement l'approche actuelle RSA 2048. Les deux types de certificats (ECC & RSA) seront toujours utilisables en parallèle, mais les solutions pour obtenir de nouveaux certificats (eHealth Certificate Manager) ne généreront plus que des certificats ECC (les ETKs resteront RSA).

Deux versions en ACC

Pour permettre une période de transition en ACC, une version est actuellement disponible en parallèle pour continuer à commander des certificats RSA.

Si vous ne savez pas quel lien utiliser, nous vous recommandons d'utiliser le 'nouveau' pour utiliser les nouveaux certificats ECC.

Liens (URLs) vers les versions :

Certificats ECC (version 2025.1.0)

Certificats RSA (version 2023.2.0)

Si vous avez un doute sur la version utilisée (et donc le type de certificat demandé), vous pouvez vérifier que la version de l'application correspond.