



Procédure de création de certificats de la plate-forme eHealth

Contenu

1. Introduction	3
1.1 But du service	3
1.2 Exigences opérationnelles	3
1.3 Exigences techniques	3
1.4 Type de certificat	4
2. Procédure de demande de certificat.....	5
2.1 Introduction de la demande d'un certificat	5
2.1.1 Menu principal	6
2.1.2 Conditions d'utilisation des certificats eHealth	7
2.1.3 Choisissez votre type d'utilisateur	7
2.1.3.1 Vous avez la nationalité belge.....	7
2.1.3.1.1 Insérez votre carte eID	8
2.1.3.1.2 Authentification.....	8
2.1.3.1.3 Choisissez votre type de certificat	9
2.1.3.1.4 Données de contact	9
2.1.3.1.4.1 Données de contact pour un certificat personnel	9
2.1.3.1.4.2 Données de contact pour une organisation	10
2.1.3.1.5 Fournissez votre mot de passe	11
2.1.3.1.6 Aperçu de la demande	11
2.1.3.1.7 Envoyer la demande	12
2.1.3.1.8 Signez en utilisant votre logiciel eID	12
2.1.3.2 Vous n'avez pas la nationalité belge	13
2.1.3.2.1 Données personnelles	13
2.1.3.2.2 Données de contact	13
2.1.3.2.3 Fournissez votre mot de passe	14
2.1.3.2.4 Envoi de la demande	14
2.1.3.2.5 Validation de la demande	14
2.1.3.2.6 Authentification de la demande	15
2.1.3.2.7 Création de la demande de certificat	15
2.2 Validation de la demande par eHealth	16
2.3 Finalisation de la demande et enregistrement du certificat	17
2.3.1 Sélectionner le fichier keystore	17
2.3.2 Finalisation de l'enregistrement et création de la clé d'encryptage	18
3. Modifiez le mot de passe de votre keystore.....	19
4. Renouvellement d'un certificat.....	22
4.1 Renouvelez votre certificat eHealth	22
4.2 Complétez votre demande de renouvellement	23
4.3 Activez votre ETK de renouvellement	23
5. Sécurité	25
6. Aide	25
7. Annexe.....	26
7.1 Comprendre le « Distinguished Name » (DN) de votre certificat	26
7.1.1 Nom du pays	26
7.1.2 Nom de l'organisation	26
7.1.3 Nom d'unité organisationnelle	26
7.1.4 Nom d'unité organisationnelle	27
7.1.5 Nom d'unité organisationnelle	27
7.1.6 Nom d'unité organisationnelle	28
7.1.7 Nom commun	28
7.1.8 Exemple	29
7.2 Autorité de certification	29

1. Introduction

1.1 But du service

Ce manuel d'utilisateur décrit la procédure afin d'obtenir un certificat eHealth et une clé d'encryption.

Le certificat d'authentification eHealth est utilisé pour chaque appel aux services web de la plate-forme eHealth. Il permet de s'authentifier en tant qu'acteur de soins de santé.

Lors de l'utilisation du service de base de cryptage, un certificat de cryptage est nécessaire afin de créer une double clé de chiffrement.

Vous pouvez lancer l'application « Certificate Manager » en cliquant sur :

http://www.ehealth.fgov.be/JWS/ETEE/etee-requestor_fr.jnlp

1.2 Exigences opérationnelles

Un certificat est assigné :

- Aux personnes physiques qui sont enregistrées dans la source authentique « Cadastre des professions de santé » ou enregistrées après validation de la plate-forme eHealth ;
- Aux représentants autorisés pour le compte d'institutions enregistrées auprès du secteur de la santé belge.

1.3 Exigences techniques

Si vous avez la nationalité belge ou résidez en Belgique, vous devez disposer :

- d'une carte d'identité belge valide;
- d'un lecteur eID;
- du middleware nécessaire afin d'utiliser l'eID (plus d'informations pour télécharger la dernière version du logiciel eID sur <http://eid.belgium.be>);
- de la version 1.6. de Java ou supérieure à 32 bits (plus d'informations pour télécharger la dernière version de Java sur <http://www.java.com/fr/download/>).

Si vous n'avez pas la nationalité belge et si vous ne résidez pas en Belgique, vous devez disposer uniquement :

- de la version 1.6. de Java ou supérieure à 32 bits (plus d'informations pour télécharger la dernière version de Java sur <http://www.java.com/fr/download/>).

1.4 Type de certificat

Il existe deux types de certificats :

- Les certificats de test : utilisés par les IT et prestataires de soins afin de tester l'intégration des services de bases eHealth;
- Les certificats de production : utilisés par les prestataires de soins pour accéder aux services de bases eHealth.

En fonction de l'utilisateur, l'environnement à utiliser peut différer (environnement de test et/ou environnement de production) :

	Certificats de test ¹	Certificats de production
Prestataires de soins de santé ²	oui	oui
IT ³	oui	non

Ce manuel décrit la procédure de création des certificats de production.

¹ Le certificat de test permet de tester en tant que prestataires de soins des données fictives dans l'environnement d'acceptation.

² Prestataires de soins professionnels, actifs dans le secteur belge des soins de santé.

³ Intégrateurs IT, fournisseurs de logiciels pour les applications à l'attention des prestataires de soins dans le secteur belge des soins de santé.

2. Procédure de demande de certificat

La procédure de demande d'un certificat eHealth comprend trois phases :

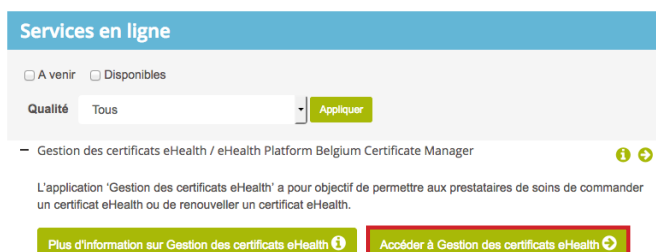
1. L'introduction de la demande d'un certificat eHealth ;
2. La validation de la demande par eHealth ;
3. La finalisation de la demande et l'enregistrement du certificat .

2.1 Introduction de la demande d'un certificat

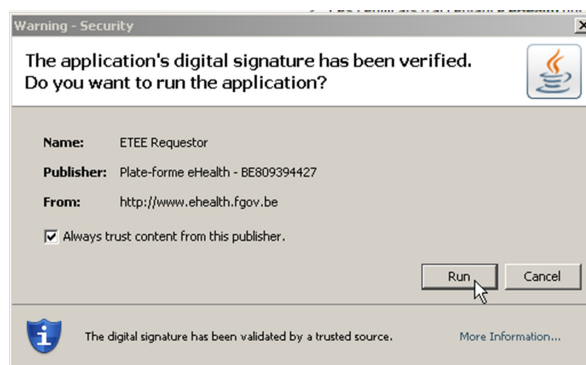
Vous devez introduire la demande au moyen de l'application « Certificate Manager » disponible sur le portail eHealth.

Attention, si vous n'avez pas la nationalité belge et si vous ne résidez pas en Belgique, veuillez suivre la procédure décrite sur <https://www.ehealth.fgov.be/ehealthplatform/fr/service-certificats-ehealth> (sous "Conditions générales / Contrat comprenant les conditions générales d'utilisation des certificats eHealth") pour obtenir l'accès au service en ligne.

Sur le portail, cliquez sur « Professionnels de la santé ». Sous « Services en ligne », cliquez sur « Gestion des certificats eHealth/eHealth Platform Belgium Certificate Manager » et ensuite « Accéder à Gestion des certificats eHealth » : http://www.ehealth.fgov.be/JWS/ETEE/etee-requestor_fr.jnlp



Après avoir cliqué sur le lien du portail, l'application Java est lancée. Vous devez alors indiquer que vous faites confiance au contenu de l'application. Cochez « Always trust content from this publisher » et cliquez sur « Run ».

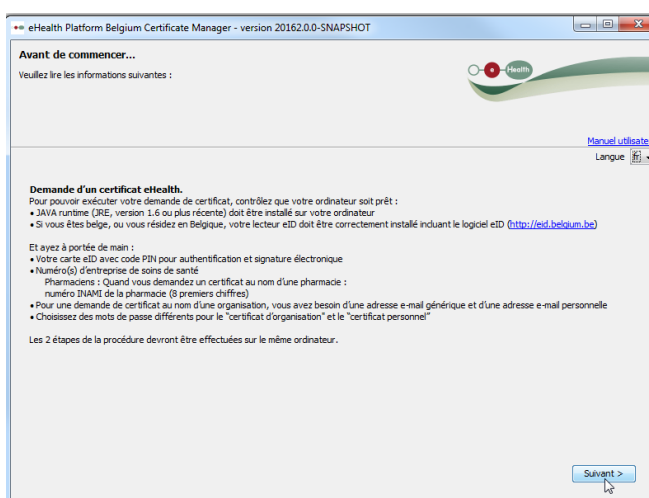


L'écran suivant vous rappelle les différentes exigences techniques, il faut disposer :

- De la version 1.6. de Java minimum ;
- D'un lecteur eID correctement installé.

Vous devez également tenir à portée de main les cartes et numéros suivants :

- Votre carte d'identité et le code PIN afférent (uniquement pour une personne de nationalité belge ou résident en Belgique);
- Uniquement pour les organisations : le numéro INAMI, le numéro BCE (i.e. le numéro d'entreprise) ou le numéro EHP (eHealth Partner) qui correspond à votre institution (par exemple : à votre cabinet médical ou à votre pharmacie).

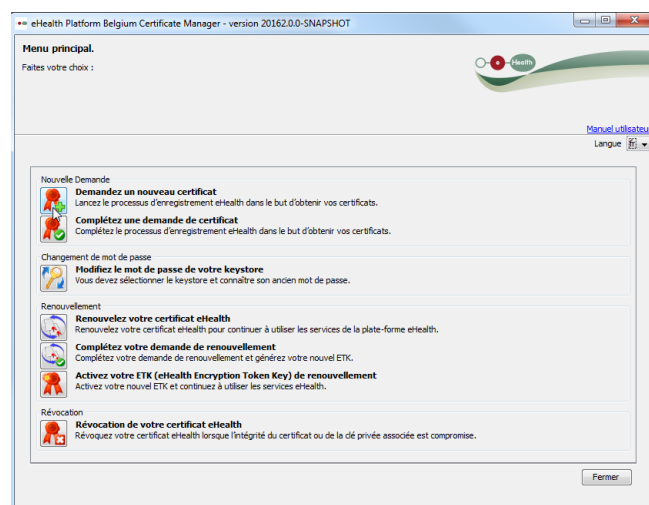


Cliquez sur « Suivant ».

2.1.1 Menu principal

Le menu principal vous permet de sélectionner l'action à entreprendre.

Pour lancer la procédure d'enregistrement d'un nouveau certificat, cliquez sur le symbole à côté de « Demandez un nouveau certificat ».

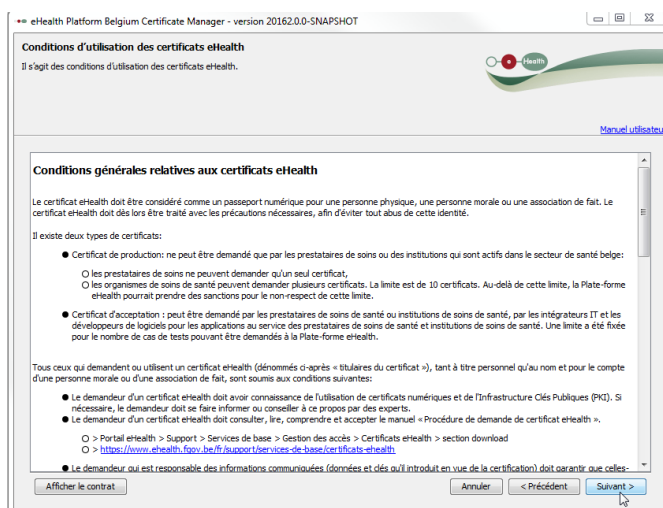


i

Vous pouvez afficher le contrat en version PDF en cliquant sur le bouton « Afficher le contrat ».

2.1.2 Conditions d'utilisation des certificats eHealth

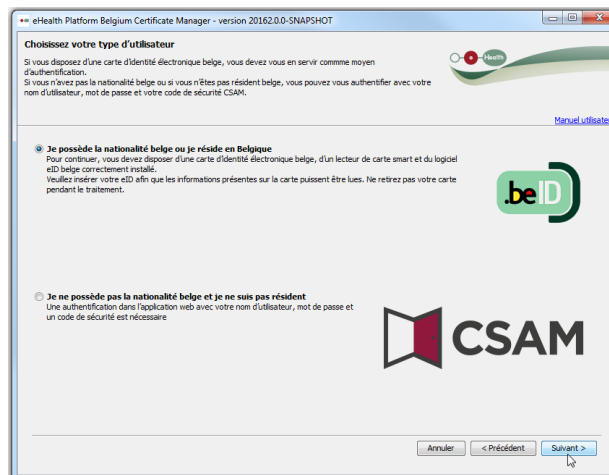
Il vous est demandé de lire et d'accepter le contrat des certificats eHealth. Veuillez lire le texte minutieusement. Cliquez sur « Suivant ».



2.1.3 Choisissez votre type d'utilisateur

2.1.3.1 Vous avez la nationalité belge ou résidez en Belgique

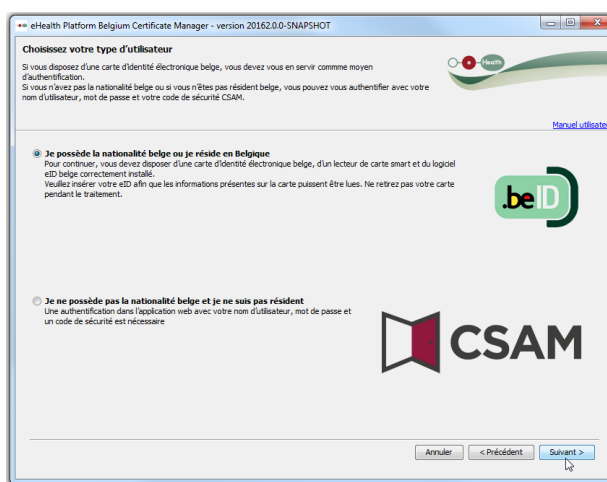
Si vous avez la nationalité belge ou si vous résidez en Belgique, cochez la première option.



2.1.3.1.1 Insérez votre carte eID

Soyez certain que tous les hardware et logiciels eID soient correctement installés. Si vous avez besoin d'aide pour configurer et vérifier votre installation, veuillez suivre le lien ou cliquer sur le symbole eID⁴.

Le bouton « Suivant » ne devient disponible que lorsque votre carte eID a été correctement lue.



⁴ eHealth n'apportera du soutien eID que si votre hardware et logiciel eID sont correctement installés, configurés et fonctionnels.

2.1.3.1.2 Authentification

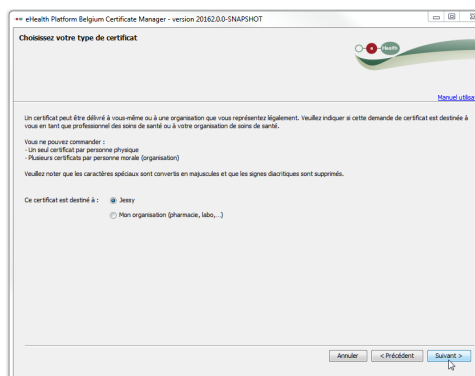
Il vous est demandé d'introduire le code PIN de votre carte eID afin de vérifier vos droits d'accès.



Attention : 3 tentatives infructueuses bloqueront votre carte eID. Si vous avez perdu votre code PIN, veuillez contacter votre autorité communale afin d'obtenir de l'aide.

2.1.3.1.3 Choisissez votre type de certificat

Veillez choisir si le certificat est pour votre usage personnel ou pour une organisation à laquelle vous êtes associé.

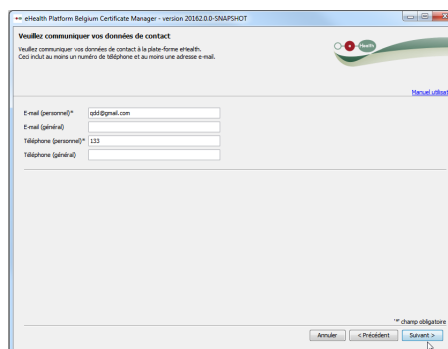


2.1.3.1.4 Données de contact

2.1.3.1.4.1 Données de contact pour un certificat personnel

Veillez introduire les données de contact demandées.

Il vous sera seulement demandé d'introduire votre adresse e-mail et numéro de téléphone personnel.



Veillez noter que l'adresse e-mail et numéro de téléphone personnels ne signifient pas votre adresse e-mail ou numéro de téléphone privés. Vos données de contact personnalisées seront celles utilisées au sein de l'organisation lors de l'envoi des notifications.



Les champs marqués d'une « * » sont obligatoires.

i

Seul l'administrateur ou le mandataire de l'organisation peut faire la demande d'un certificat pour une organisation. Aucune autre demande ne sera traitée. Le formulaire de procuration est disponible sur la page « Support » du portail eHealth .

i

En fonction du type d'organisation, certains champs s'afficheront.

i

Une description de chaque champ est fournie par l'assistant

**i**

Le champ « Nom de l'organisation » doit comporter uniquement les caractères suivants:

- Lettres (A-Z),
- Chiffres (0-9),
- Tiret (-),
- Underscore (_),
- Espace (<space>).

2.1.3.1.4.2 Données de contact pour une organisation

Si le certificat est pour une organisation à laquelle vous êtes associé, vous avez deux options :

Cas de figure 1 : Vous choisissez une organisation pour laquelle vous êtes reconnu comme gestionnaire.

Vous devez fournir toutes les données demandées sur l'organisation.

Choisissez l'organisation pour laquelle vous souhaitez demander un certificat. Le système proposera toutes vos organisations connues.

Les champs « ID de l'application » et « Utilisation » sont facultatifs.

Le champ « ID de l'application » vous permet d'identifier un certificat lorsque vous disposez de plusieurs certificats par organisation.

Pour le champ « Utilisation », sélectionnez les services de base auxquels votre organisation veut faire appel avec le certificat demandé. Un accord du comité sectoriel est nécessaire pour l'usage de chacun de ces services de base.

Cliquez sur « Suivant ».

Cas de figure 2 : Vous choisissez une autre organisation pour laquelle vous pouvez gérer des certificats.

Cliquez sur « Suivant ».

i

Soyez certain de vous souvenir de votre mot de passe. Perdre le mot de passe signifie que vous perdrez l'accès à vos clés personnelles et ne serez plus capable de vous identifier ni de décrypter les messages qui vous seront envoyés. Vous devrez alors contacter eHealth, révoquer votre ancien certificat et demander votre nouveau certificat.

Le nom de l'organisation doit être le nom exact figurant dans le Moniteur belge.

Vous devez fournir toutes les données demandées sur l'organisation.

Sélectionnez le type d'organisation via le menu déroulant.

Complétez le Nom de l'organisation, le Numéro d'identification.

Le champ ID de l'application vous permet d'identifier un certificat lorsque vous disposez de plusieurs certificats par organisation.

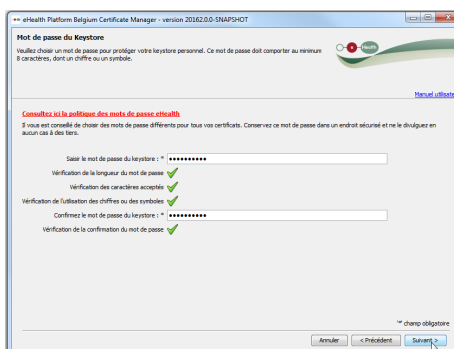
Pour le champ Utilisation, sélectionnez le(s) service(s) dans le cadre de la demande du certificat.

Cliquez sur « Suivant ».

2.1.3.1.5 Fournissez votre mot de passe

Veillez introduire un mot de passe de qualité afin de protéger votre keystore. Les vérificateurs de qualité vous donneront un feedback en temps réel sur la qualité de votre mot de passe. Ce mot de passe vous sera demandé lors de chaque ouverture de session.

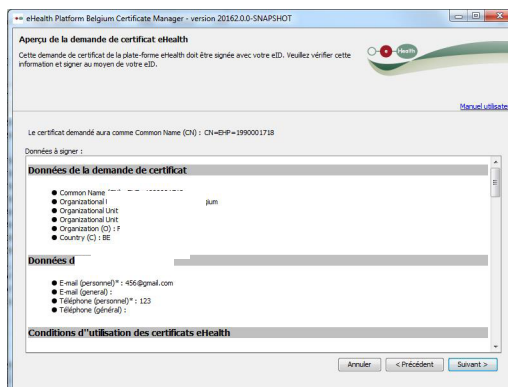
Il vous sera ensuite demandé d'introduire ce mot de passe une deuxième fois afin d'en confirmer l'exactitude. Cliquez sur « Suivant ».



2.1.3.1.6 Aperçu de la demande

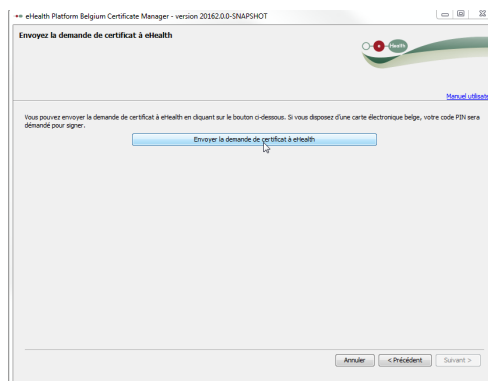
Cet écran affiche un aperçu de toutes les informations contenues dans le fichier de demande de signature du certificat eHealth. Veillez passer ces informations en revue et éventuellement les corriger en retournant dans un des écrans précédents en cliquant sur « Précédent ».

En cliquant sur « Suivant », vous arriverez à l'application du logiciel de contrôle de votre carte eID.



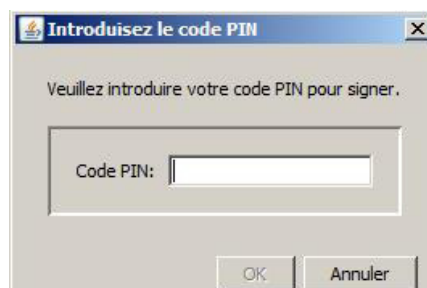
2.1.3.1.7 Envoyer la demande

Veillez confirmer l'envoi de la demande en cliquant sur « Envoyer la demande de certificat eHealth ».



2.1.3.1.8 Signez en utilisant votre logiciel eID

Il vous sera maintenant demandé d'introduire à nouveau le code PIN de votre carte eID afin de signer la demande.



Attention : 3 tentatives infructueuses bloqueront votre carte eID. Si vous avez perdu votre code PIN, veuillez contacter votre autorité communale afin d'obtenir de l'aide.

2.1.3.2 Vous n'avez pas la nationalité belge et vous ne résidez pas en Belgique

Veillez suivre la procédure décrite sur <https://www.ehealth.fgov.be/ehealthplatform/fr/service-certificats-ehealth> (sous "Méthode hybride pour la demande d'un certificat eHealth par des prestataires de soins étrangers, non-résidents en Belgique (sans carte eID) et actifs dans le secteur des soins de santé belge") afin d'obtenir l'accès au service en ligne. Une fois le service en ligne lancé, cochez la deuxième option.

Choisissez votre type d'utilisateur

Si vous disposez d'une carte d'identité électronique belge, vous devez vous en servir comme moyen d'authentification.
Si vous n'avez pas la nationalité belge ou si vous n'êtes pas résident belge, vous pouvez vous authentifier avec votre nom d'utilisateur, mot de passe et votre code de sécurité CSAM.

Je possède la nationalité belge ou je réside en Belgique
Pour continuer, vous devez disposer d'une carte d'identité électronique belge, d'un lecteur de carte smart et du logiciel eID belge correctement installé.
Veillez insérer votre eID afin que les informations présentes sur la carte puissent être lues. Ne retirez pas votre carte pendant le traitement.

Je ne possède pas la nationalité belge et je ne suis pas résident
Une authentification dans l'application web avec votre nom d'utilisateur, mot de passe et un code de sécurité est nécessaire.

Annuler < Précédent Suivant >

i

Les champs marqués d'une « * » sont obligatoires.

i

Une description de chaque champ est fournie par l'assistant



2.1.3.2.1 Données personnelles

Vous devez fournir toutes les données personnelles demandées.

Remplissez vos données personnelles

Vous devez remplir vos données personnelles.

NISS (Numéro bio) * [input field] [help icon]

Prénom * [input field] [help icon]

Nom de famille * [input field] [help icon]

Annuler < Précédent Suivant >

2.1.3.2.2 Données de contact

Veillez introduire les données de contact demandées.

Veuillez communiquer vos données de contact

Veillez communiquer vos données de contact à la plate-forme eHealth.
Ceci inclut au moins un numéro de téléphone et au moins une adresse e-mail.

E-mail (personnel) * [input field]

E-mail (général) [input field]

Téléphone (personnel) * [input field]

Téléphone (général) [input field]

Annuler < Précédent Suivant >

i

Soyez certain de vous souvenir de votre mot de passe. Perdre le mot de passe signifie que vous perdrez l'accès à vos clés personnelles et ne serez plus capable de vous identifier ni de décrypter les messages qui vous seront envoyés. Vous devrez alors contacter eHealth, révoquer votre ancien certificat et demander votre nouveau certificat.

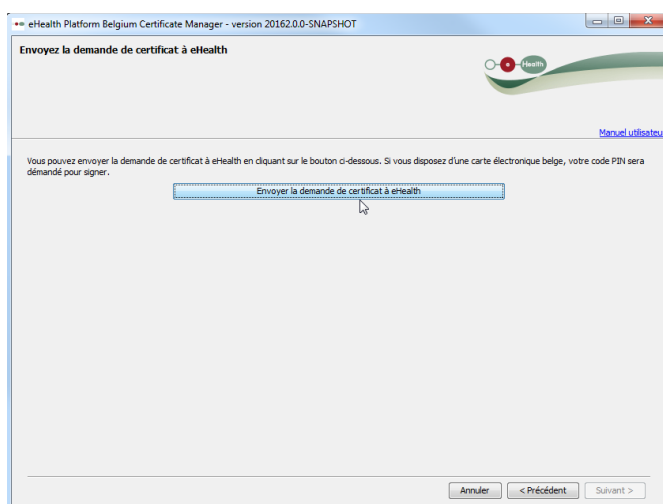
2.1.3.2.3 Fournissez votre mot de passe

Veillez introduire un mot de passe de qualité afin de protéger votre keystore. Les vérificateurs de qualité vous donneront un feedback en temps réel sur la qualité de votre mot de passe. Ce mot de passe vous sera demandé lors de chaque ouverture de session.

Il vous sera ensuite demandé d'introduire ce mot de passe une deuxième fois afin d'en confirmer l'exactitude. Cliquez sur « Suivant ».

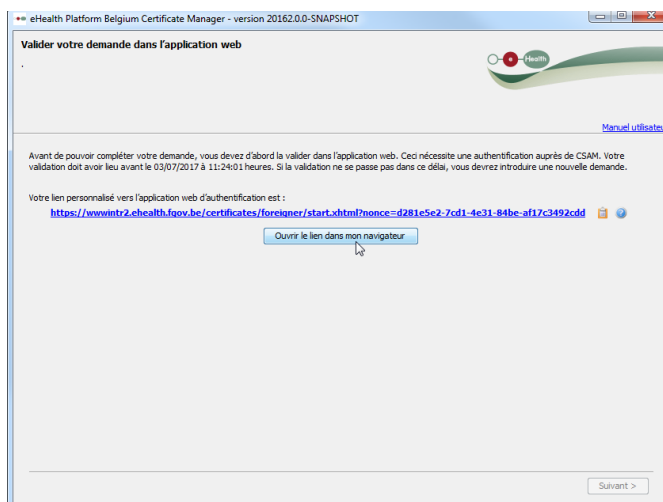
2.1.3.2.4 Envoi de la demande

Cliquez sur « Envoyer la demande de certificat à eHealth ».



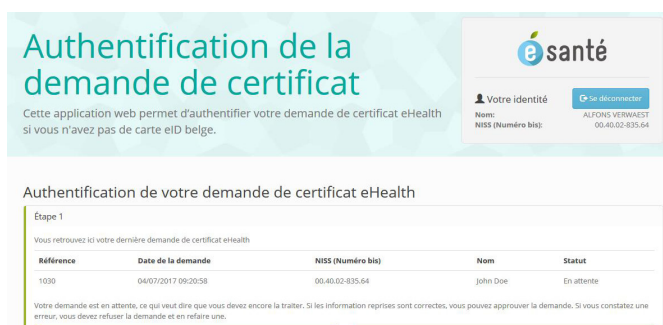
2.1.3.2.5 Validation de la demande

Il vous est demandé de valider votre demande dans une application web. Cliquez sur le lien ou un des deux boutons.



2.1.3.2.6 Authentification de la demande

Pour authentifier votre demande, cliquez sur « Approuver » dans l'application web.



Vous devez, ensuite, télécharger, remplir le contrat et l'envoyer par courrier postal ou par e-mail avec une copie recto/verso de votre carte d'identité.

Conditions d'utilisation des certificats eHealth

Ce contrat est conclu entre la plate-forme eHealth et

Nom *: _____

Prénom *: _____

avec numéro NISS (n° Bis, 11 chiffres) *: _____

dénommé ci-après l'UTILISATEUR

Conditions générales relatives aux certificats eHealth

Le certificat eHealth doit être considéré comme un passeport numérique pour une personne physique, une personne morale ou une association de fait. Le certificat eHealth doit dès lors être traité avec les précautions nécessaires, afin d'éviter tout abus de cette identité.

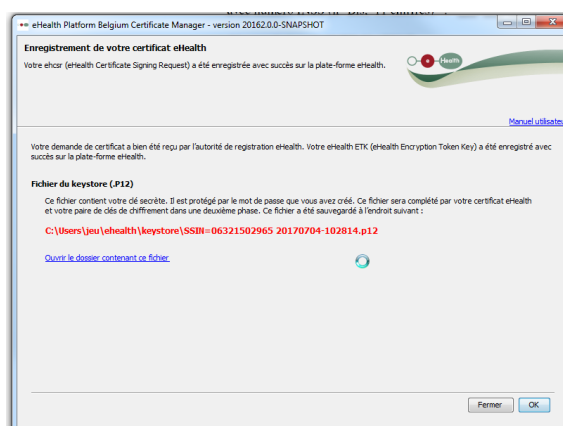
Il existe deux types de certificats:

La réception de ce contrat est la condition pour démarrer le processus de validation (voir 2.2)

Vous recevrez, après quelques jours ouvrables, un premier e-mail vous confirmant l'approbation et un deuxième vous confirmant la délivrance.

2.1.3.2.7 Création de la demande de certificat

L'écran suivant indique que la demande de certificat a été introduite avec succès.



Le fichier .P12 contient votre clé privée protégée par un mot de passe. N'envoyez jamais ce fichier à eHealth ou une autre partie. Gardez le fichier .P12 et son mot de passe en sécurité à tout moment.

Votre fichier se trouve dans un dossier de stockage eHealth personnel. Vous pouvez directement ouvrir ce dossier sur votre ordinateur. Il se trouve dans votre « home » directory sous : \eHealth\keystore\...

Vous pourrez alors compléter votre demande.

2.2 Validation de la demande par eHealth

Votre demande a été délivrée à la plate-forme eHealth. La plate-forme eHealth va, à présent, vérifier si vous disposez des autorisations nécessaires. Cette phase peut prendre quelques jours.

Vous allez recevoir deux notifications distinctes par e-mail :

1. Le premier pour confirmer que vous respectez les exigences de la plate-forme eHealth pour l'obtention d'un certificat et que le certificat d'authentification va être généré.

Le cas échéant, vous recevrez une notification vous indiquant que l'obtention du certificat vous est refusée ainsi que la raison du refus. Dans ce cas, une nouvelle demande devra être introduite ;

```

    Cher DART VAN RR,

    Votre demande de certificat d'authentification eHealth (Common Name=004106310) avec numéro de demande 5453 a été acceptée et
    validée.
    Votre certificat sera produit dans les plus brefs délais. Vous recevrez une notification par e-mail lorsque votre certificat eHealth
    sera disponible.

    Meilleures salutations,
    Plate-forme eHealth - Gestion des accès
    -----
    Gewachte DART VAN RR,

    Uw aanvraag van een eHealth-authenticatiecertificaat (Common Name=004106310) met aanvraagnummer 5453 werd gevalideerd en werd
    aan de certificatie-autoriteit overgemaakt. Uw certificaat zal zo snel mogelijk worden aangemaakt.
    Zodra uw eHealth-authenticatiecertificaat beschikbaar is, ontvangt u een notificatiemail.

    Met vriendelijke groeten,
    eHealth platform - Toegangbeheer
  
```

2. Le deuxième pour confirmer que le certificat a été généré et que vous devrez réinitialiser le « Certificate Manager » afin de télécharger le certificat d'authentification et de créer votre clé d'encryptage. Cet e-mail contient la référence de votre demande.

```

    Cher DART VAN RR,

    Le certificat d'authentification eHealth relatif à votre demande de certificat (Common Name=004106310) validé avec numéro de
    demande 5453 a été produit par l'autorité de certification et fourni à la plate-forme eHealth.
    Veuillez exécuter l'étape suivante ("Complétez une demande de certificat") du STIX-requestor à partir du 13/06/2017 08:30:51 afin
    d'acquiescer votre certificat.
    Après cette exécution, le certificat sera valable.

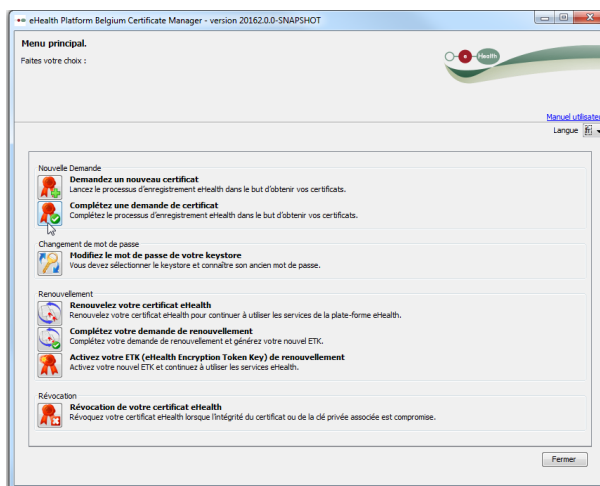
    Meilleures salutations,
    Plate-forme eHealth - Gestion des accès
    -----
    Gewachte DART VAN RR,

    Het eHealth-authenticatiecertificaat voor uw gevalideerde certificatieaanvraag (Common Name=004106310) met aanvraagnummer 5453
    werd door de certificatie-autoriteit geproduceerd en aan het eHealth-platform meegezonden.
    U kunt de volgende stap van de STIX-requestor ("Volledig de aanvraag voor het eHealth-certificaat en STIX") uitvoeren om uw
    certificaat te verwerven vanaf 13/06/2017 08:30:51.
    Na deze uitvoering is het certificaat geldig.

    Met vriendelijke groeten,
    eHealth platform - Toegangbeheer
  
```

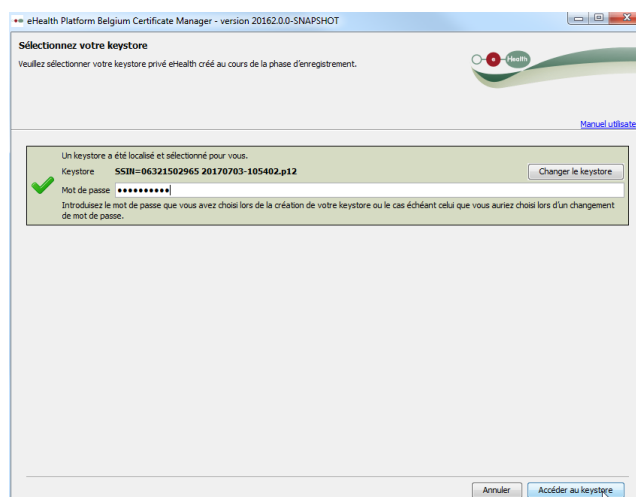

2.3 Finalisation de la demande et enregistrement du certificat

Après avoir réceptionné le deuxième e-mail confirmant la délivrance du certificat, choisissez « Complétez une demande de certificat ».



2.3.1 Sélectionner le fichier keystore

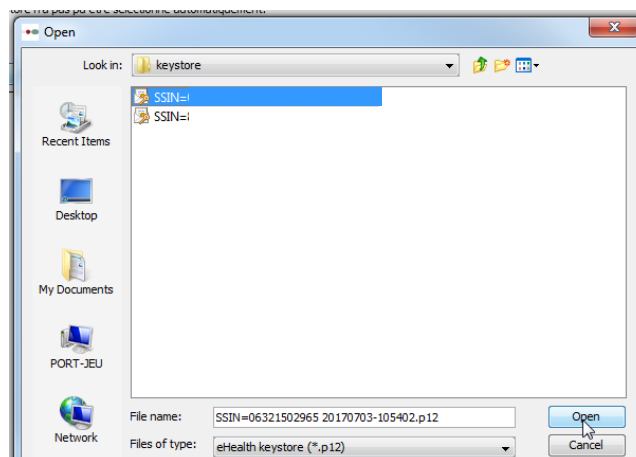
Veillez introduire le mot de passe du fichier keystore. Si le mot de passe est correct, vous pouvez accéder au fichier keystore. Cliquez sur « Accéder au keystore ».



i

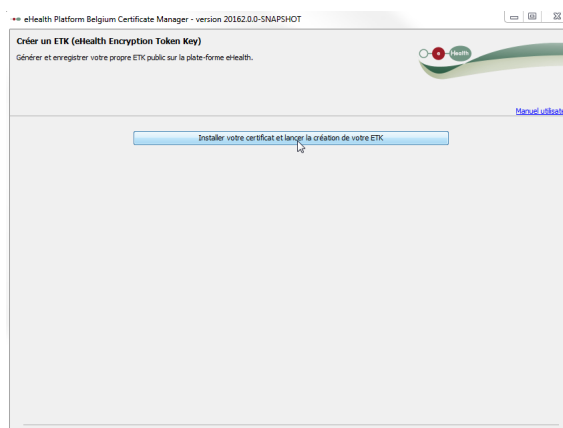
Par défaut, le fichier keystore le plus récent est automatiquement sélectionné.

Pour sélectionner un autre fichier keystore, cliquez sur « Changer le keystore » et sélectionnez le keystore souhaité.



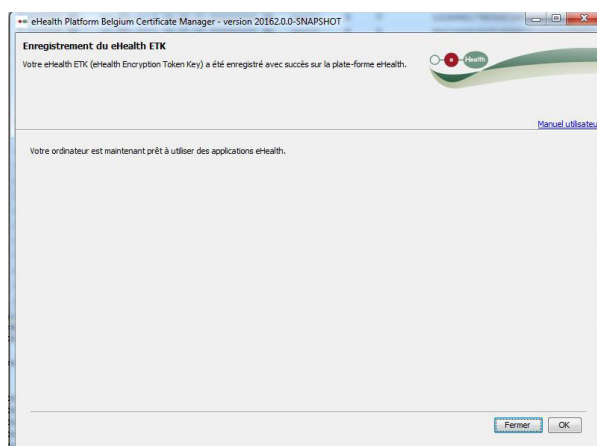
2.3.2 Finalisation de l'enregistrement et création de la clé d'encryptage

Cliquez d'abord sur le bouton « Installer votre certificat et lancer la création de votre ETK⁵ ». Celui-ci se situe au-dessus de la barre de progression « Création de votre eHealth ETK ».



⁵eHealth Encryption Token Key.

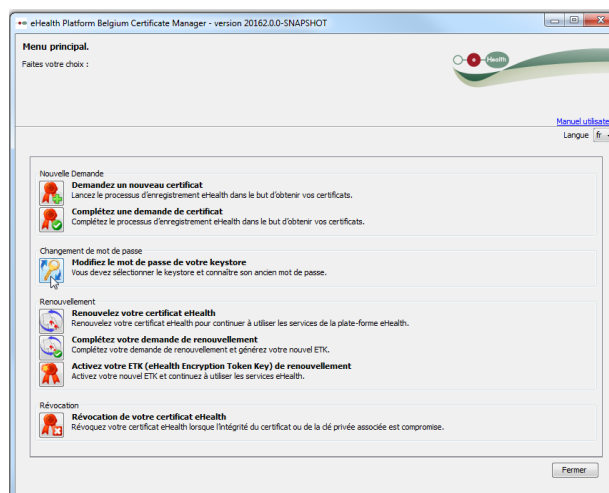
L'écran suivant indique que votre clé d'encryptage a été enregistrée avec succès.



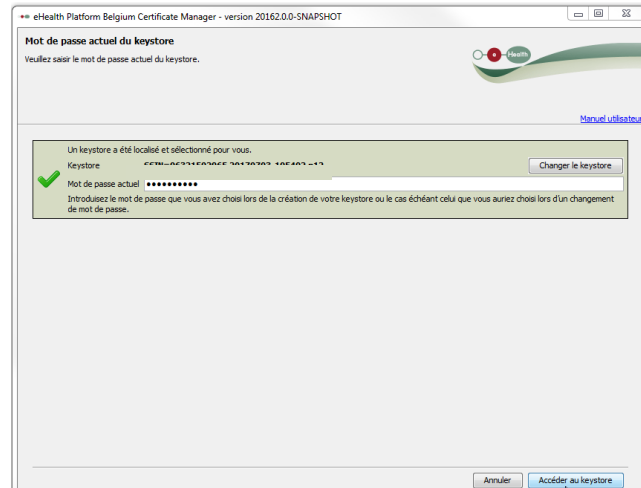
La procédure de demande de certificat est terminée.

3. Modifiez le mot de passe de votre keystore

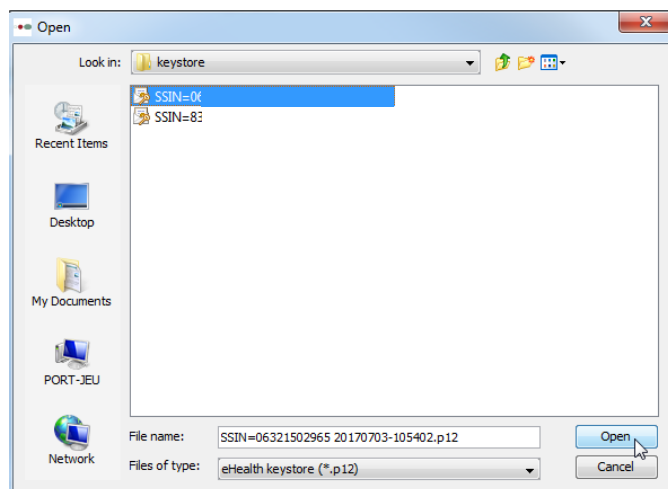
Si vous souhaitez, modifier votre mot de passe, cliquez sur « Modifiez le mot de passe de votre keystore » dans le menu principal, .



Sélectionnez le keystore dont vous souhaitez changer le mot de passe. Et introduisez le mot de passe choisi lors de la création de votre keystore et cliquez sur « Accéder au keystore ».



Pour sélectionner un autre fichier keystore, cliquez sur « Changer le keystore » et sélectionnez le keystore souhaité.



Ensuite, introduisez le nouveau mot de passe souhaité et confirmez-le.

eHealth Platform Belgium Certificate Manager - version 20162.0.0-SNAPSHOT

Nouveau mot de passe du keystore

Vous devez choisir un nouveau mot de passe pour protéger votre keystore personnel. Ce mot de passe remplacera l'ancien et doit comporter au minimum 8 caractères, dont au moins un chiffre ou un symbole.

[Manuel utilisateur](#)

Consultez ici la politique des mots de passe eHealth

Nous vous conseillons de choisir des mots de passe différents pour tous vos certificats. Conservez ce mot de passe dans un endroit sécurisé et ne le divulguez en aucun cas à des tiers.

Introduisez le mot de passe du keystore : *

Vérification de la longueur du mot de passe ✓

Vérification des caractères acceptés ✓

Vérification de l'utilisation des chiffres ou des symboles ✓

Confirmez le nouveau mot de passe du keystore : *

Vérification de la confirmation du mot de passe ✓

* champ obligatoire

Annuler < Précédent Suivant >

L'écran suivant indique que votre nouveau mot de passe a été enregistré avec succès.

eHealth Platform Belgium Certificate Manager - version 20162.0.0-SNAPSHOT

Changement du mot de passe du keystore

[Manuel utilisateur](#)

Le mot de passe de votre keystore a été changé avec succès.

i

La fonctionnalité de « Renouvellement » n'est pas disponible pour les étrangers. Dans ce cas, vous devrez faire une nouvelle demande de certificat.

4. Renouvellement d'un certificat

4.1 Renouvelez votre certificat eHealth

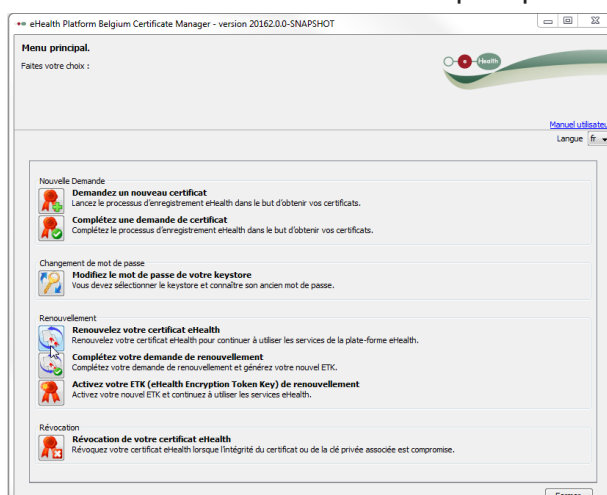
Le renouvellement d'un certificat signifie qu'une nouvelle paire de clés et un nouveau certificat de cryptage vont être générés pour le certificat existant. Durant la période de renouvellement, il y aura donc 2 certificats valides mais un seul actif. Le titulaire du certificat devra ensuite activer le nouveau certificat.

Actuellement, la période de validité d'un certificat est de 36 mois (production) et 12 mois (test) à partir de la date de création. Le renouvellement est permis 3 mois avant la date d'échéance c'est-à-dire à partir du 36^e mois. Avant cette date, le renouvellement n'est pas autorisé.

Des rappels automatiques seront envoyés par e-mail vers les adresses indiquées lors de l'étape 2.1.6. « Enregistrement des données de contact » un mois avant la date d'échéance.

Attention, l'introduction d'une demande de renouvellement n'est plus possible une fois la date d'expiration dépassée. Dans ce cas, une nouvelle demande devra être introduite.

Afin de garantir la continuité de cet outil, il est nécessaire de renouveler votre certificat. Vous devez faire la demande d'un nouveau certificat via la fonctionnalité « Renouvellement » (il ne s'agit donc pas d'une prolongation). Pour cela, cliquez sur « Renouvelez votre certificat eHealth » dans le menu principal.

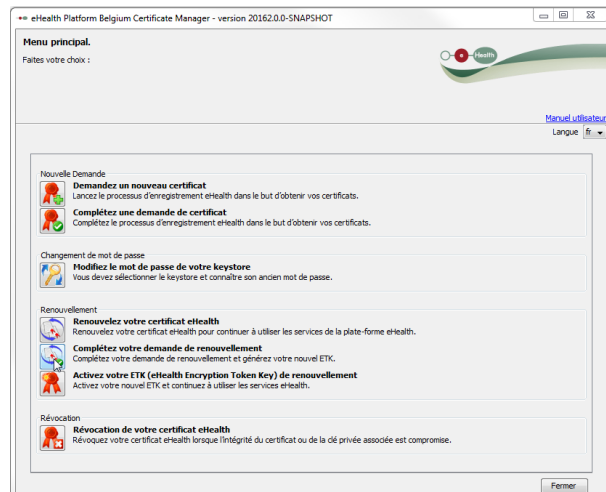


La procédure est la même que l'introduction d'une demande de certificat, veuillez donc suivre les mêmes étapes à partir du point 2.1.2.

Après avoir suivi ces étapes, vous devez encore « Compléter la demande » (4.2.) et ensuite « Activer votre ETK » (4.3.). Ces étapes sont à réaliser une fois que vous êtes prêt à utiliser votre nouveau certificat (par exemple, au moment de l'expiration de l'ancien certificat).

4.2 Complétez votre demande de renouvellement

Vous avez la possibilité de reprendre le remplissage de votre demande de renouvellement. Cliquez sur « Complétez votre demande de renouvellement » dans le menu principal.



La procédure est la même que celle pour compléter une demande de certificat, veuillez donc suivre les mêmes étapes à partir du point 2.3.

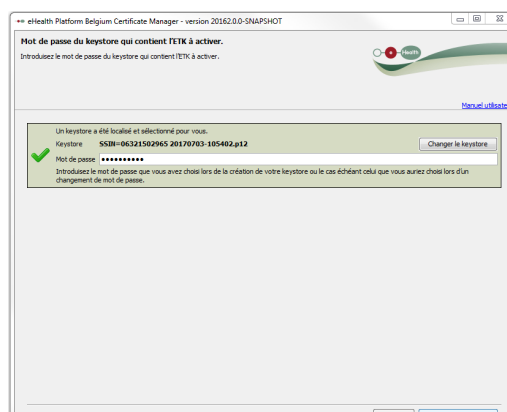
4.3 Activez votre ETK de renouvellement

Une fois que votre nouveau certificat a été enregistré avec succès, l'utilisateur doit désactiver l'ancien certificat et activer le nouveau.

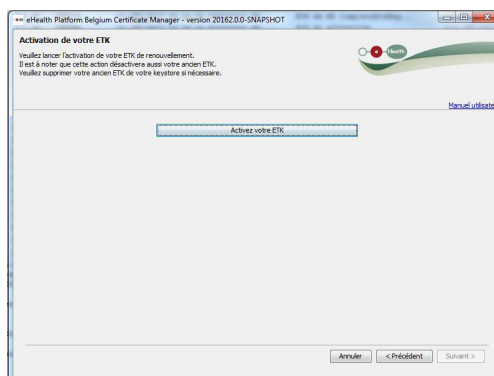
Pour cela, cliquez sur « Activez votre ETK de renouvellement ».



Sélectionner le keystore qui contient la nouvelle clé d'encryption à activer en cliquant sur « **Changer le keystore** ».
Introduisez le mot de passe.
Si le mot de passe est correct, vous pouvez accéder au keystore.



Cliquez sur « **Accéder au keystore** ».
Cliquez d'abord sur « **Activer votre ETK** ».



L'écran indique ensuite que votre clé d'encryptage a été renouvelée avec succès.
Via cette opération, votre ancien ETK/certificat est également automatiquement désactivé.

5. Sécurité

Votre keystore ou mot de passe sont strictement personnels et ne sont autorisés à aucun transfert.

Chaque utilisateur est soumis à leur confidentialité. Chaque utilisateur est également responsable de l'usage de ses données incluant l'usage par un tiers, jusqu'à leur désactivation.

Nous vous invitons, dès lors, à prendre connaissance des règles de sécurité (disponibles sur la page « Support » du portail eHealth).

Les informations relatives à la « Révocation d'un certificat » sont également disponibles sur la page « Support » du portail eHealth.

6. Aide

Le centre de contact eHealth est joignable de plusieurs manières :

- Téléphone :
02 / 788 51 55 (disponible les jours ouvrables de 7h00 à 20h00)
- E-mail :
 - support@ehealth.fgov.be
- Formulaire web :
 - <https://www.ehealth.fgov.be/ehealthplatform/fr/contact>

Afin de faciliter l'échange téléphonique, veuillez avoir à portée de main :

- Votre numéro INAMI;
- Votre carte d'identité;
- Votre numéro NISS;
- Une copie de votre diplôme;
- Éventuellement le numéro de référence présent dans les e-mails de la plate-forme eHealth.

7. Annexe

7.1 Comprendre le « Distinguished Name » (DN) de votre certificat

Le certificat eHealth contient, parmi d'autres informations comme votre clé publique, 7 valeurs qui identifient le propriétaire comme « Distinguished Name ». Le DN est composé de « Relative Distinguished Names ». Ces RDN doivent être pris en compte. Il s'agit de champs devant être remplis.

Les trois premiers champs (Nr 1-3) doivent avoir une valeur fixe prédéfinie. Les autres champs seront remplis en utilisant l'information que vous donnez à la « requestor application ».

Nr	FieldName	Contents (if default value required) or Description
1	countryName	Fixed value: « BE »
2	organizationName	Fixed value: « Federal Government »
3	1. organizationalUnitName	Fixed value: « eHealth-platform Belgium »
4	2. organizationalUnitName	The official name of your organization e.g. « HOSPITAL ABC »
5	3. organizationalUnitName	Identification type and Number (see further in this document for details) e.g. : « NIHII-HOSPITAL =12345678 »
6	4. organizationalUnitName	ApplicationID, an optional field reserved for organizations e.g. : « URGENCES »
7	commonName	The name for the certificate. This is a concatenation of fore mentioned fields 5 and 6. Separated by a coma and a space, if field 6 is applicable. e.g.: « NIHII-HOSPITAL=12345678, URGENCES ».

7.1.1 Nom du pays

La valeur pour le Nom du pays est composée d'une chaîne de 2 caractères correspondant à l'ISO 3166-1-alpha-2 du code du pays. Dans ce cas-ci, la valeur est « BE ».

Ce champ est mis par défaut sur « BE ».

7.1.2 Nom de l'organisation

Le Nom de l'organisation doit être « Federal Government ».

Ce champ est mis par défaut sur « Federal Government ».

7.1.3 Nom d'unité organisationnelle

Il y a 4 différents champs avec comme RDN « organizationalUnitName ». Le premier Nom d'unité organisationnelle est une valeur fixe et est définie comme : « eHealth-platform Belgium ».

Ce champ est mis par défaut sur « eHealth-platform Belgium ».

7.1.4 Nom d'unité organisationnelle

Si la demande de certificat concerne une personne physique, la valeur du prénom est accolée au nom de famille en lettres capitales. Ex.: si le prénom est « Jan » et le nom de famille « Peters », la valeur du champ sera « JANPETERS ».

Si la demande de certificat concerne une organisation (numéro BCE), c'est une valeur qui nécessite d'être la réplique exacte du nom officiel de l'organisation comme il est défini dans la DB Public Search du SPF Economie. Il est nécessaire d'introduire les lettres en lettres capitales, les caractères diacritiques ne sont pas autorisés.

7.1.5 Nom d'unité organisationnelle

Ce champ est nécessaire pour identifier le demandeur du certificat par le biais d'un numéro d'identification officiel dans un format spécifique. Ce format est : TYPE identification=Identification VALUE.

Tous les caractères de ce champ doivent être en lettres capitales. Les espaces ou caractères spéciaux ne sont pas autorisés. Les caractères autorisés sont [A-Z], [0-9], [-], [=].

Vous pouvez chercher dans le tableau ci-dessous quel cas concerne votre demande de certificat. Les noms d'unités organisationnelles suivants sont possibles, par type et rôle spécifique.

Tableau 1 : Types d'identifications possibles pour les Noms d'unités organisationnelles

Certificate holder	Role	organizationalUnitName	Identification TYPE	example	
Physical Person	Care provider	Physical Person (care provider)	Social Security Number. 11 digits. (required for physical persons)	SSIN	SSIN=12345678901
		Physical Person, representing an enterprise or department	Social Security Number. 11 digits. (required for physical persons)	SSIN	SSIN=12345678901
	Test user	Software-Tester software company active in Belgian Healthcare sector <i>Strictly limited use on eHealth acceptance environment</i> Testcertificaat	Social Security Number. 11 digits. (required for physical persons)	SSIN	SSIN=12345678901
Moral Person	Care Institution	Hospital	INAMI/RIZIV number for hospitals. 8 digits.	NIHII-HOSPITAL	NIHII-HOSPITAL=71099812
		Pharmacy	INAMI/RIZIV number used for pharmacies. 8 digits.	NIHII-PHARMACY	NIHII-PHARMACY=71099812
		Labo	INAMI/RIZIV number for laboratoria. 8 digits.	NIHII-LABO	NIHII-LABO=71099812
		Healthcare actor without registration obligation (not having RIZIV/INAMI or KBO/CBE statute) e.g. hubs, grouppractice, ...	EHealth Platform Number (EHP). 10 digits	EHP	EHP=1234567894
		Enterprise or Entity (care institute) without NIHII number e.g. Stichting Kankerregister, RIZIV/INAMI, FOD,SPF	Request form towards eHealth platform	CBE	CBE=1234567894
	Other	Service provider e.g. Nursing Group	INAMI/RIZIV number for hospitals. 8 digits.	NIHII-Group	NIHII-Group=71099812
		Office de Tarification Tarificatiedienst	INAMI/RIZIV number for hospitals. 8 digits.	NIHII-ODT-PHARMACY	NIHII-ODT-PHARMACY=71099812
Rust- en verzorgingstehuis/Maison de repos		INAMI/RIZIV number for hospitals. 8 digits.	NIHII-RETIREMENT	NIHII-RETIREMENT=75099812	

7.1.6 Nom d'unité organisationnelle

Dans ce champ, référencié comme « ID Application », vous pouvez entrer une sous-entité spécifique, département, nom d'application ou toute autre information distinguant les différents certificats de votre organisation. C'est le cas si vous avez plusieurs départements étant tous des points d'aboutissement confidentiellement séparés pour les communications sécurisées.

Ex. : le département « NEONAT » a une boîte mail séparée du département « CARDIOLOGIE ». Vous pourriez également avoir un département « RADIOAPP » qui reçoit des messages structurés et qui requiert également un déchiffrement pour les communications sécurisées.

Le champ « 4. organizationUnitName » est uniquement autorisé si le certificat concerne une organisation. Si la demande de certificat concerne une personne physique – c'est-à-dire lorsque vous utilisez le type « NIHII » ou « SSIN » dans le champ « 3. organizationUnitName » – la valeur du RDN « 4. organizationUnitName » doit être nulle.

L'information « sous-entité/département/nom d'application » sera intégrée dans le certificat et sera disponible comme critère de recherche « ID Application » pour la communauté eHealth.

7.1.7 Nom commun

Le Nom commun doit être minutieusement composé parce qu'il est composé des champs précédents dans un ordre bien défini, avec un séparateur spécifique. Il est composé de :

- La valeur du type d'identification et numéro du champ « 3. organizationUnitName »;
- L'ID Application entré précédemment (si d'application) dans le champ « 4. organizationUnitName ».

Ex. : « NIHII-HOSPITAL=12345678, URGENCES »

Dans notre exemple, le Nom commun serait limité à « NIHII-HOSPITAL=12345678 » en l'absence d'un « ID Application ».

7.1.8 Exemple

Voici un exemple fictif des 7 RDN définis par eHealth pour un certificat d'authentification eHealth. Il s'agit ici d'une organisation pour laquelle un « ID Application » est défini (« URGENCES »).

eHealth certificate	
countryName	BE
organizationName	Federal Government
1. organizationalUnitName	eHealth-platform Belgium
2. organizationalUnitName	UNIVERSITAIRE ZIEKENHUIZEN ABC
3. organizationalUnitName	NIHII-HOSPITAL=12345678
4. organizationalUnitName	URGENCES
commonName	NIHII-HOSPITAL=12345678, URGENCES

7.2 Autorité de certification

Les autorités de certification pour les certificats d'authentification eHealth sont :

- Anciens certificats : Certipost N.V., Centre de la Monnaie, 1000 Bruxelles, Belgique;
- Nouveaux certificats de production (à partir du 17/05/2016) : QuoVadis Trustlink BVBA Schaliënhoevedreef 20T 2800 Mechelen, Belgique;
- Nouveaux certificats de test (à partir du 05/06/2016) : QuoVadis Trustlink BVBA Schaliënhoevedreef 20T 2800 Mechelen, Belgique.