Manuel d'utilisation

Procédure de création de certificats de test eHealth

VERSION DECEMBRE 2013

Contenu

1. Introduction

1.1 But du service

Ce manuel d'utilisateur décrit la procédure pour obtenir un certificat de test 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://wwwacc.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 » ;
- Aux représentants autorisés pour le compte d'institutions enregistrées auprès du secteur de la santé belge.

1.3 Exigences techniques

Afin d'introduire la demande, 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/).

1.4 Exigences administratives

La demande de certificat de test doit être associée à une requête formelle de certificat de test. Les sociétés de logiciels qui développent des logiciels pour les prestataires de soins et/ou hôpitaux doivent remplir un formulaire de procuration disponible sur le portail eHealth : https://www.ehealth.fgov.be/sites/default/files/en-savoir-plus/fiche/formulaire_de_procuration_pour_lobtention_dun_certificat_dacceptance_ehealth.pdf

La période de validité des certificats de test est de maximum 15 mois.

1.5 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 test. Pour la création d'un certificat de production, veuillez vous référer au manuel : https://www.ehealth.fgov.be/sites/activeprd.ehealth.fgov.be/files/certificats-ehealth/procedure/manuel_utilisateur.pdf.

[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

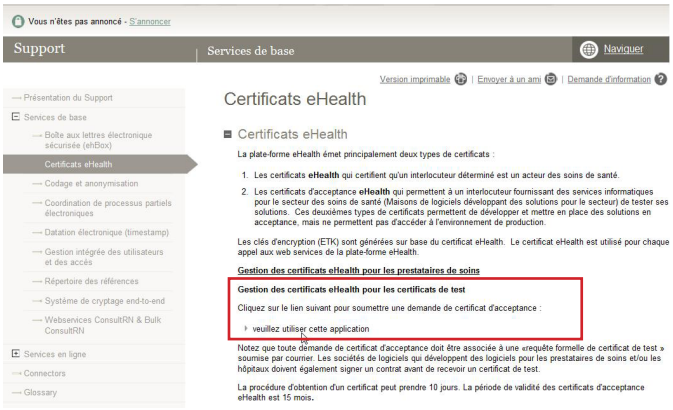
La procédure de demande d'un certificat eHealth comprend trois phases :

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.

Cliquez sur «Support», ensuite «Services de base», «Certificats eHealth» et enfin sur «Veuillez utiliser cette application».



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

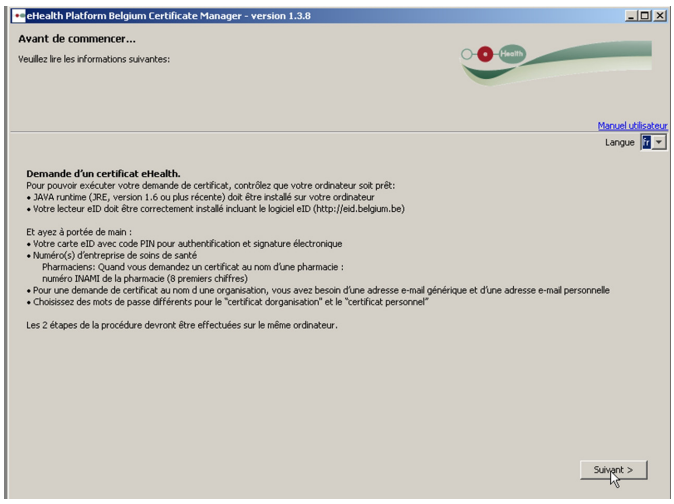
Après avoir cliqué sur le lien du portail, l'application Java est lancée. Vous devez alors indiquer que vous faites confiance au contenu de l'application. Cochez "Always trust content from this publisher" et cliquez sur "Run".

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 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).

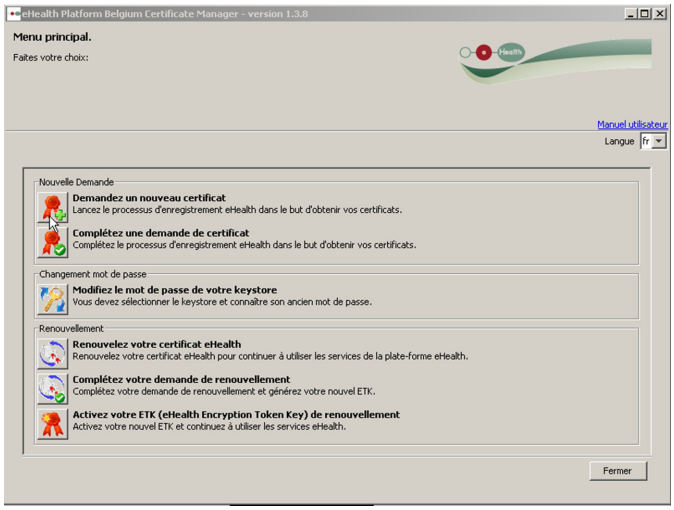


Cliquez sur « Suivant ».

2.1.1 Menu principal

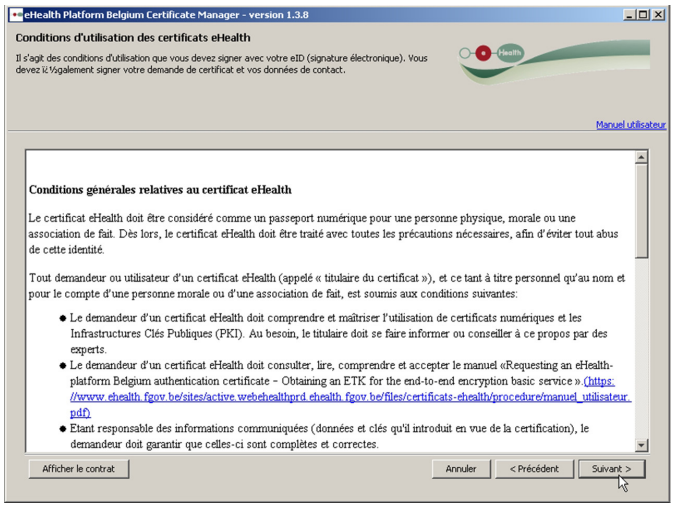
Le menu principal vous permet de sélectionner l'action à entreprendre.

Pour lancer votre procédure d'enregistrement d'un nouveau certificat, cliquez sur le symbole à côté de "Demandez un nouveau certificat".



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».

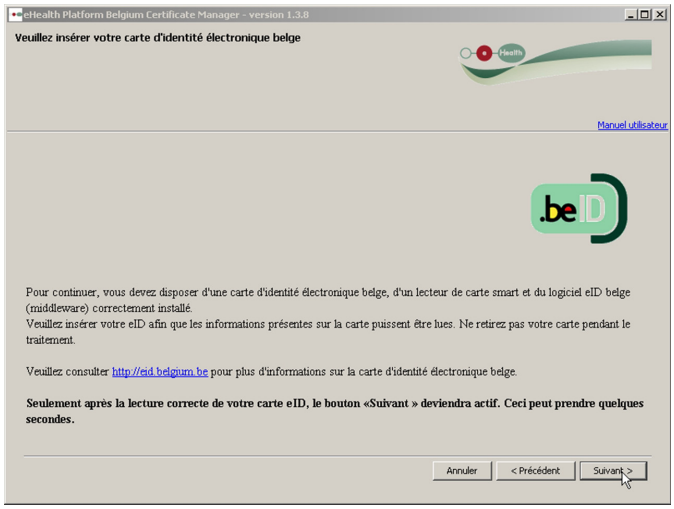


> Vous pouvez afficher le contrat en version PDF en cliquant sur le bouton «Afficher le contrat».

2.1.3 Insérez votre carte eID

Soyez certain que tous les hardwares 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 eID[4].

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

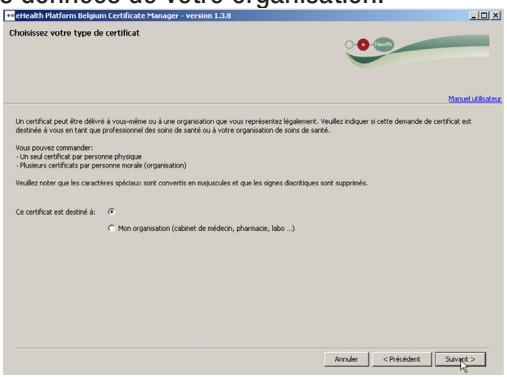


[4] eHealth n'apportera du soutien eID que si votre hardware et logiciel eID sont correctement installés, configurés et fonctionnels.

2.1.4 Choisissez votre type de certificat

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

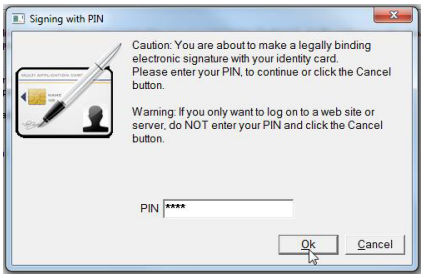
Si votre choix se porte sur l'organisation, vous recevrez un deuxième écran vous invitant à spécifier les données de votre organisation.



> **i**
>
> 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.

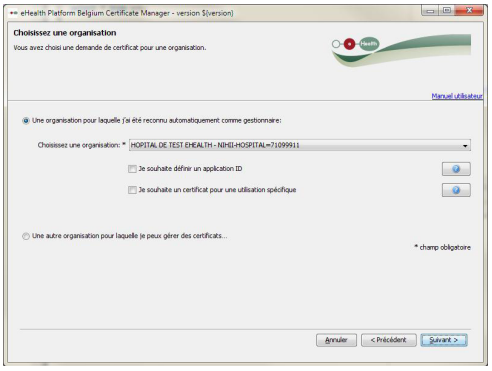
2.1.5 Authentification

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



2.1.6 Ecran des données de votre organisation

Si vous choisissez un certificat personnel, l'écran des données de l'organisation n'apparaîtra pas. Dans ce cas, vous êtes directement dirigé vers l'étape 2.1.8.



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

Sont affichées sur cet écran les organisations pour lesquelles vous avez automatiquement été reconnu comme gestionnaire. Si l'organisation pour laquelle vous souhaitez demander un certificat ne figure pas dans la liste, choisissez l'option 'Une autre organisation pour laquelle je peux gérer des certificats...'.

Vous souhaitez demander un certificat ne figure pas dans la liste, choisissez l'option 'Une autre organisation pour laquelle je peux gérer des certificats...'.

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.

> **i**
>
> Une description de chaque champ est fournie par l'assistant  .

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

Les champs « Je souhaite définir un application ID » et « Je souhaite un certificat pour une utilisation spécifique » sont facultatifs.

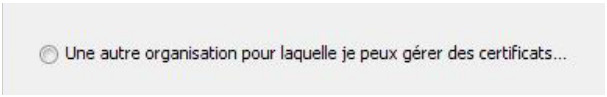
Le champ « Je souhaite définir un application ID » vous permet d'identifier un certificat lorsque vous disposez de plusieurs certificats par organisation.

Pour le champ « Je souhaite un certificat pour une utilisation spécifique », 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 ».

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

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

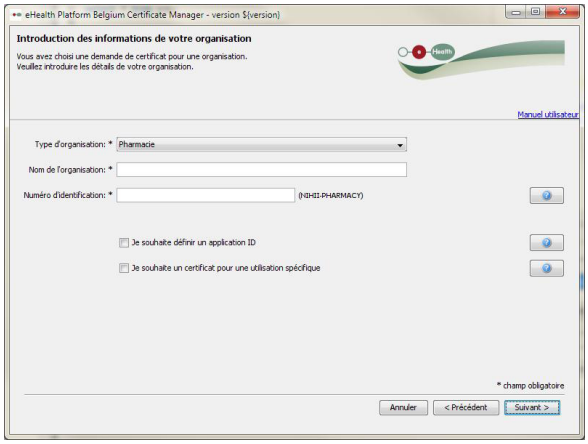


Cliquez sur « Suivant ».

i

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

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



Si votre organisation ne figure pas dans la liste, vous devez introduire manuellement les données de votre organisation.

- Le type d'organisation doit être sélectionné via le menu déroulant. Seuls les types d'organisation figurant dans cette liste peuvent demander des certificats eHealth.
- Le nom de l'organisation doit être renseigné, il s'agit du nom exact tel qu'il a été publié dans le Moniteur belge.
- Le numéro d'identification de l'organisation doit être introduit. Il s'agit généralement du numéro d'entreprise ou du numéro INAMI. En ce qui concerne les pharmacies, il s'agit du numéro de l'officine avec le numéro de contrôle[1] à l'instar d'un numéro INAMI.

Cliquez sur « Suivant ».

[1] 97 moins le reste de la division du numéro d'officine par 97.

2.1.7 Sélection de l'application ID

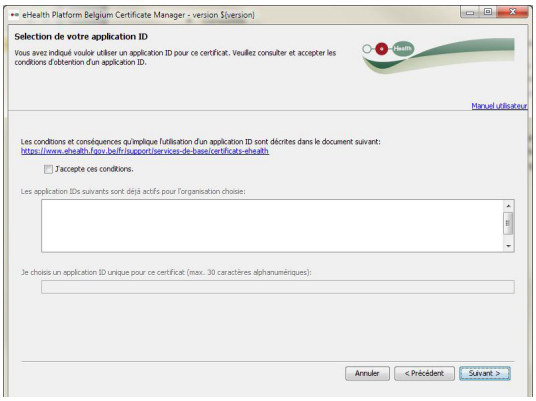
L'application ID permet d'identifier un certificat lorsque vous disposez de plusieurs certificats par organisation.

Que vous ayez été automatiquement reconnu comme gestionnaire de certificat ou ayez vous-même complété les données de l'organisation, vous pouvez, dans les deux cas, définir un application ID ou demander une utilisation spécifique.

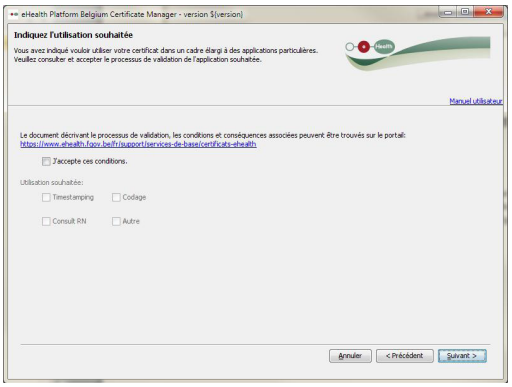
Si vous avez choisi d'indiquer un application ID, vous devez accepter les conditions et les conséquences qui y sont liées.

Si vous acceptez les conditions, une liste des applications ID actives pour l'organisation sélectionnée s'affiche à l'écran.

Vous pouvez également choisir l'application ID unique pour le certificat sélectionné (en fonction du type d'organisation choisi).



Cliquez sur « Suivant ».



La sélection d'une utilisation spécifique permet d'envoyer automatiquement votre certificat aux services compétents pour la configuration de l'accès. Actuellement, trois services sont soutenus de la sorte:

- Timestamping
- Codage
- ConsultRN

Un accord du Comité sectoriel s'avère nécessaire pour l'utilisation de chacun de ces services de base.

> **i**
>
> Les messages électroniques (p.ex. via l'eHealthBox of Recip-e) sont souvent cryptés pour le certificat SANS application ID. C'est pourquoi il est conseillé de toujours utiliser un certificat sans application ID, à moins que l'usage d'un application ID soit vraiment indispensable.

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 .

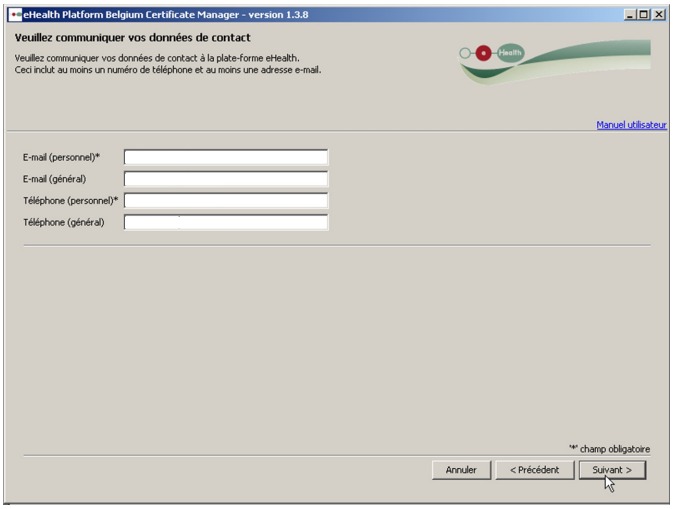
2.1.8 Données de contact

Veuillez introduire les données de contact demandées.

Si vous demandez le certificat pour une organisation que vous pouvez légalement représenter, il vous est demandé de fournir aussi bien un numéro de téléphone et une adresse email personnelle que générale.

Si vous demandez un certificat personnel, il vous sera seulement demandé d'introduire votre adresse email et numéro de téléphone personnel.

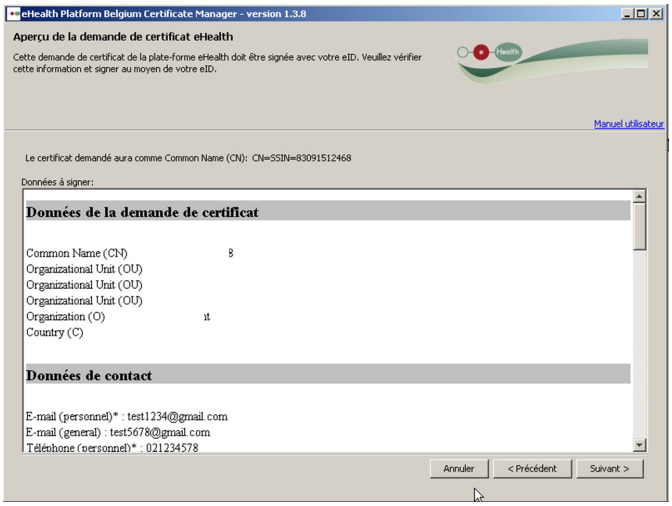
Veuillez noter que l'adresse email et numéro de téléphone personnels ne signifient pas votre adresse email ou numéro de téléphone privés. Vos données de contact personnalisées seront celles utilisées au sein de l'organisation lors de l'envoi des notifications (pour plus d'informations sur les notifications, voir 2.2.1 et 4.1).



2.1.9 Aperçu de la demande

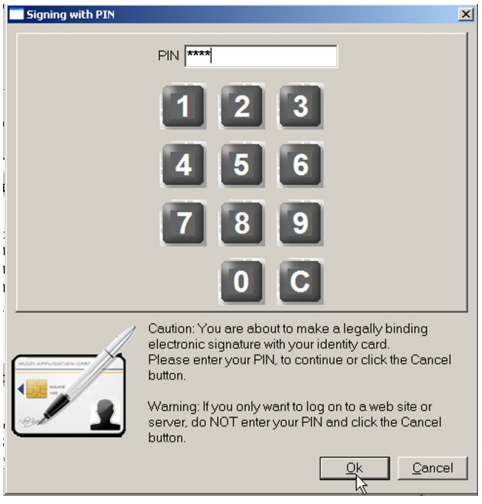
Cet écran affiche un aperçu de toutes les informations contenues dans le fichier de demande de signature du certificat eHealth. Veuillez passer ces informations en revue et éventuellement les corriger en retournant dans un des écrans précédents en cliquant sur « Précédent ».

Ces informations seront signées électroniquement par votre carte eID. En cliquant sur « Suivant », vous arriverez à l'application du logiciel de contrôle de votre carte eID.



2.1.9 Signez en utilisant votre logiciel eID

Il vous sera maintenant demandé d'introduire le code PIN de votre carte eID.

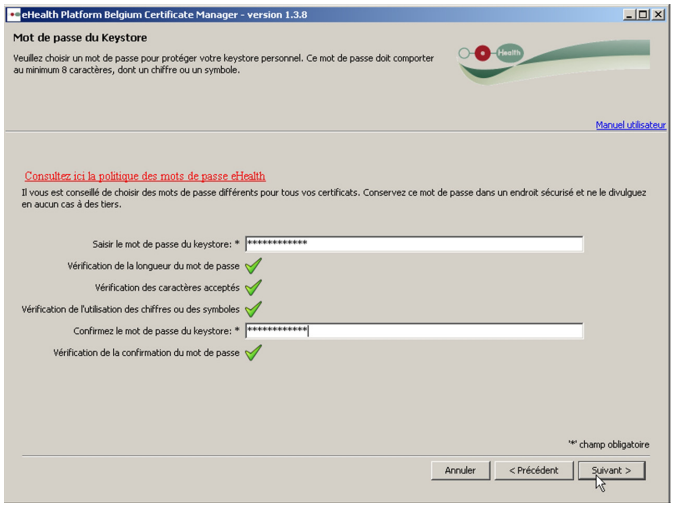


> **i**
>
> Attention : 3 tentatives infructueuses bloqueront votre certificat de carte eID. Si vous avez perdu votre code PIN, veuillez contacter votre autorité communale afin d'obtenir de l'aide.

2.1.10 Fournissez votre mot de passe

Veuillez 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».



Vous pourrez, ensuite, procéder à la finalisation de la première étape de la procédure de la demande.

2.1.11 Aperçu de l'achèvement

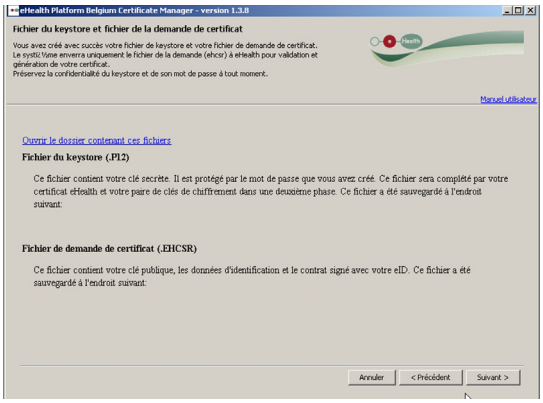
Vos trois fichiers ont été créés avec succès :

- Le premier 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.
- Le deuxième fichier .ehcsr contient vos données d'identification et la clé d'authentification publique, vos données de contact et votre contrat. Ce fichier sera utilisé pour créer votre certificat. Vous pouvez le garder dans vos archives mais il n'aura plus d'utilité une fois que le certificat sera correctement publié. Le fichier .ehcsr a été signé électroniquement avec votre carte d'identité belge.
- Le troisième fichier .reqid contient la référence de votre demande. Ce fichier sera utilisé pour identifier votre demande.

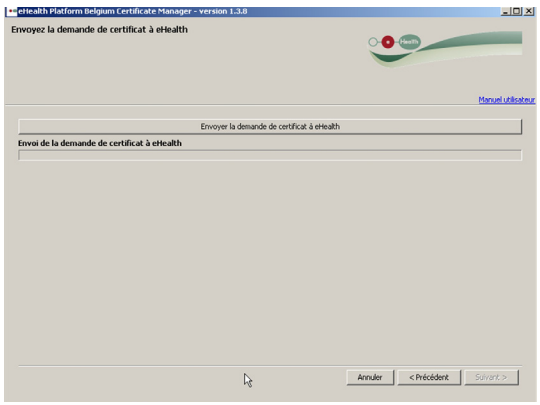
Vos fichiers se trouvent dans un dossier de stockage eHealth personnel. Vous pouvez directement ouvrir ce dossier sur votre ordinateur. Il se trouve dans votre "home" directory sous : \eHealth\keystore\...

> **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.

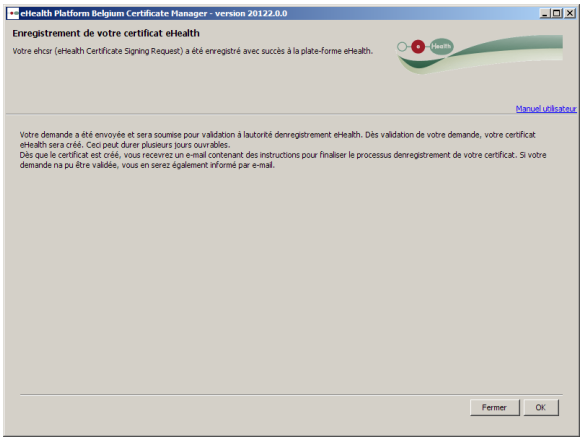
Cliquez sur « Suivant ».



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



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



2.2 Validation de la demande par eHealth

2.2.1 Génération du certificat d'authentification eHealth par eHealth

Votre demande a été délivrée à la plate-forme eHealth. La plate-forme eHealth va, à présent, vérifier votre identité. Cette phase peut prendre quelques jours.

Vous allez recevoir deux notifications distinctes par email :

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 ;
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 email contient la référence de votre demande.

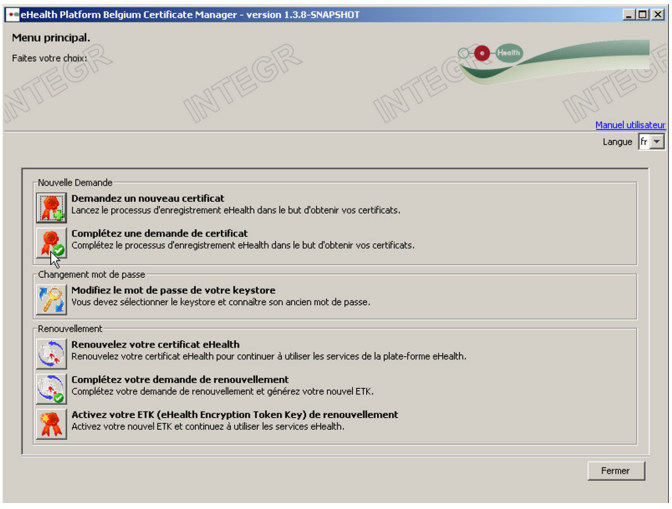
Vous pourrez alors compléter votre demande.

2.3 Finalisation de la demande et enregistrement du certificat

Cliquez sur l'adresse url indiquée dans le deuxième email de notification ou introduisez l'url connue :

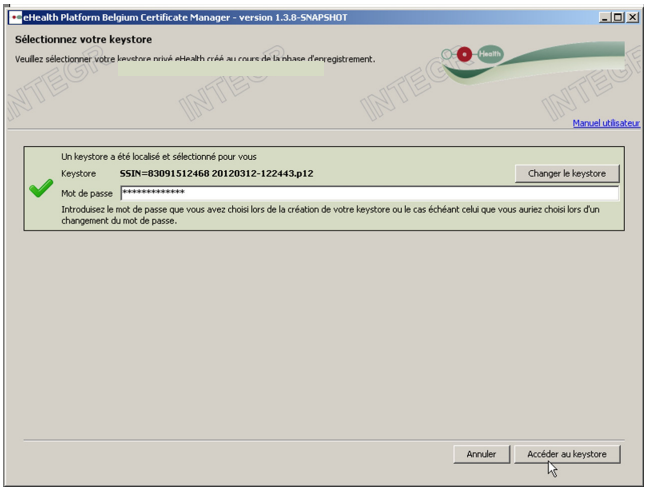
- http://wwwacc.ehealth.fgov.be/JWS/ETEE/etee-requestor_fr.jnlp

Choisissez « Complétez une demande de certificat ».



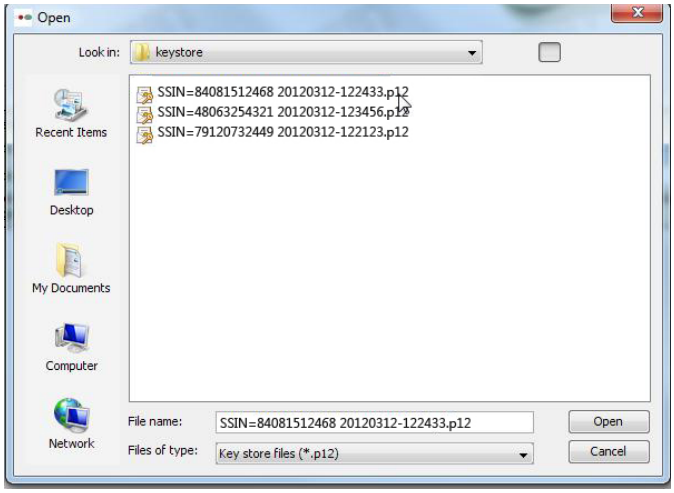
2.3.1 Sélectionner le fichier keystore

Veuillez 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».



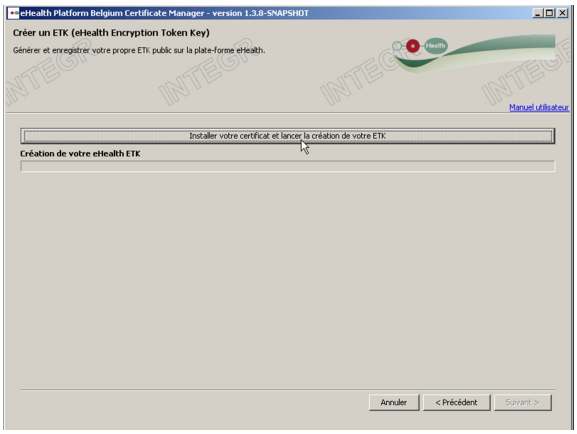
> **i**
>
> Par défaut, le fichier keystore le plus récent est automatiquement sélectionné.

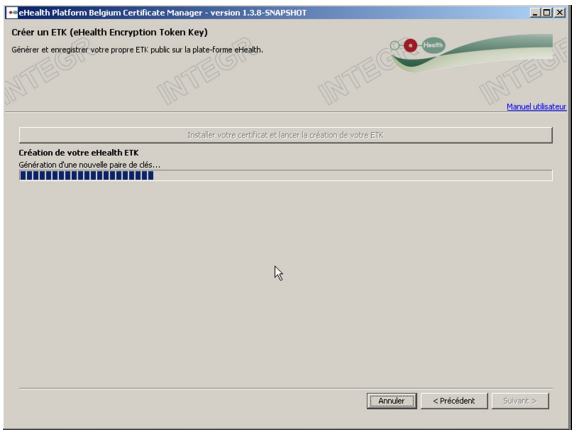
Pour sélectionner un autre fichier keystore, cliquez sur «Changer le keystore» et sélectionnez le keystore souhaité.



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 ETK[5]". Celui-ci se situe au-dessus de la barre de progression « Création de votre eHealth ETK ».



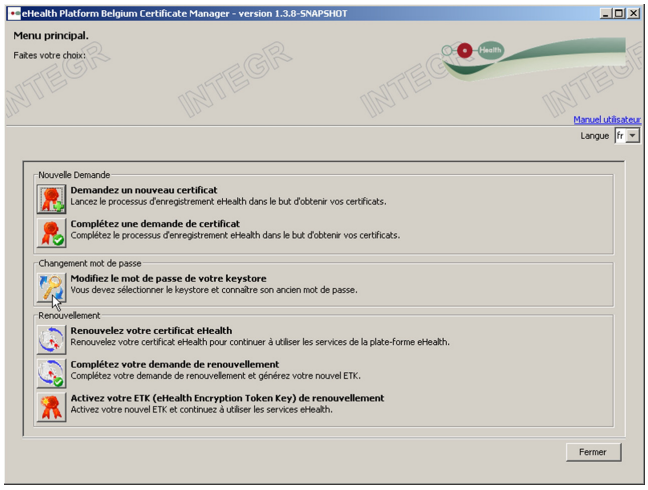


L'écran suivant indique que votre clé d'encryptage a été enregistrée avec succès.

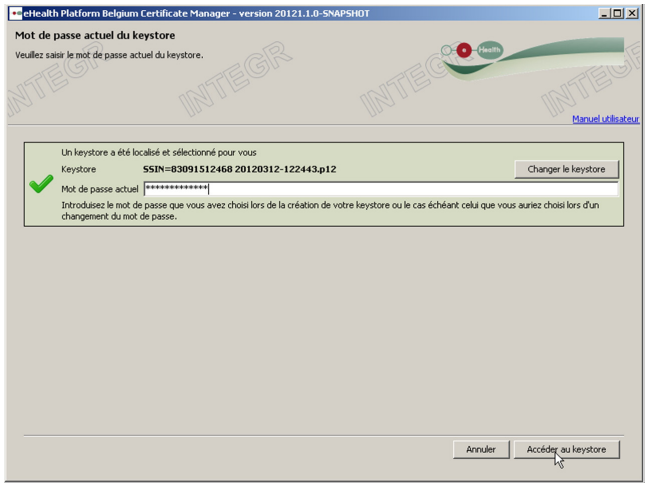
[5]eHealth Encryption Token Key.

3. Modifiez le mot de passe de votre keystore

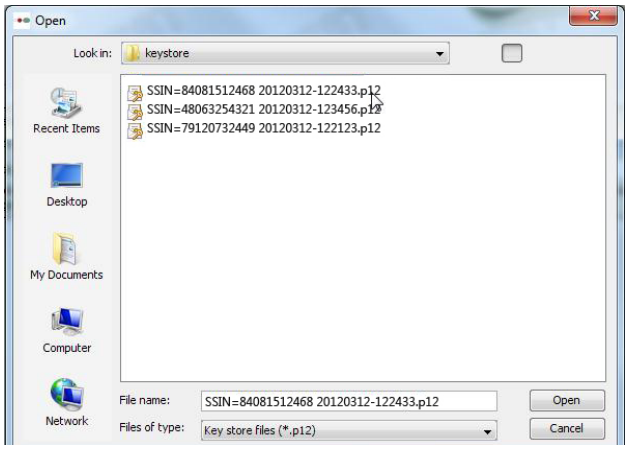
Dans le menu principal, cliquez sur «Modifiez le mot de passe de votre keystore».



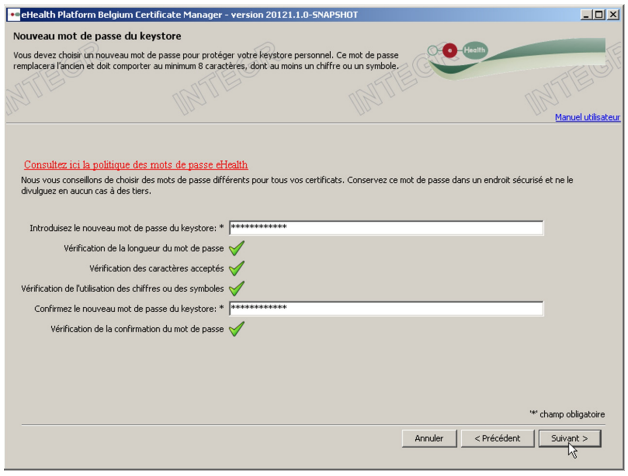
Sélectionnez le keystore dont vous souhaitez changer le mot de passe. Et introduisez le mot de passe choisi lors de la création de votre keystore et cliquez sur « Accéder au keystore ».



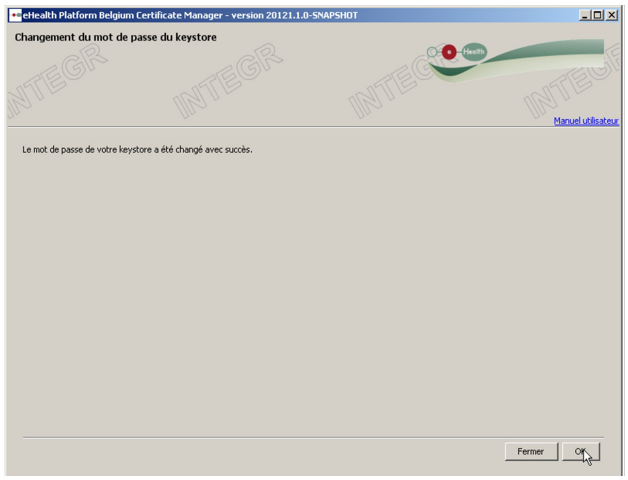
Pour sélectionner un autre fichier keystore, cliquez sur «Changer le keystore» et sélectionnez le keystore souhaité.



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



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



4. Renouvellement d'un certificat

4.1 Renouvelez votre certificat eHealth

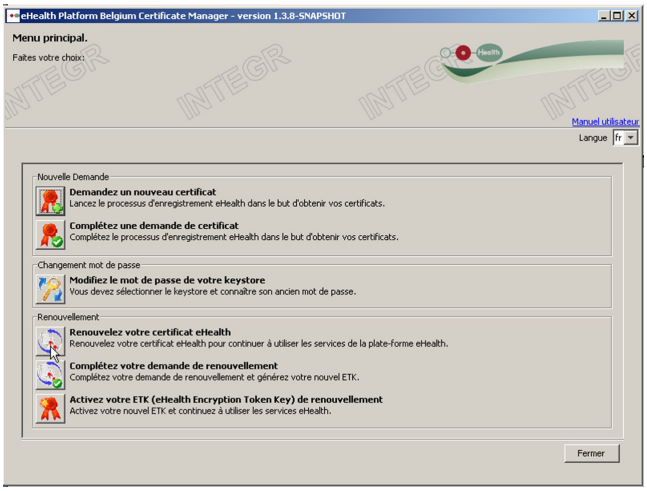
Actuellement, la période de validité d'un certificat de test est de 15 mois à partir de la date de création.

Le renouvellement est permis 2 mois avant la date d'échéance c'est-à-dire à partir du 13e mois. Avant cette date, le renouvellement n'est pas autorisé.

Des rappels automatiques seront envoyés par email 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.



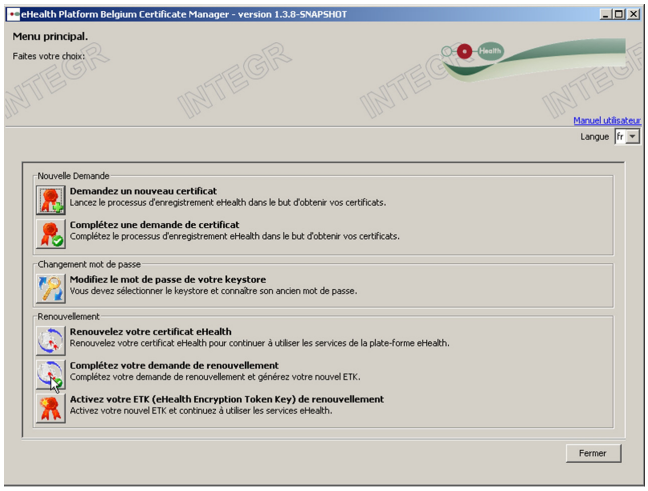
La procédure est la même que l'introduction d'une demande de certificat, veuillez donc suivre les mêmes étapes à partir du point 2.1.2.

Après avoir suivi ces étapes, vous devez encore "Compléter la demande" (4.2.) et ensuite "Activer votre ETK" (4.3.).

> **i**
>
> La fonctionnalité de "Renouvellement" 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.

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.

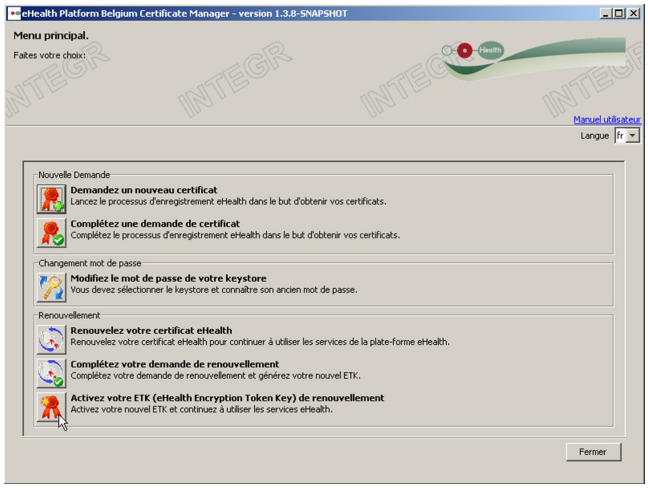


La procédure est la même que celle pour compléter une demande de certificat, veuillez donc suivre les mêmes étapes à partir du point 2.3.

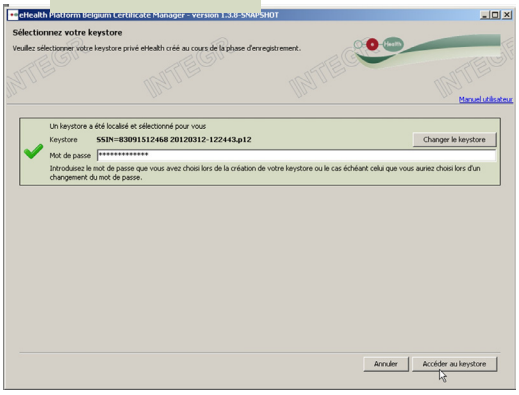
4.3 Activez votre ETK de renouvellement

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

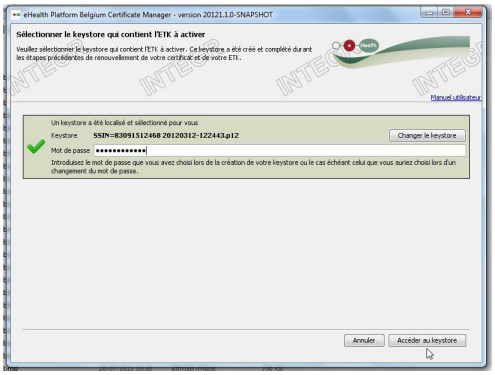
Pour cela, cliquez sur « Activez votre ETK de renouvellement ».



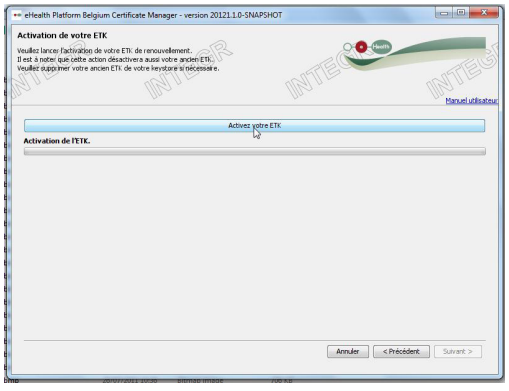
Sélectionner le keystore qui contient la nouvelle clé d'encryption à activer en cliquant sur « Changer le keystore ».
Introduisez le mot de passe.
Si le mot de passe est correct, vous pouvez accéder au keystore.



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.

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/fr/contact

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

- Votre numéro INAMI;
- Votre votre eID;
- Une copie de votre diplôme.

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 « JAN PETERS ».

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 *Strictly limited use on eHealth acceptance environment* 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, groupppractice, ...*	EHealth Platform Number (EHP). 10 digits Request form towards eHealth platform	EHP	EHP=1234567894
		Enterprise or Entity (care institute) without NIHII number *e.g. Stichting Kankerregister, RIZIV/INAMI, FOD,SPF*	Enterprise Number (BCE or KBO). 10 digits	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 déchiffrage pour les communications sécurisées.

Le champ « 4. organizationalUnitName » 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. organizationalUnitName » – la valeur du RDN « 4. organizationalUnitName » 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. organizationalUnitName » ;
- L'ID Application entré précédemment (si d'application) dans le champ « 4. organizationalUnitName ».

Ex. : « NIHII-HOPITAL=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 HOSPTITAL ABC
3. organizationalUnitName	NIHII-HOSPITAL=12345678
4. organizationalUnitName	URGENCES
commonName	NIHII-HOSPITAL=12345678, URGENCES

7.2 Autorité de certification

L'autorité de certification pour les certificats d'authentification eHealth est S.A. Certipost N.V., Centre de la Monnaie, 1000 Bruxelles, Belgique.