

Handleiding

Aanmaakprocedure voor eHealth-testcertificaten



Inhoud

1. Inleiding.....	3
1.1 Doel van de dienst	3
1.2 Operationele vereisten	3
1.3 Technische vereisten	3
1.4 Administratieve vereisten	3
1.5 Type certificaat	4
2. Aanvraagprocedure voor een certificaat	5
2.1 Invoering van de certificaataanvraag	5
2.1.1 Hoofdmenu	6
2.1.2 Gebruiksvoorwaarden voor eHealth-certificaten	7
2.1.3 Voer uw eID-kaart in	7
2.1.4 Kies uw type certificaat.....	8
2.1.5 Authenticatie.....	8
2.1.6 Scherm met gegevens van uw organisatie	8
2.1.7 Selectie van de toepassings-ID	11
2.1.8 Contactgegevens	12
2.1.9 Overzicht van de aanvraag.....	13
2.1.10 Ondertekenen met behulp van uw eID-software.....	13
2.1.11 Een wachtwoord instellen	14
2.1.12 Overzicht van voltooiing	14
2.2 Validering van de aanvraag door eHealth	16
2.2.1 Genereren van het authenticatiecertificaat door eHealth.....	16
2.3 Voltooiing van de aanvraag en registratie van het certificaat	16
2.3.1 Het keystore-bestand selecteren.....	17
2.3.2 Voltooiing van de registratie en aanmaak van de versleutelsleutel	18
3. Wijzig het wachtwoord van uw keystore.....	18
4. Vernieuwing van een certificaat.....	21
4.1 Vernieuw uw eHealth-certificaat.....	21
4.2 Uw aanvraag tot vernieuwing vervolledigen.....	22
4.3 Activeer uw vernieuwde ETK.....	22
5. Beveiliging	24
6. Hulp.....	24
7. Bijlage	25
7.1 De “Distinguished Name” (DN) van uw certificaat begrijpen	25
7.1.1 Naam van het land.....	25
7.1.2 Naam van de organisatie	25
7.1.3 Naam van de organisatie-eenheid.....	25
7.1.4 Naam van de organisatie-eenheid.....	26
7.1.5 Naam van de organisatie-eenheid	26
7.1.6 Naam van de organisatie-eenheid	27
7.1.7 Algemene naam.....	27
7.1.8 Voorbeeld	28
7.2 Certificeringsautoriteit.....	28



1. Inleiding

1.1 Doel van de dienst

Deze gebruikershandleiding beschrijft de procedure om een testcertificaat voor eHealth en een vercijfersleutel te verkrijgen.

Het authenticatiecertificaat van eHealth wordt gebruikt elke keer er een beroep gedaan wordt op de webservices van het eHealth-platform. Het certificaat zorgt ervoor dat men zich kan authenticeren als actor van de gezondheidszorg.

Tijdens het gebruik van de basisdienst voor vercijfering is een vercijfercertificaat nodig om een dubbele vercijfersleutel aan te maken.

U kan de applicatie “Certificate Manager” starten door te klikken op:

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

1.2 Operationele vereisten

Een certificaat wordt toegekend:

- een geldige Belgische identiteitskaart;
- Aan de natuurlijke personen die zich registreren in de authentieke bron “Kadaster van gezondheidsberoepen”;
- Aan de gemachtigde vertegenwoordigers voor rekening van de geregistreerde instellingen bij de Belgische gezondheidssector.

1.3 Technische vereisten

Om een aanvraag in te voeren, moet u beschikken over:

- een eID-lezer;
- de middleware die vereist is om de eID te gebruiken (meer informatie om de laatste versie van de eID-software te downloaden op <http://eid.belgium.be>);
- de Java-versie 1.6 of hoger 32 bits (meer informatie om de laatste versie van Java te downloaden op <http://www.java.com/nl/download/>).

1.4 Administratieve vereisten

De aanvraag van een testcertificaat moet gepaard gaan met een “formeel verzoek tot testcertificaat”. De softwarebedrijven die software ontwikkelen voor zorgverleners en/of ziekenhuizen moeten een procuratieformulier invullen. Dit is beschikbaar op het eHealth-portaal: https://www.ehealth.fgov.be/sites/default/files/ehealth-certificaten/fiche/volmachtsformulier_voor_het_verkrijgen_van_een_acceptatiecertificaat_nl.pdf.

De geldigheidsduur van de testcertificaten is maximaal 15 maanden.



1.5 Type certificaat

Er bestaan twee types certificaat:

- De testcertificaten: gebruikt door IT-deskundigen en zorgverleners om de integratie van de eHealth-basisdiensten te testen;
- De productiecertificaten: gebruikt door zorgverleners om toegang te krijgen tot de basisdiensten van eHealth.

De omgeving kan naargelang de gebruiker veranderen (testomgeving en/of productieomgeving):

	Testcertificaat ¹	Productiecertificaat
Zorgverleners ²	Ja	Ja
IT ³	Ja	Nee

Deze handleiding beschrijft de procedure om testcertificaten aan te maken. Voor de aanmaak van een productiecertificaat, zie de handleiding: <https://www.ehealth.fgov.be/sites/activeprd.ehealth.fgov.be/files/ehealth-certificaten/procedure/gebruiksdocumentatie.pdf>.



¹ Het testcertificaat zorgt ervoor dat zorgverleners fictieve gegevens in een acceptatieomgeving kunnen testen.

² Professionele zorgverleners, actief in de Belgische gezondheidssector.

³ IT-integrators, leveranciers van software voor de applicaties bestemd voor zorgverleners in de Belgische gezondheidssector.

2. Aanvraagprocedure voor een certificaat

De aanvraagprocedure voor een eHealth-certificaat telt drie stappen:

1. De invoering van de aanvraag voor een eHealth-certificaat;
2. De validering van de aanvraag door eHealth;
3. De finalisering van de aanvraag en de registratie van het certificaat.

2.1 Invoering van de certificaataanvraag

U moet de aanvraag indienen met behulp van de applicatie “Certificate Manager” die beschikbaar is op het eHealth-portaal.

Klik op “Support”, vervolgens op “Basisdiensten”, “eHealth-certificaten” en tot slot op “Gelieve deze toepassing te gebruiken”.

Printvriendelijke versie | Verstuur naar een vriend | Informatieaanvraag

eHealth-certificaten

■ eHealth-certificaten

Het eHealth-platform geeft voornamelijk twee soorten certificaten uit:

1. De **eHealth-certificaten** waarbij wordt bevestigd dat een bepaalde partner een actor in de gezondheidszorg is.
2. De **eHealth-acceptatiecertificaten** op basis waarvan een partner die informaticadiensten voor de sector van de gezondheidszorg levert (softwarehuizen die oplossingen voor de sector ontwikkelen) zijn oplossingen kan uitstellen. Op basis van deze tweede soort certificaten kunnen oplossingen worden ontwikkeld en in acceptatie worden genomen, maar het is niet mogelijk om toegang te krijgen tot de productieomgeving.

De encryptiesleutels (ETK) worden op basis van het eHealth-certificaat gegenereerd. Het eHealth-certificaat wordt gebruikt telkens de webservices van het eHealth-platform worden aangeroepen.

Beheer van de eHealth-certificaten voor de zorgverleners

Beheer van de eHealth-certificaten voor de testcertificaten

Klik op de volgende link om een acceptatie-certificaataanvraag in te dienen:

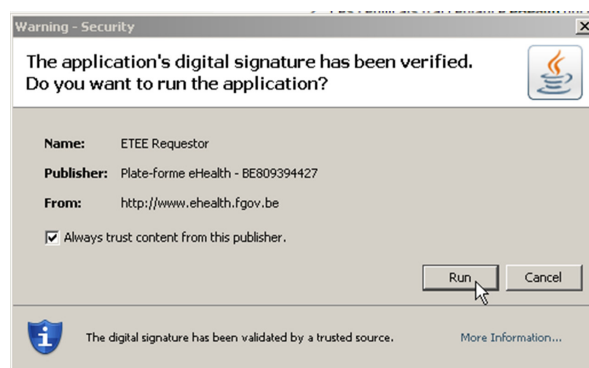
[Gelieve deze toepassingen te gebruiken](#)

Werk op dat een eHealth-acceptatiecertificaat is schijnbaar moet worden ingediend voor een acceptatiecertificaat. Als ook de softwarehuizen die software ontwikkelen voor zorgverleners en/of ziekenhuizen dienen een contract te tekenen voor zij een testcertificaat ontvangen.

De procedure voor het verkrijgen van een certificaat kan tot 10 dagen duren. De eHealth-acceptatiecertificaten zijn 15 maanden geldig.

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

Nadat u op de link van het portaal geklikt hebt, start de Java-applicatie. U moet aanduiden dat u de informatie van de toepassing vertrouwt. Vink “Always trust content from this publisher” aan en klik op “Run”.

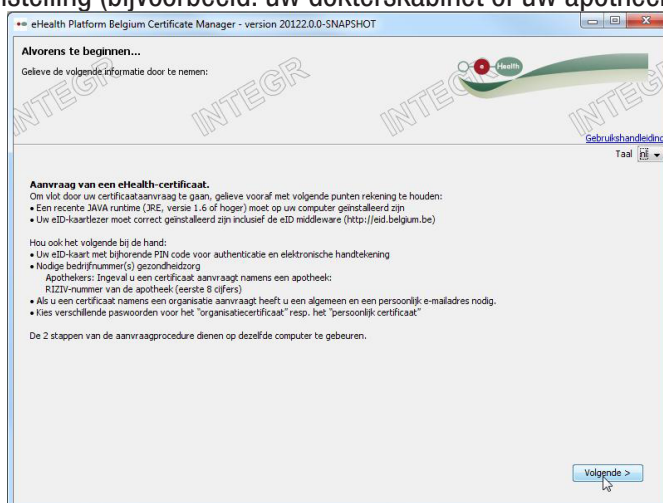


Het volgend scherm herhaalt de verschillende technische vereisten:

- Versie 1.6. van Java of hoger;
- Een eID-lezer die correct geïnstalleerd is.

U moet eveneens de volgende kaarten en cijfers binnen handbereik houden:

- Uw identiteitskaart en de bijhorende PIN-code;
- Enkel voor de organisaties: het RIZIV- of KBO-nummer (i.e. het ondernemingsnummer), of het EHP-nummer (eHealth Partner) dat overeenstemt met uw instelling (bijvoorbeeld: uw dokterskabinet of uw apotheek).

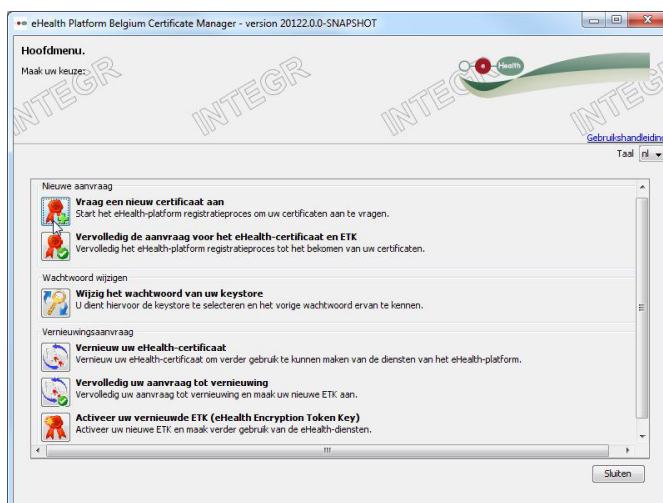


Klik op “Volgende”.

2.1.1 Hoofdmenu


In het hoofdmenu kunt u de uit te voeren actie kiezen.

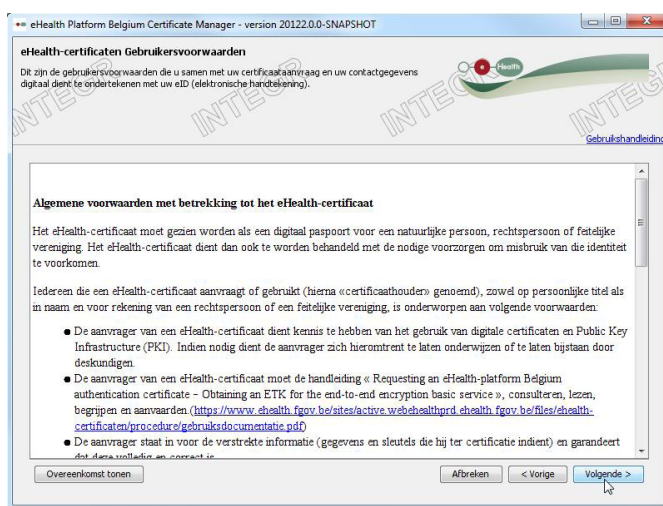
Om de registratieprocedure van een nieuw certificaat te starten, klikt u op het symbool naast “Vraag een nieuw certificaat aan”.



2.1.2 Gebruiksvoorwaarden voor eHealth-certificaten

U wordt gevraagd om de overeenkomst voor eHealth-certificaten te lezen en te aanvaarden. Lees de tekst zeer aandachtig. Klik op “Volgende”.


U kan de overeenkomst in PDF-formaat bekijken door op de knop “Overeenkomst tonen” te klikken.



2.1.3 Voer uw eID-kaart in

Wees er zeker van dat alle hard- en software voor de eID-kaart correct geïnstalleerd zijn. Als u hulp nodig heeft om uw installatie te configureren of te controleren, volg dan de link of klik op het eID-symbool⁴.

De knop “Volgende” verschijnt enkel wanneer uw eID-kaart correct gelezen werd.



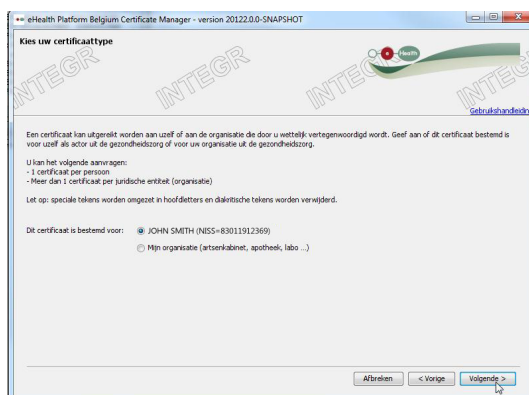
⁴eHealth verleent enkel ondersteuning bij uw eID als uw hard- en software correct geïnstalleerd, geconfigureerd en functioneel zijn.



2.1.4 Kies uw type certificaat

Geef aan of het certificaat voor persoonlijk gebruik is of dient voor een organisatie waar u lid van bent.

Als u kiest voor een organisatie, dan zal u een tweede scherm zien waar u de gegevens van uw organisatie kan invullen.



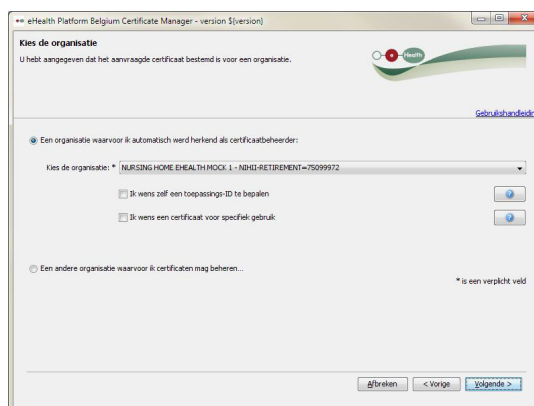
2.1.5 Authenticatie

U moet de PIN-code van uw eID ingeven zodat uw toegangsrechten gecontroleerd kunnen worden.



2.1.6 Scherm met gegevens van uw organisatie

Als u een persoonlijk certificaat kiest, dan verschijnt het scherm met gegevens voor de organisatie niet. In dit geval wordt u direct doorverwezen naar stap 2.1.8.



Hier worden de organisaties weergegeven waarvoor u automatisch herkend werd

i

Opgelet : 3 mislukte pogingen zullen uw eID blokkeren. Als u uw PIN-code verloren hebt, gelieve hulp te vragen aan uw gemeente.

i

De velden met een "*" zijn verplicht.



als verantwoordelijke. Wanneer de organisatie waarvoor u een certificaat wil aanvragen niet in de lijst staat, kiest u voor 'Een andere organisatie waarvoor ik certificaten mag beheren...'

Voorbeeld 1: U selecteert een organisatie waarvoor u erkend bent als lokale beheerder



U moet nu de gevraagde gegevens over de organisatie ingeven.

Kies de organisatie waarvoor u een certificaat wenst aan te vragen. Het systeem zal u al uw gekende organisaties voorstellen.

De velden "Ik wens zelf een toepassings-ID te bepalen" en "Ik wens een certificaat voor specifiek gebruik" zijn optioneel.

Het veld "Ik wens zelf een toepassings-ID te bepalen" laat u toe een certificaat te identificeren wanneer u over meerdere certificaten per organisatie beschikt.

Voor het veld "Ik wens een certificaat voor specifiek gebruik" selecteert u de basisdiensten waarop uw organisatie beroep wenst te doen volgens het gevraagde certificaat. Een akkoord van het sectoraal comité is noodzakelijk voor het gebruik van elk van deze basisdiensten.


Klik op "Volgende".

Voorbeeld 2: U selecteert een andere organisatie waarvoor certificaten mag beheren.



Klik op "Volgende".

i

Een beschrijving van elk veld wordt geleverd door de hulp-functie 

i

In functie van het type organisatie zullen bepaalde velden verschijnen.



i

Het veld “Naam organisatie” kan enkel de volgende karakters bevatten:

- Letters (A-Z),
- Cijfers (0-9),
- Streepje (-),
- Underscore (_),
- Spatie (<space>).

Indien uw organisatie niet werd weergegeven in de lijst, moet u de gegevens van de organisatie zelf invullen.

- Het type organisatie selecteert u uit de lijst. Enkel de organisatietypes uit deze lijst kunnen eHealth certificaten aanvragen.
- De naam van de organisatie moet de exacte naam zijn zoals deze voorkomt in het Staatsblad.
- Het identificatienummer van de organisatie. Dit is meestal het ondernemings- of RIZIV-nummer. Voor apotheken gaat het om het apotheknummer met controlegetal¹ zoals bij een RIZIV-nummer.

Klik op “Volgende”.



¹ 97 min de rest van de deling van het apotheknummer door 97.



Elektronische berichten (bv. via de eHealthBox of Recip-E) zijn vaak versleuteld voor het certificaat ZONDER toepassings-ID. Daarom wordt aangeraden om steeds gebruik te maken van een certificaat zonder toepassings-ID tenzij het gebruik van een toepassings-ID echt noodzakelijk is.

2.1.7 Selectie van de toepassings-ID

De toepassings-ID laat u toe een certificaat te identificeren wanneer u over meerdere certificaten per organisatie beschikt.

Of u nu automatisch werd herkend als certificaatbeheerder of zelf de gegevens van de organisatie hebt ingevuld, in beide gevallen kan u een toepassings-ID bepalen of een specifiek gebruik aanvragen.

Wanneer u gekozen hebt om een toepassings-ID op te geven, moet u akkoord gaan met de voorwaarden en gevolgen die hieraan vast hangen.

Indien u akkoord gaat krijgt u een lijst met reeds bestaande toepassings-ID's te zien voor deze organisatie.

U kan eveneens de unieke toepassings-ID kiezen voor het geselecteerde certificaat (afhankelijk van het gekozen organisatietype).

Klik op "Volgende".

Een specifiek gebruik selecteren zorgt ervoor dat uw certificaat automatisch wordt doorgestuurd naar de bevoegde diensten voor de configuratie van de toegang. Momenteel worden er op deze manier drie diensten ondersteund:

- Timestamping
- Codage
- ConsultRN

Een akkoord van het sectoraal comité is noodzakelijk voor het gebruik van elk van deze basisdiensten.





Enkel de administrator of de volmachtverlener van de organisatie kan de certificaataanvraag indienen. Geen enkele andere aanvraag zal worden behandeld. Het formulier voor de volmacht is beschikbaar op de « Support »-pagina van het eHealth-portaal

2.1.8 Contactgegevens

Als u een certificaat aanvraagt voor een organisatie die u wettelijk kunt vertegenwoordigen, dan wordt u ook een persoonlijk en algemeen telefoonnummer en een persoonlijk en algemeen e-mailadres gevraagd.

Als u een persoonlijk certificaat aanvraagt, dan moet u enkel uw persoonlijk e-mailadres en telefoonnummer invoeren.

Let op: uw persoonlijk e-mailadres en telefoonnummer zijn niet uw privé-telefoonnummer en e-mailadres. Hier gaat het om de gepersonaliseerde contactgegevens binnen de organisatie die zullen gebruikt worden bij het versturen van meldingen (voor meer informatie over de notificaties, zie 2.2.1 en 4.1).

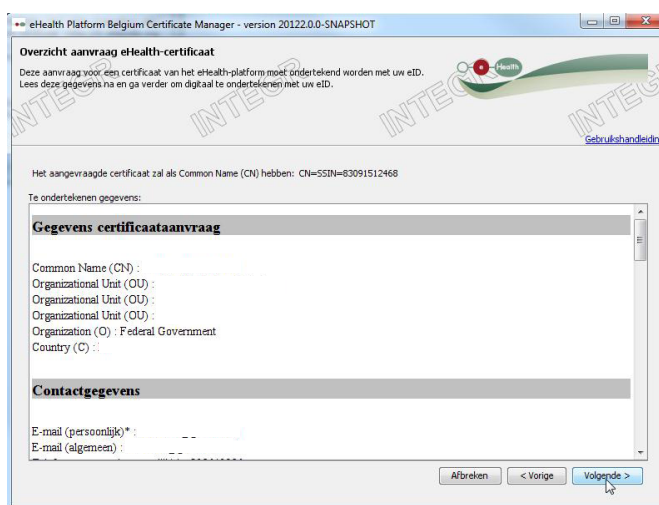
The screenshot shows a web browser window titled "eHealth Platform Belgium Certificate Manager - version 20122.0.0-SNAPSHOT". The main heading is "Vul de contactgegevens in". Below this, there are instructions: "U dient uw contactgegevens aan het eHealth-platform te bezorgen. U voert tenminste een telefoonnummer en een e-mailadres in." There are four input fields: "E-mail (persoonlijk)*", "E-mail (algemeen)", "Telefoonnummer (persoonlijk)*", and "Telefoonnummer (algemeen)". The asterisk indicates a required field. At the bottom right, there is a note: "** is een verplicht veld". Navigation buttons include "Afbreken", "< Vorige", and "Volgende >". A watermark "INTEC" is visible across the page.



2.1.9 Overzicht van de aanvraag

Dit scherm toont een overzicht van alle informatie aangaande de aanvraag tot ondertekening van het eHealth-certificaat. Lees de gegevens na en verbeter ze eventueel door terug te keren naar de vorige schermen via de knop "Vorige".

Deze informatie zal door uw eID-kaart elektronisch getekend worden. Door op "Volgende" te klikken komt u bij de controleapplicatie van uw eID-kaart.



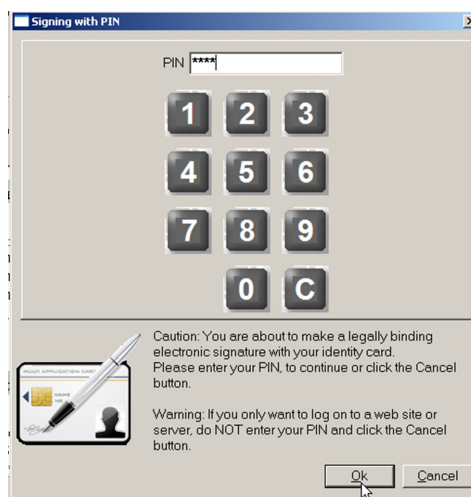
The screenshot shows a window titled "eHealth Platform Belgium Certificate Manager - version 20122.0.0-SNAPSHOT". The main heading is "Overzicht aanvraag eHealth-certificaat". Below this, there is a note: "Deze aanvraag voor een certificaat van het eHealth-platform moet ondertekend worden met uw eID. Lees deze gegevens na en ga verder om digitaal te ondertekenen met uw eID." A link for "Gebruikshandleiding" is visible. The text states: "Het aangevraagde certificaat zal als Common Name (CN) hebben: CN=SSIN=83091512468". Under "Te ondertekenen gegevens:", there are two sections: "Gegevens certificaataanvraag" and "Contactgegevens". The "Gegevens certificaataanvraag" section lists: Common Name (CN):, Organizational Unit (OU):, Organizational Unit (OU):, Organizational Unit (OU):, Organization (O): Federal Government, and Country (C):. The "Contactgegevens" section lists: E-mail (persoonlijk)*: and E-mail (algemeen):. At the bottom, there are buttons for "Afbreken", "< Vorige", and "Volgende >".

2.1.10 Ondertekenen met behulp van uw eID-software

Er zal gevraagd worden uw PIN-code van uw eID-kaart opnieuw in te voeren om de aanvraag te tekenen.

i

Opgelet : 3 mislukte pogingen zullen uw eID blokkeren. Als u uw PIN-code verloren hebt, gelieve hulp te vragen aan uw gemeente.



The screenshot shows a dialog box titled "Signing with PIN". It features a PIN input field with four asterisks. Below the input field is a numeric keypad with buttons for digits 1-9, 0, and a 'C' button. At the bottom, there are "Ok" and "Cancel" buttons. A warning message reads: "Caution: You are about to make a legally binding electronic signature with your identity card. Please enter your PIN, to continue or click the Cancel button." Below the warning, there is a smaller warning: "Warning: If you only want to log on to a web site or server, do NOT enter your PIN and click the Cancel button." An icon of a stethoscope and a person's head is visible in the bottom left corner of the dialog box.





Zorg dat u uw wachtwoord kan onthouden. Als u het wachtwoord kwijt bent, hebt u geen toegang meer tot uw persoonlijke sleutels en zal u zich niet meer kunnen identificeren, noch kan u berichten ontcijferen. U moet dan eHealth contacteren en uw oud certificaat herroepen en een nieuw aanvragen.

2.1.11 Een wachtwoord instellen

Stel een sterk wachtwoord in om uw keystore te beveiligen. De wachtwoordcontroles zullen u direct feedback geven over de sterkte van uw wachtwoord. Dit wachtwoord zal u bij het openen van elke sessie opgevraagd worden.

Er zal u daarna gevraagd worden om dit wachtwoord een tweede maal in te voeren om de juistheid ervan te controleren. Klik op “Volgende”.

Vervolgens kan u de eerste stap van de aanvraagprocedure afronden.

2.1.12 Overzicht van voltooiing

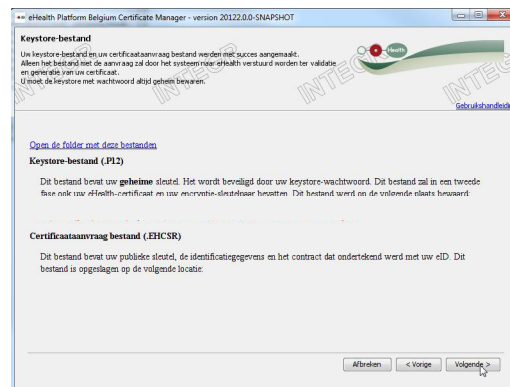
Uw drie bestanden werden met succes aangemaakt:

- Het eerste bestand .P12 bevat uw privésleutel beschermd door een wachtwoord. Stuur dit bestand nooit naar eHealth of een andere partij. Bewaar op elk moment het bestand .P12 en zijn wachtwoord op een veilige manier.
- Het tweede bestand .ehcsr bevat uw identificatiegegevens en de openbare authenticatiesleutel, uw contactgegevens en uw overeenkomst. Dit bestand zal gebruikt worden om uw certificaat aan te maken. U kan dit bewaren in uw archief, maar het zal geen enkel nut meer hebben eens het certificaat correct gepubliceerd is. Het bestand .ehcsr werd elektronisch ondertekend met uw Belgische eID-identiteitskaart.
- Het derde bestand .reqid bevat de referentie van uw aanvraag. Dit bestand zal gebruikt worden om uw aanvraag te identificeren.

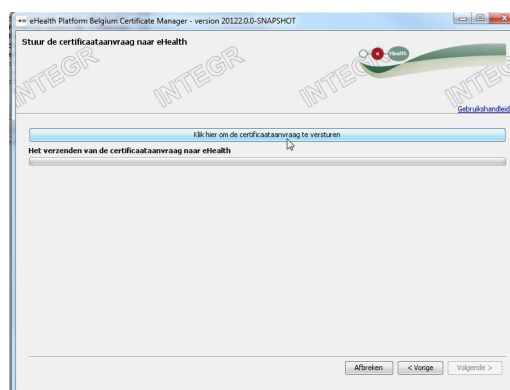
Uw bestanden bevinden zich in een persoonlijk eHealth-opslagdossier. U kan dit dossier rechtstreeks op uw computer openen. Het staat in uw “Home Directory” onder :\\ehealth\keystore\...



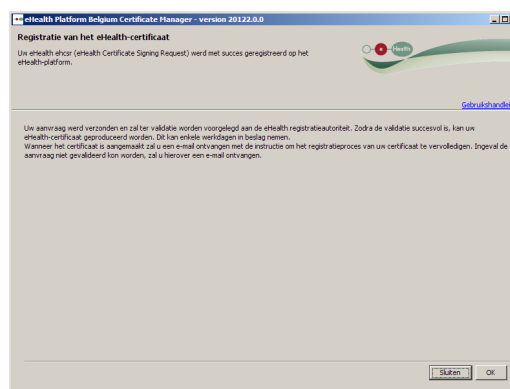
Klik op "Volgende".



Klik op "Klik hier om de certificaataanvraag te versturen".



Het volgende scherm toont aan dat de aanvraag met succes beëindigd werd.



2.2 Validering van de aanvraag door eHealth

2.2.1 Genereren van het authenticatiecertificaat door eHealth

Uw aanvraag werd ontvangen door het eHealth-platform. Het eHealth-platform zal verifiëren of u over de nodige autorisaties beschikt. Dit kan enkele dagen in beslag nemen.

U zal twee verschillende e-mails ontvangen:

1. De eerste om te bevestigen dat u voldoet aan de vereisten van het eHealth-platform om een certificaat te verkrijgen en dat het authenticatiecertificaat aangemaakt zal worden. U kan ook een melding ontvangen waarin staat dat u het certificaat werd geweigerd en waarom. In dit geval moet een nieuwe aanvraag ingediend worden;
2. De tweede om te bevestigen dat het certificaat werd aangemaakt en dat u de "Certificate Manager" opnieuw moet opstarten om het authenticatiecertificaat te downloaden en uw vercijfersleutel aan te maken. Deze mail bevat de referentie van uw aanvraag.

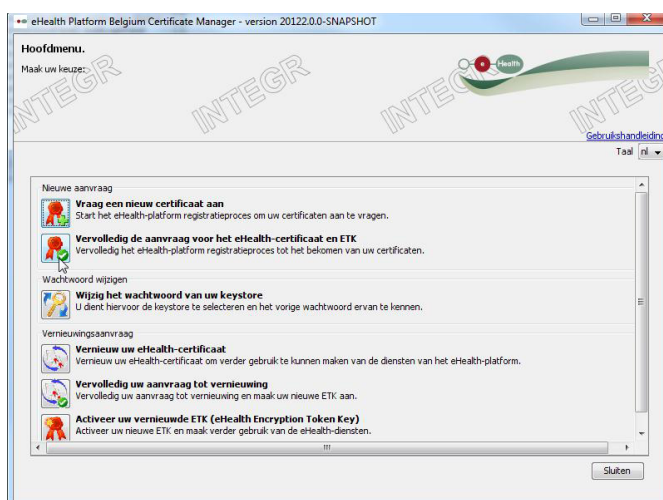
Vervolgens kan u uw aanvraag vervolledigen.

2.3 Voltooiing van de aanvraag en registratie van het certificaat

Klik op de url in de tweede e-mail of voeg de gekende url in:

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

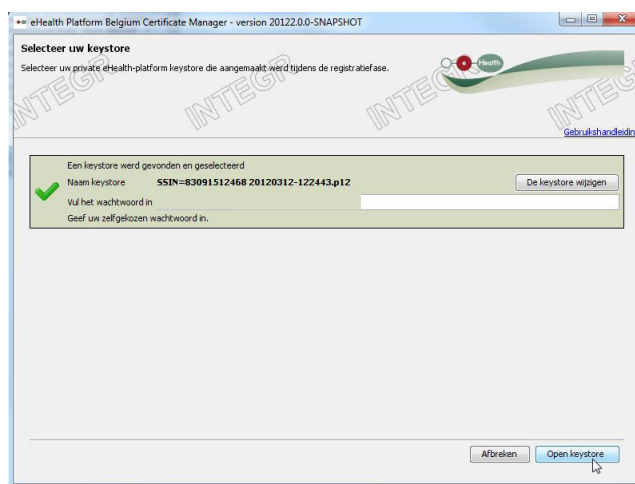
Kies "Vervolledig de aanvraag voor het eHealth-certificaat van uw certificaten".



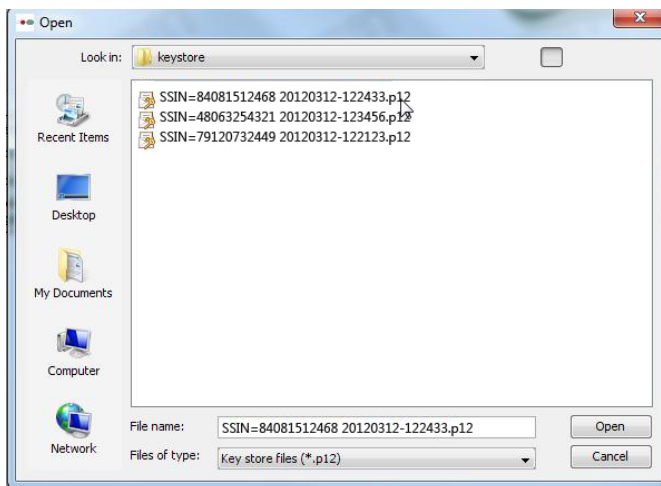
2.3.1 Het keystore-bestand selecteren

Voer het wachtwoord in van het keystore-bestand. Als het wachtwoord correct is, krijgt u toegang tot dit bestand. Klik op “Open keystore”.


Het nieuwste keystore-
bestand wordt automatisch
geselecteerd.

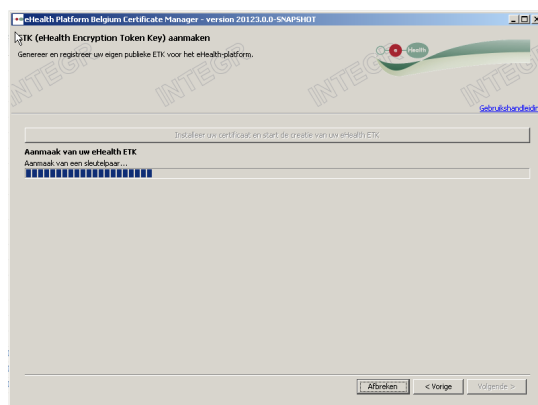
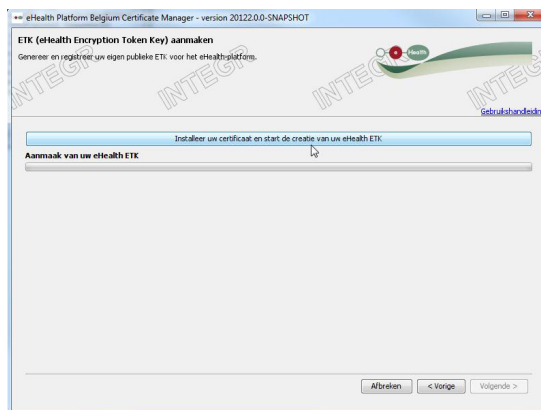


Om een ander keystore-bestand te selecteren, klik op “Keystore veranderen” en selecteer de gewenste keystore.

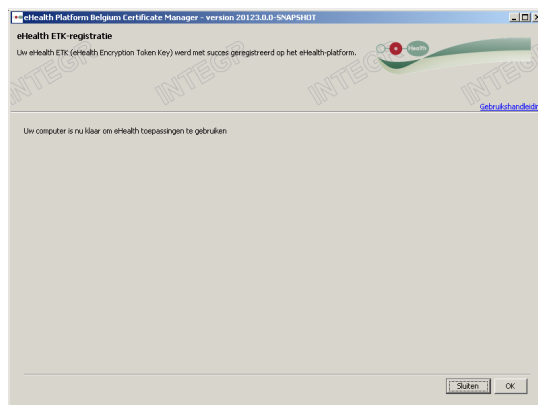


2.3.2 Voltooiing van de registratie en aanmaak van de verscijfersleutel

Klik eerst op de knop "Installer uw certificaat en start de creatie van uw eHealth ETK⁵". Deze bevindt zich boven de laadbalk "Aanmaak van uw eHealth eTK".



Het volgend scherm toont aan dat uw verscijfersleutel met succes geregistreerd werd.

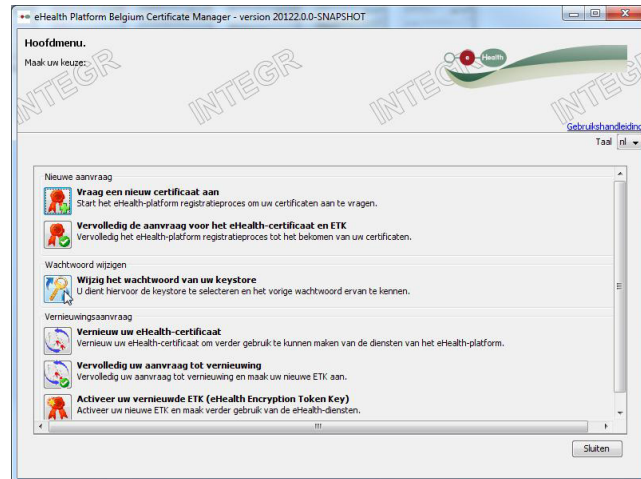


⁵eHealth Encryption Token Key.

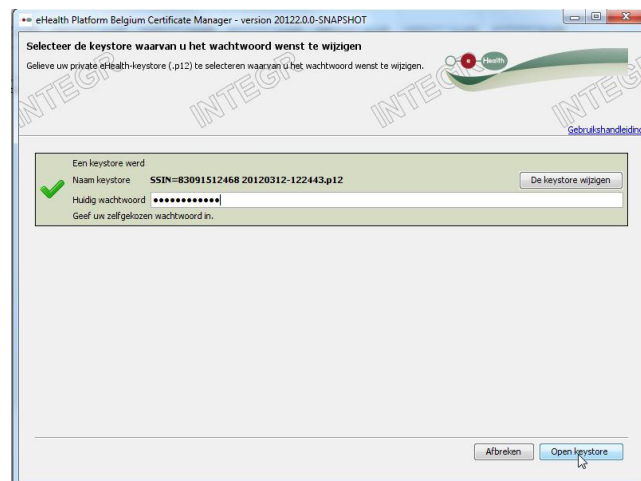


3. Wijzig het wachtwoord van uw keystore

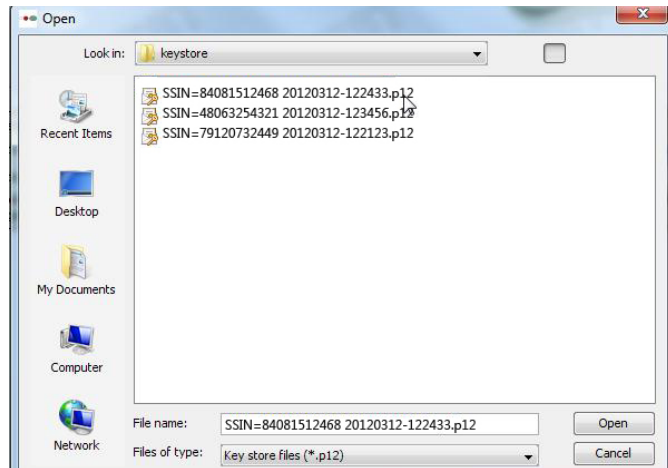
In het hoofdmenu klikt u op “Wijzig het wachtwoord van uw keystore”.



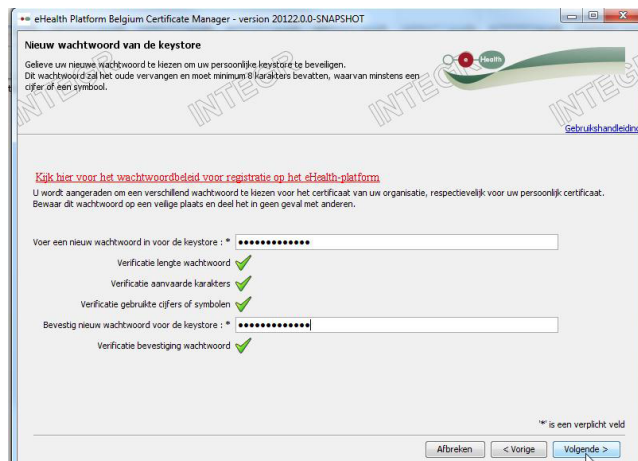
Selecteer de keystore waarvan u het wachtwoord wenst te veranderen en voer het wachtwoord in dat u koos tijdens de aanmaak van uw keystore en klik op de “Keystore wijzigen”.



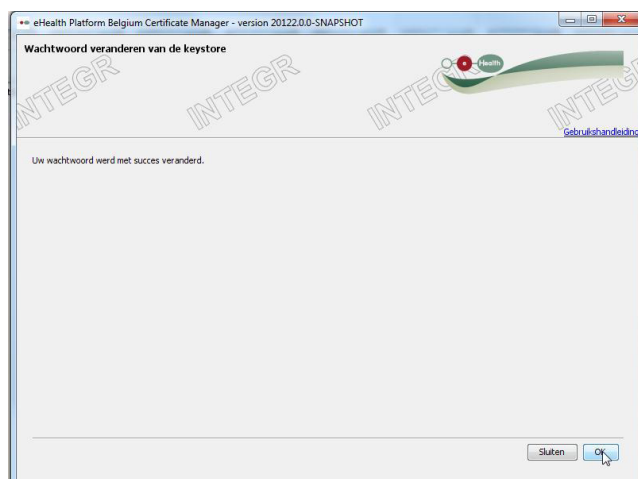
Om een ander keystore-bestand te selecteren, klik op “Keystore veranderen” en selecteer de gewenste keystore.



Voer vervolgens het nieuwe gewenste wachtwoord in en bevestig het.



Het volgende scherm toont u dat het nieuwe wachtwoord met succes geregistreerd werd.



4. Vernieuwing van een certificaat

4.1 Vernieuw uw eHealth-certificaat

De geldigheidsperiode voor een testcertificaat bedraagt momenteel 15 maanden, te tellen vanaf de aanmaakdatum.

De vernieuwing is 2 maanden voor de vervaldatum mogelijk dit wil zeggen vanaf de 13e maand. Voor deze datum wordt de vernieuwing niet toegestaan.

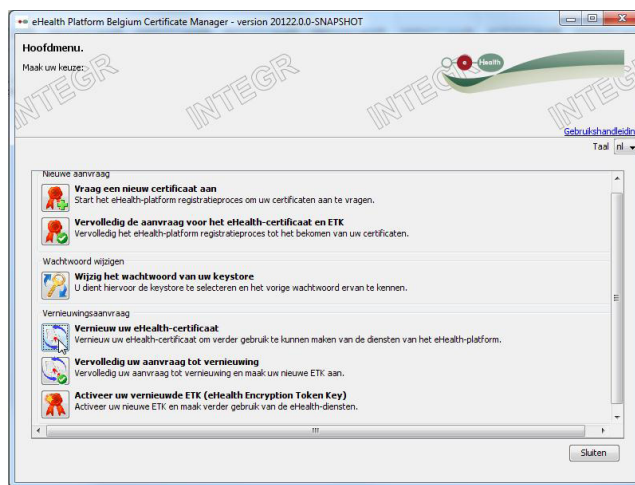
Automatische herinneringen zullen een maand voor de vervaldatum per e-mail gestuurd worden naar de adressen aangegeven tijdens de stap 2.1.6 “Registratie van de contactgegevens”.

Opgepast: de vernieuwingsaanvraag is niet meer mogelijk eens de vervaldatum voorbij is. In dat geval zal een nieuwe aanvraag ingevoerd moeten worden.

Om de continuïteit van deze tool te garanderen, is het noodzakelijk uw certificaat te vernieuwen. U moet een nieuw certificaat aanvragen via de functionaliteit “Vernieuwing” (het gaat dus niet om een verlenging). Daarvoor klikt u op “Vernieuw

i

De vernieuwingsfunctionaliteit houdt in dat een nieuw paar vercijfersleutels en een nieuw vercijfercertificaat zullen worden aangemaakt voor het bestaande certificaat. Tijdens deernieuwings-periode bestaan er dus 2 geldige certificaten, maar een enkel is actief. De certificaathouder zal vervolgens het nieuwe certificaat activeren.



uw eHealth-certificaat” in het hoofdmenu.

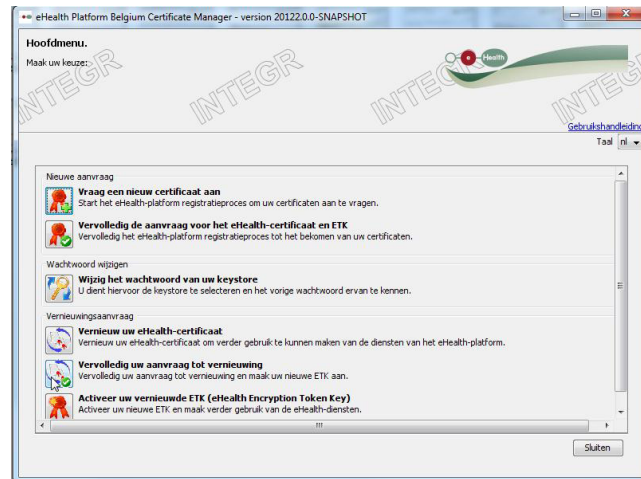
De procedure is dezelfde als bij de invoering van een certificaataanvraag. Volg dus dezelfde stappen vanaf punt 2.1.2.

Na deze stappen gevolgd te hebben, moet u nog “De aanvraag invullen” (4.2.) en vervolgens “Activeer uw vernieuwde ETK” (4.3.).



4.2 Uw aanvraag tot vernieuwing vervolledigen

U hebt de mogelijkheid om het invullen van uw aanvraag tot vernieuwing te hervatten. Klik op "Vervolledig uw aanvraag tot vernieuwing" in het hoofdmenu.

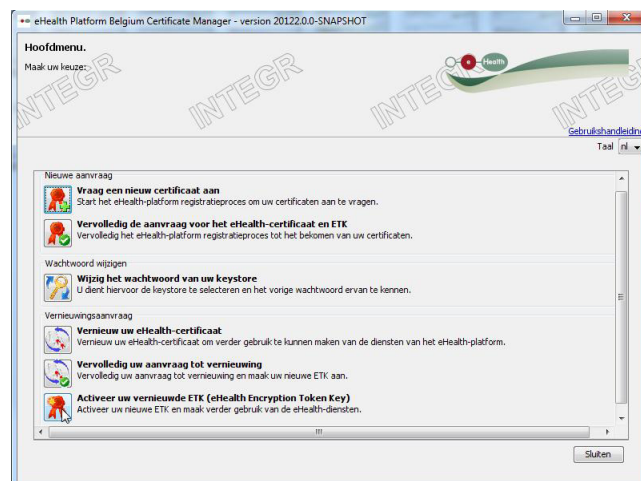


De procedure is dezelfde als voor een certificaataanvraag. Volg dus dezelfde stappen vanaf punt 2.3.

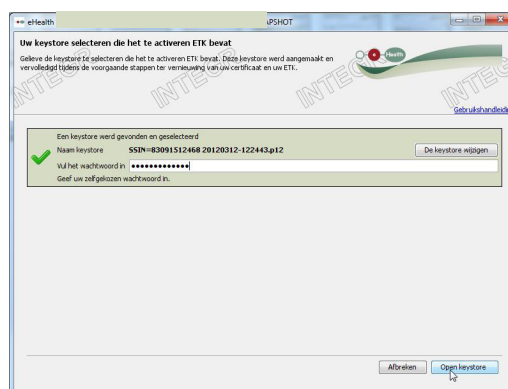
4.3 Activeer uw vernieuwde ETK

Eens uw nieuwe certificaat met succes geregistreerd werd, moet de gebruiker het oude certificaat deactiveren en het nieuwe activeren.

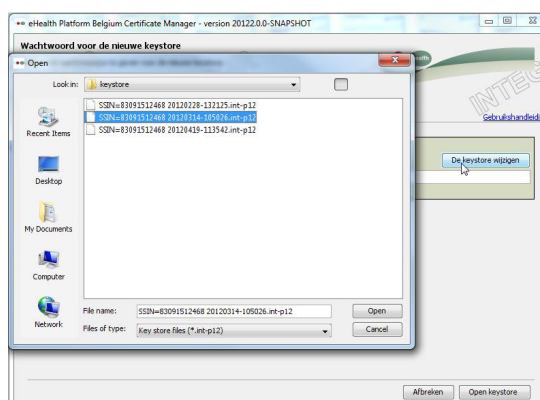
Daarvoor klikt u op "Activeer uw vernieuwde ETK".



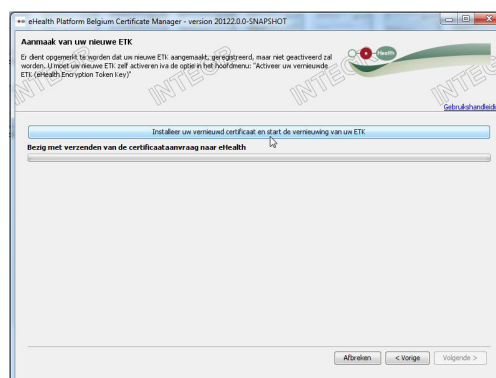
Selecteer de keystore die de nieuwe vertcijfersleutel bevat die geactiveerd moet worden door op de “Keystore wijzigen” te klikken.
Voer het wachtwoord in.
Als het wachtwoord correct is, hebt u toegang tot de keystore.



Klik op “Open Keystore”.



Klik eerst op “Installer uw vernieuwd certificaat en start de vernieuwing van uw ETK”.



Het scherm duidt vervolgens aan dat uw vertcijfersleutel met succes vernieuwd werd.



5. Beveiliging

Uw keystore of wachtwoord zijn uitsluitend persoonlijk en mogen niet overgedragen worden.

Elke gebruiker wordt geacht deze gegevens vertrouwelijk te behandelen. Elke gebruiker is eveneens verantwoordelijk voor het gebruik van zijn gegevens alsook door een derde, tot de deactivatie ervan.

Wij nodigen u uit om kennis te nemen van de veiligheidsregels (beschikbaar op de “Support”-pagina’s van het eHealth-Portaal).

De informatie met betrekking tot “revocatie van een certificaat” is ook beschikbaar op de “Support”-pagina van het eHealth-Portaal.

6. Hulp

Het contactcenter eHealth is bereikbaar via:

- Telefoon:
02 / 788 51 55 (alle werkdagen beschikbaar van 7u00 tot 20u00)
- E-Mail:
 - support@ehealth.fgov.be
- Webformulier:
 - <https://www.ehealth.fgov.be/nl/contact>

Om het telefonisch onderhoud te vergemakkelijken, gelieve volgende documenten binnen handbereik te houden:

- Uw RIZIV-nummer;
- Uw eID;
- Een kopie van uw certificaat.



7. Bijlage

7.1 De “Distinguished Name” (DN) van uw certificaat begrijpen

Het eHealth-certificaat bevat naast andere informatie zoals uw publieke sleutel 7 waarden die de eigenaar identificeren als “Distinguished name”. De DN bestaat uit “Relative Distinguished names”. Deze RDN's moeten worden ingevuld.

De eerste drie velden (nr 1-3) moeten een vooraf bepaalde vaste waarde hebben. De andere velden zullen ingevuld worden met de informatie die u gaf aan de “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. : “SPOEDDIENSTEN”
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, SPOEDDIENSTEN”.

7.1.1 Naam van het land

De waarde voor de naam van het land bestaat uit een keten van 2 karakters die overeenkomen met de ISO3166-1-alpha-2 van de code van het land. In dit geval is de waarde “BE”.

Dit veld staat automatisch op “BE”.

7.1.2 Naam van de organisatie

De naam van de organisatie moet “Federal Government” zijn.

Dit veld staat automatisch op “Federal Government”.

7.1.3 Naam van de organisatie-eenheid

Er zijn 4 verschillende velden met als RDN “organizationalUnitName”. De eerste naam van de organisatie-eenheid is een vaste waarde en wordt gedefinieerd als volgt: “eHealth-platform Belgium”.

Dit veld staat automatisch op “eHealth-platform Belgium”.



7.1.4 Naam van de organisatie-eenheid

Als de certificaataanvraag een natuurlijke persoon betreft, dan wordt de waarde van de voornaam geplakt aan de familienaam in hoofdletters. Bv.: als de voornaam “Jan” is en de familienaam “Peters”, dan wordt de waarde van het veld “JAN PETERS”.

Als de certificaataanvraag een organisatie betreft (KBO-nummer), dan is het een waarde die de exacte kopie moet zijn van de officiële naam van de organisatie zoals gedefinieerd in de DB Public search van de FOD Economie. Het is noodzakelijk om hoofdletters in te voeren en diakritische tekens zijn niet toegestaan.

7.1.5 Naam van de organisatie-eenheid

Dit veld is nodig om de aanvrager van een certificaat te identificeren met behulp van een officieel identificatienummer in een specifiek formaat. Dit formaat is: TYPE identification=Identification VALUE.

Alle karakters van dit veld moeten hoofdletters zijn. Spaties of speciale karakters zijn niet toegelaten. De toegestane karakters zijn [A-Z], [0-9], [-], [=].

U kan in de tabel hieronder zoeken tot welk geval uw certificaataanvraag behoort. De volgende namen van organisatie-eenheden zijn mogelijk, per type en specifieke rol.

Tabel 1: Mogelijke identificatietypes voor de namen van organisatie-eenheden

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, grouppractice, ...	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 of 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 Naam van de organisatie-eenheid

In dit veld, vernoemd als “ID Application”, kunt u een specifieke deelentiteit, departement, applicatiennaam of andere informatie invoeren die de verschillende certificaten van uw organisatie onderscheidt. Dit is het geval als u meerdere departementen hebt die allemaal eindpunten zijn die vertrouwelijk worden gescheiden voor beveiligde communicaties.

bv.: het departement “neonAT” heeft een andere e-mail dan het departement “CARDIOLOGIE”. U zou eveneens een departement “RADIOAPP” kunnen hebben dat gestructureerde berichten ontvangt en dat eveneens een vercijfering vereist voor beveiligde communicatie.

Het veld “4. organizationalUnitName” wordt enkel toegestaan als het certificaat een organisatie betreft. Als de certificaataanvraag een natuurlijke persoon betreft – dit wil zeggen wanneer u het type “NIHII” of “SSIN” gebruikt in het veld “3. organizationalUnitName” – moet de waarde van de RDN “4. organizationalUnitName” nul zijn.

De informatie “deelentiteit/departement/applicatiennaam” zal geïntegreerd worden in het certificaat en zal beschikbaar zijn als zoekcriterium “ID Application” voor de eHealth-gemeenschap.

7.1.7 Algemene naam

De algemene naam moet zorgvuldig samengesteld worden, omdat hij bestaat uit de vorige velden die in een welbepaalde volgorde staan met een specifiek scheidingsteken. De naam bestaat uit:

- De waarde van het identificatietype en het nummer van het veld “3. organizationalUnitName”;
- De ID Applicatie die eerder werd ingevoerd (indien van toepassing) in het veld “4. organizationalUnitName”.

bv.: “NIHII-HOSPITAL=12345678, SPOEDDIENSTEN”

In ons voorbeeld zou de algemene naam beperkt zijn tot “NIHII-HOSPITAL=12345678” Zonder een “ID Applicatie”.



7.1.8 Voorbeeld

Hieronder ziet u een fictief voorbeeld voor de 7 RDN's gedefinieerd door eHealth voor een eHealth-authenticatiecertificaat. Het gaat om een organisatie waarvoor een "ID Applicatie" gedefinieerd werd ("SPOEDDIENSTEN").

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

7.2 Certificeringsautoriteit

De certificeringsautoriteit voor de eHealth-authenticatiecertificaten is Certipost N.V., Muntcentrum, 1000 Brussel, België.

