# Welcome Pack

Het eHealth-platform stelt de partners een gedetailleerde inventaris ter beschikking met de nodige informatie voor de integratie van zijn verschillende diensten. Deze catalogus omvat alles “wat men moet weten”, “wat men dient te begrijpen” en “wat men dient te voorzien” alvorens een project op te starten. Het bevat ook alle nuttige contactadressen.

## Een project dient minstens aan de volgende voorwaarden te voldoen - de inproductiestelling hangt af van de strikte naleving van deze voorwaarden

1. Kennisneming door de partner van de informatie uit ons Welcome Pack
2. Opstellen en goedkeuren van een uniek dossier
3. Goedkeuring door het Sectoraal Comité (indien nodig)
4. Opstellen en goedkeuren van een planning
5. Opstellen en beschikbaar stellen van de technische documentatie (indien nodig)

# Projectproces

1. Kennisneming door de partner van de informatie uit ons Welcome Pack
2. Contactname met onze projectcel door de partner, met een samenvatting van het project: finaliteit van het project, gedefinieerde stromen, vereiste diensten, enz.
3. Interne analyse van het project > Indien akkoord, toewijzing aan een projectleider
4. Indien nodig, indiening van een uniek dossier door de partner
5. Juridisch onderzoek van het project door het eHealth-platform (vereist het project een beraadslaging of een advies van het Sectoraal Comité?)
6. Voorstel van planning in samenspraak met cel IT - opname van het project in de release calendar
7. Contact met de cel IT indien nodig (ondersteuning bij de integratie van de nodige componenten)
8. Indien nodig, beschikbaarstelling van de technische documenten door de partner

## Basisdiensten

1. Coördinatie van elektronische deelprocessen
2. eHealth-certificaten
3. Portal
4. Timestamping
5. Verwijzingsrepertorium (Metahub)
6. Pseudonimisering & Anonimisering
7. Systeem voor end-to-endversleuteling
8. eHealthBox
9. RR Consult
10. I.AM (Identity & Access Management)

## Architectuur

1. Architecturen

## Application LiveCycle

1. Releases Management
2. eHealth Business Continuity Plan
3. Serviceniveaus

## Connectors

1. eHealth platform services connectors

## Onlinediensten

1. Toegang tot de gezondheidskluizen
2. WalCareNet - MemberData

## Informatieveiligheid & Privacy

1. Toolbox
2. Minimale Normen Ziekenhuizen
3. Opleiding & GDPR

## Standards

1. Standards

# Belangrijk bericht

Het eHealth-platform herinnert zijn partners eraan dat het belangrijk is steeds contact op te nemen met de diensten van het eHealth-platform wanneer zij een nieuw project willen ontwikkelen of een bestaand project wensen uit te breiden. Indien zij dit niet doen, kan dit op verschillende niveaus een impact hebben op het eHealth-platform.

Wat de opvolging van de projecten betreft, riskeert het eHealth-platform immers geen globaal zicht meer te hebben op alle projecten die gebruik maken van zijn basisdiensten. Hierdoor zouden incoherenties op architectuurvlak kunnen ontstaan. Een dergelijke manier van werken zou ook kunnen leiden tot een overbelasting van de technische capaciteit van het eHealth-platform in geval van massale en gelijktijdige verzending van berichten, waardoor de beschikbaarheid van de basisdienst voor alle partners in het gedrang komt.

In de algemene voorwaarden met betrekking tot de toekenning van het eHealth-certificaat (acceptatie en productie) wordt sinds september 2013 bepaald dat "elk gebruik van het eHealth-certificaat in voorkomend geval beperkt moet worden tot het toepassingsgebied van de bestaande juridische beraadslagingen. In geval van uitbreiding, aanpassing of evolutie van het doeleinde of van de draagwijdte van dit gebruik moet verplicht met het eHealth-platform contact worden opgenomen".

Het eHealth-platform verzoekt zijn partners bijgevolg om hun verantwoordelijkheid op te nemen en de voorwaarden van het uniek dossier na te leven.

# Basisdiensten

## 1. Coördinatie van elektronische deelprocessen

Deze dienst is gericht op de harmonieuze en flexibele integratie van de verschillende diensten (basisdiensten en toepassingen) binnen een bepaald gegevensuitwisselingssysteem.

De dienst ziet toe op de structurering van de berichten, zodat ze door de verschillende systemen begrepen worden, en waakt erover dat de functionaliteiten compatibel zijn en conform aan bepaalde standaarden en dat er geen verschillen zijn inzake veiligheidsniveaus in de verschillende stappen van de procedure.

Deze coördinatie is transparant voor de gebruiker en gebeurt onder andere aan de hand van een Enterprise Service Bus (ESB).

### Welke functionaliteiten biedt de dienst?

De dienst procescoördinatie biedt de volgende functionaliteiten:

- Standaardisering van de berichten en fouten;
- Controle en propagatie van de identiteit van de gebruiker:
    - de toegepaste controle hangt af van de dienst die opgeroepen wordt door de gebruiker;
- Beheer van de veiligheidsloggings;
- Orkestratie van de oproepen:
    - omvorming van de berichten;
    - verrijking van de berichten;
    - transfer van de berichten naar de webservices van de partners of van het eHealth-platform

### In de praktijk

**Afhankelijkheden, aanbevelingen en waarschuwingen**

**Aanbevelingen**

- de diensten van de partners moeten voorzien in de nodige maatregelen om de stabiliteit en de conformiteit van de diensten die door onze ESB worden opgeroepen te garanderen;
- de diensten van de partners moeten in staat zijn incidenten te onderzoeken;
- elke service consumer moet de richtlijnen over het beveiligen van webservices volgen.

**Waarschuwingen**

- de diensten die asynchroon gegevens uitwisselen mogen geen gebruikmaken van deze dienst.

**Wat zijn de voorwaarden voor de integratie van een dienst binnen het eHealth-platform ?**

- Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform via eHealthppkb@ehealth.fgov.be en geef een duidelijke beschrijving van de context en de doelstelling van uw project en een raming op het vlak van volume.
- Om de integratie van het oproepen van de diensten te vergemakkelijken, kan het eHealth-platform deze diensten opnemen in de 'connectoren'.

Meer informatie: support@ehealth.fgov.be

# 2. eHealth-certificaten

### Wat is een eHealth-certificaat?

De certificaten die uitgereikt worden door het eHealth-platform laten toe aan een persoon of een organisatie om zich te authentiseren als zorgverlener of erkende instelling.

Wanneer een zorgverlener toegang wenst tot bepaalde basisdiensten van het eHealth-platform met gebruik van een system-to-systemverbinding en niet een webtoepassing, moet hij over een eHealth-certificaat beschikken. Op basis van dit certificaat kan de "systeem"-partner worden geïdentificeerd en geauthentiseerd terwijl het op basis van de eID of de token mogelijk is om de gebruiker (de persoon) te identificeren en authentiseren.

Dit geldt zowel voor het gebruik van basisdiensten als voor het gebruik van toepassingen die aangeboden worden in de vorm van webservices.

Eenmaal het certificaat geconfigureerd is in de software van de zorgverlener of de instelling kan gebruik worden gemaakt van de diensten die door het eHealth-platform ter beschikking worden gesteld en die een authenticatie vereisen.

Een eHealth-certificaat kan worden aangevraagd en geïnstalleerd via een toepassing die gedownload kan worden op de site van het eHealth-platform.

Wanneer u beschikt over een Java-versie die recenter is dan Java 8, kan de bovenstaande link **niet** meer gebruikt worden om de toepassing te starten. Daarom wordt de applicatie via deze link eveneens aangeboden in een ZIP-file. In dit geval kan u het bestand uitpakken naar een map op uw computer en het programma starten via het .cmd (Windows) of .sh (MacOS, Linux) bestand.

De software-integratoren (niet de zorgverleners) kunnen bovendien test-certificaten aanvragen. Op basis van deze certificaten kunnen de IT-medewerkers van deze software-integratoren, die actief zijn in de Belgische gezondheidszorg, de integratie van onze basisdiensten testen. Meer informatie over acceptatie-certificaten.

### Welke functionaliteiten biedt een eHealth-certificaat?

Het certificaat biedt de volgende functionaliteiten:

- de mogelijkheid voor de zorgverlener of de instelling om zich te authentiseren in het kader van het gebruik van de eHealth-webservices, onder meer door een sessie token aan te vragen op basis waarvan toegang verleend wordt tot deze diensten
- de mogelijkheid om berichten te vercijferen, bijvoorbeeld in het kader van het gebruik van een eHealthBox
    - het certificaat en het daaraan verbonden paswoord dienen dan als private sleutel voor de vercijfering
- de mogelijkheid voor een zorgverlener of instelling om vercijferde berichten te ontvangen
    - samen met het certificaat wordt immers een publieke sleutel aangemaakt en ter beschikking gesteld van het publiek via een daartoe bestemde webservice (ETEE ETKDepot)

### In de praktijk

#### Afhankelijkheden, aanbevelingen & waarschuwingen

Voor een individuele zorgactor betekent dit dat:

- de doelgroep in een gevalideerde authentieke bron geregistreerd is
- de actor over een sterk authenticatiemiddel beschikt (eID)

    - voor niet-Belgische zorgverleners, die de facto niet over een eID beschikken, maar die wel actief zijn in België en behoefte hebben aan toegang tot de online diensten en die dus een certificaat nodig hebben, bestaat er een hybride oplossing.

Voor zorgorganisaties betekent dit dat:

- de doelgroep in een gevalideerde authentieke bron geregistreerd is, incl. de gevolmachtigde certificaathouder namens de zorginstelling
- de certificaathouder over een sterk authenticatiemiddel beschikt
- de minimale veiligheidsnormen van de KSZ worden gerespecteerd
- de interne werking van de zorgorganisatie moet garanderen dat enkel geautoriseerde personen toegang hebben tot het systeem
- de beraadslagingen van het informatieveiligheidscomité inzake het delen van zorggegevens tussen zorgorganisaties worden gerespecteerd

Om een eHealth-certificaat te gebruiken voor de authenticatie in het kader van een webservice, dient de zorgverlener te beschikken over een medisch softwarepakket dat deze dienst geïntegreerd heeft (dit is het geval voor alle softwarepakketten die geregistreerd werden door het eHealth-platform).

Vooraleer aan de slag te gaan met (de aanvraag van) een eHealth certificaat: neem steeds kennis van de project onboarding informatie in het Welcome Pack, het gebruiksreglement alsook de richtlijnen voor veilig gebruik van eHealth certificaten in het kader van een medische context.

## Aanvraag van een certificaat - Werkwijze

**Wie kan een certificaat aanvragen?**

- de zorgverleners die actief zijn in de Belgische gezondheidszorgsector

Belangrijk:

- er moet een onderscheid worden gemaakt tussen een individueel (persoonlijk) certificaat en een certificaat voor een organisatie (voor een zorginstelling)
    - in het geval van een certificaat voor een organisatie of een instelling is een gevolmachtigd certificaathouder namens de rechtspersoon verantwoordelijk voor het correcte beheer en gebruik van het certificaat. Dit betekent dat deze certificaathouder verantwoordelijk is voor de strikte naleving van de gebruiksvoorwaarden.
- een certificaat is 36 maanden geldig (hernieuwbaar vanaf 90 dagen vóór het einde van de periode van 36 maanden/3 jaar)

**Aanvraagprocedure**

Dien uw aanvraag in via de toepassing eHealth Certificate Manager

Deze toepassing biedt de volgende functionaliteiten:

- aanvraag van een eHealth-certificaat en encryptiesleutels (zie End-to-end vercijfering voor de sleutels)
- hernieuwing van een certificaat (binnen de hernieuwingsperiode van drie maanden);
- intrekking van een certificaat;
- wijziging van het paswoord voor de encryptiesleutels.

# 3. Portal

Het Portaal van de diensten eGezondheid is vanuit historisch oogpunt een gecoördineerd en beveiligd toegangspunt voor de actoren in de gezondheidszorg tot de verschillende beschikbare applicaties en informatie over online gezondheid (eGezondheid). Het biedt tevens alle beschikbare informatie voor de technische ondersteuning van de ICT-ontwikkelaars bij de integratie van onze basisdiensten. Het beheer van de inhoud van het portaal wordt verzekerd aan de hand van een 'Content Management System' (cms) dat toelaat de inhoud (teksten, FAQ, onlinesupport, documenten, navigatiestructuur, enz.) op een dynamische manier uit te werken en te actualiseren.

### Welke functionaliteiten biedt een cms?

De integratie van een cms voor het beheer van een website of een applicatie biedt de volgende functionaliteiten (niet-exhaustieve opsomming)

- Beheer van generieke inhoud: news, FAQ, support,...
    - kenmerken van een type content
        - verplichte of optionele velden
        - mogelijkheid om links tussen content te creëren
        - meer dan 30 mogelijke gegevenstypes (data, numerieke gegevens, vrije tekst, kleuren)
        - meerdere talen mogelijk
- Beheer van de toegangs- en publicatierechten volgens gebruikersprofiel (auteur, publisher, admin, ...)
- Beheer van de publicatieketen (workflow) voor de goedkeuring en de publicatie van de inhoud
- Beheer van de verschillende versies

- Historiek van de wijzigingen volgens datum en auteur
- Mogelijkheid om verschillende publicatieformaten te beheren: JSON, XML, HTML, …

### In de praktijk

**Afhankelijkheden, aanbevelingen en waarschuwingen**

Het is wenselijk dat de toepassing of website over zijn eigen cache-geheugen beschikt teneinde

- over een fallbackscenario te beschikken in geval van onbeschikbaarheid van het cms
- niet telkens het cms te moeten oproepen bij elk request (belastingsherverdeling vermijden) bijvoorbeeld en het cms maximaal om de minuut op te roepen

**Wat zijn de voorwaarden voor de integratie van de dienst binnen het eHealth-platform?**

Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform via eHealthppkb@ehealth.fgov.be en geef een duidelijke beschrijving van de context van uw project

# 4. Timestamping

### Wat is timestamping?

Het eHealth-platform biedt aan zijn partners een dienst timestamping (elektronische datering of gecertificeerde tijdstempel) aan.

Timestamping is een systeem dat toelaat een bewijs te bewaren van het bestaan van een document en de inhoud ervan op een bepaalde datum. De term 'bewijs' verwijst naar het feit dat niemand, zelfs niet de eigenaar van het document, het timestamping-certificaat kan wijzigen.

### Welke functionaliteiten biedt timestamping?

Deze dienst biedt verschillende functionaliteiten:

- een klassieke webservice voor elektronische datering (TimeStampAuthority) die instaat voor de certificering van het document en, indien nodig, voor de archivering ervan (facultatief);
- een webservice voor de raadpleging (TimeStampConsult) van de getimestampte documenten die de controle van de getimestampte documenten gedurende een bepaalde periode verzekert.

## In de praktijk

### Afhankelijkheden, aanbevelingen & waarschuwingen

De dienst timestamping van het eHealth-platform wordt momenteel gebruikt in het kader van:

- het elektronisch voorschrift in de ziekenhuizen (hoofdzakelijk);
- het ambulant elektronisch voorschrift (Recip-e);
- MyCareNet;
- RCT.

### Wat zijn de voorwaarden voor de integratie van de dienst Timestamping van het eHealth-platform ?

- Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform, Valérie Forton, en geef een duidelijke beschrijving van de context en de finaliteit van uw project.
- Indien akkoord, dient u te beschikken over een eHealth-certificaat

### Elektronisch voorschrift in de ziekenhuizen - Specifieke context

Concreet stelt een ziekenhuisarts een elektronisch voorschrift op (te certificeren document) dat naar de apotheek van zijn ziekenhuis wordt verstuurd. Dit voorschrift wordt ‘gehasht’, dat wil zeggen dat het omgevormd wordt tot een unieke cijfercode zonder logische betekenis.

Elke 5 minuten worden de cijfercodes samengebracht in een pakket, de zogenaamde ‘TimeStampBag’. Dit pakket wordt naar het eHealth-platform verstuurd zodat de‘Timestamping’-dienst er een precieze datum en uur aan zou toevoegen. Dit 'pakket', voorzien van een datering, wordt vervolgens teruggestuurd naar het ziekenhuis voor bewaring in het ziekenhuisarchief. Het eHealth-platform bewaart zelf een kopie van het 'pakket' met datering. Het eHealth-platform levert met andere woorden het bewijs dat de elektronische voorschriften op een bepaalde datum en tijdstip werden aangemaakt, maar heeft zelf geen kennis van de inhoud ervan aangezien die gecodeerd is. In geval van controle wordt het hashingsysteem opnieuw toegepast op het voorschrift. De verkregen code wordt vergeleken met de code die bij het eHealth-platform wordt bewaard. Indien beide codes identiek zijn, betekent dit dat het voorschrift niet gewijzigd werd.

### Hoe kan een ziekenhuis timestamping gebruiken voor de elektronische voorschriften?

- Het eHealth-platform stelt de ziekenhuizen de tool TimeStamping Client ter beschikking, die dienst doet als referentie-implementatie.

- De documentatie die de installatie en werking van deze tool beschrijft, is hieronder beschikbaar.
- Een ziekenhuis kan echter ook zijn eigen oplossing ontwikkelen of de oplossing van een softwareleverancier installeren, voor zover die voldoet aan dezelfde specificaties als de referentie-implementatie.
- In elk geval dient deze oplossing te interageren met het eHealth-platform via de diensten TimeStamping Authority en TimeStamping Consultation teneinde de voorschriften te dateren en controles te verrichten tussen het archief van het ziekenhuis en het archief van het eHealth-platform.

### Wettelijke voorwaarden voor het gebruik van de dienst Timestamping

Wat timestamping en de ziekenhuisvoorschriften betreft, is het gebruik van deze dienst wettelijk geregeld (zie de verordening van 5 december 2016 betreffende het elektronisch voorschrift binnen het ziekenhuis).

Meer informatie: support@ehealth.fgov.be

## 5. Verwijzingsrepertorium (Metahub)

### Wat is de dienst ‘Verwijzingsrepertorium’ (Metahub) ?

De dienst Metahub van het eHealth-platform alsook de bijbehorende diensten ‘Consent’, ‘Therlink’ en ‘Exclusions’ vormen samen een reeks diensten voor het beheer van de toegang tot de medische gegevens van een patiënt. Deze diensten zijn, naargelang het geval, toegankelijk voor de hubs, de individuele zorgverleners, bepaalde zorginstellingen zoals ziekenhuizen of apotheken en ten slotte ook voor de patiënten.

Het betreft dus een index van de gezondheidsgegevens van de patiënten.

Een dergelijke index is de hoeksteen voor een gedecentraliseerd systeem inzake uitwisseling van gezondheidsgegevens tussen zorgverleners en zorginstellingen.

Wat dit betreft, is het belangrijk erop te wijzen dat het verwijzingsrepertorium is opgebouwd uit 2 'lagen':

- een eerste laag, 'metahub' genaamd, bevindt zich op het niveau van het eHealth-platform en duidt aan dat informatie beschikbaar is in
  - een lokaal of regionaal netwerk, 'hub' genaamd, of
  - indien er geen aansluiting op een hub is, in een gezondheidskluis
- een tweede laag situeert zich op het niveau van de hubs
  - elke hub houdt een verwijzingsrepertorium bij waarin hij aanduidt bij welke zorginstelling of bij welk ander uitwisselingsnetwerk aangesloten op de hub een gezondheidsgegeven met betrekking tot een patiënt beschikbaar is

De volgende concepten worden gebruikt door de diensten die verbonden zijn aan de dienst Metahub en laten toe de toegang tot de medische gegevens van de patiënt te beheren:

- de patiëntlink of de link tussen een hub en een patiënt laat toe te achterhalen in welke hub(s) gegevens met betrekking tot de patiënt kunnen worden geraadpleegd
    - het geheel van ‘patiëntlinks’ vormt samen het verwijzingsrepertorium
- de toestemming van de patiënt voor het delen van zijn gezondheidsgegevens
    - er wordt geen toegang verleend tot de gegevens van een patiënt zonder zijn toestemming
- de therapeutische relatie tussen een patiënt en een zorgverlener (KB 78)
    - het betreft een vastgestelde zorgrelatie (bijvoorbeeld het feit een huisarts te raadplegen)
    - in afwezigheid van een therapeutische relatie krijgt een zorgverlener geen toegang tot de gegevens van de patiënt, tenzij in geval van nood volgens een zogenaamde ‘breaking the glass’-procedure
- de zorgrelatie tussen een patiënt en een zorgverlener/zorgorganisatie (buiten KB 78)
- de uitsluiting van een zorgverlener/zorgorganisatie door een patiënt
    - de zorgverlener/zorgorganisatie krijgt geen enkele toegang tot de gegevens van een patiënt indien een uitsluiting geregistreerd werd (ook als er een therapeutische relatie /zorgrelatie geregistreerd is)

Daarbij kunnen we verwijzen naar vijf fundamentele regels:

- het delen van documenten waarnaar er een referentie bestaat in het verwijzingsrepertorium is slechts mogelijk voor zover de patiënt zijn toestemming gegeven heeft
- de raadpleging van een referentie door een zorgverlener/zorgorganisatie vereist het bestaan van een 'therapeutische relatie' of 'zorgrelatie' tussen deze zorgverlener/zorgorganisatie en de betrokken patiënt
- de patiënt heeft te allen tijde de mogelijkheid om een herroeping te doen van:
    - zijn toestemming voor de uitwisseling van gezondheidsgegevens
    - een of meerdere eerder geregistreerde therapeutische relaties/zorgrelaties
- de patiënt beschikt op elk moment over de mogelijkheid om een zorgverlener/zorgorganisatie uit te sluiten van de toegang tot zijn gegevens
- het delen van de gegevens waarvoor er een referentie bestaat kan enkel op basis van de toegangsmatrix

De diensten verbonden aan de Metahub zijn beschikbaar in de vorm van webservices (toegankelijk via een medisch softwarepakket of een toepassing van derden) en zijn voor sommige functionaliteiten beschikbaar voor de patiënt in de vorm van een webtoepassing (toegankelijk via een pc en een eID, ITSME of TOTP).

## Wat zijn de functionaliteiten van de diensten verbonden aan de dienst Metahub ?

De webservice Metahub is enkel toegankelijk voor de hubs en biedt de volgende functionaliteiten:

- de aanmaak of verwijdering van links tussen de hub en patiënten die erin gekend zijn (patiëntlinks) met het oog op de werking van de verwijzingsrepertoria voor de toegang tot de gegevens van de patiënten
- de raadpleging van deze 'patiëntlinks' in het kader van de verwijzingsrepertoria voor de toegang tot de gegevens van de patiënten
- de aangifte, herroeping of raadpleging van de toestemming van de patiënt voor de uitwisseling van zijn gezondheidsgegevens
- de aangifte, herroeping of raadpleging van therapeutische relaties/zorgrelaties tussen een patiënt en een zorgverlener/zorgorganisatie (KB 78 / buiten KB 78)
- de aangifte, herroeping of raadpleging van uitsluitingen tussen een patiënt en een zorgverlener/zorgorganisatie (KB 78 / buiten KB 78)
- de raadpleging van de historiek van de activiteiten verbonden aan een patiënt binnen de dienst Metahub

De webservice voor het beheer van de toestemming is toegankelijk voor de patiënten (en hun lasthebbers of ouders), voor de individuele zorgverleners en de ziekenhuizen en biedt de volgende functionaliteiten:

- de aangifte, herroeping of raadpleging van de toestemming van de patiënt voor het delen van zijn gezondheidsgegevens

De webservice voor het beheer van de therapeutische relaties is toegankelijk voor de patiënten (alsook hun lasthebbers of ouders), voor de individuele zorgverleners/zorgorganisaties en biedt de volgende functionaliteiten:

- de aangifte, herroeping of raadpleging van therapeutische relaties tussen een patiënt en een zorgverlener of een apotheek

De webservice voor het beheer van de uitsluitingen is toegankelijk voor de patiënten (en hun lasthebbers of ouders) en biedt de volgende functionaliteiten:

- de aangifte, herroeping of raadpleging van uitsluitingen tussen een patiënt en een zorgverlener/zorgorganisatie

De webtoepassing voor het beheer van de toestemming van de patiënt voor het delen van zijn gezondheidsgegevens, de therapeutische relaties/zorgrelaties en de uitsluitingen is toegankelijk voor de patiënten via het portaal MijnGezondheid en biedt de volgende functionaliteiten:

- de aangifte, herroeping of raadpleging van de toestemming van de patiënt voor het delen van zijn gezondheidsgegevens
- de aangifte, herroeping of raadpleging van therapeutische relaties / zorgrelaties tussen een patiënt en een zorgverlener/zorgorganisatie
- de aangifte, herroeping of raadpleging van uitsluitingen tussen een patiënt en een zorgverlener/zorgorganisatie
- de opzoeking van een zorgverlener op basis van zijn naam en voornaam of RIZIV-nummer om een therapeutische relatie/zorgrelatie of een uitsluiting te registreren
- de opzoeking van een zorgorganisatie op basis van haar naam, adres of RIZIV-nummer om een therapeutische relatie/zorgrelatie of een uitsluiting te registreren

## In de praktijk

### Afhankelijkheden, aanbevelingen en waarschuwingen

Om gebruik te maken van de webservice voor het beheer van de toestemming van de patiënt voor het delen van zijn gezondheidsgegevens, de webservice voor het beheer van de therapeutische relaties en de webservice voor het beheer van de uitsluitingen, zal de zorgverlener/zorgorganisatie of de patiënt moeten beschikken over een medisch softwarepakket dat deze dienst integreert.

De webservice voor het beheer van de toestemming van de patiënt voor het delen van zijn gezondheidsgegevens, de webservice voor het beheer van de therapeutische relaties/zorgrelaties en de webservice voor het beheer van de uitsluitingen zijn beschikbaar als REST-diensten die de integratie in mobiele of webapplicaties van derden faciliteren.

De webservice Metahub is enkel toegankelijk voor de hubs die erkend zijn door het eHealth-platform en dient dus geïntegreerd te worden in de informatica-oplossing van de hub.

De definitie van de principes, de functionaliteiten en de architectuur van het verwijzingsrepertorium en de relatie met de verschillende gezondheidssystemen die erop aangesloten zijn gebeurt onder leiding van diverse werkgroepen die opgericht zijn door het Overlegcomité met de gebruikers van het eHealth-platform.

Het is belangrijk erop te wijzen dat er een specifieke goedkeuringsprocedure van toepassing is (Overlegcomité met de gebruikers, het Beheerscomité en het Informatieveiligheidscomité).

De wetgevende teksten op dit vlak zijn beschikbaar via de pagina met de belangrijkste reglementen.

De realisatie, het onderhoud en het operationele beheer van de verschillende componenten van het verwijzingsrepertorium zijn verdeeld over de verschillende partners die betrokken zijn bij het project: het eHealth-platform staat in voor het gedeelte 'Metahub', terwijl de organisaties van zorgverleners en zorginstellingen, alsook de andere betrokken instanties elk verantwoordelijk zijn voor hun eigen 'hub' of gezondheidssysteem.

### Wat zijn de voorwaarden voor de integratie van de dienst Metahub van het eHealth-platform ?

Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform Peter Laridon en geef een duidelijke beschrijving van de context en de doelstelling van uw project en een raming op het vlak van volume.

Om de oproep van de webservice voor het beheer van de toestemming en de webservice voor het beheer van de therapeutische relaties te integreren, stelt het eHealth-platform ‘connectoren’ ter beschikking van de actoren in de gezondheidszorg.

Stuur een mail om meer info te vragen

## 6. Pseudonimisering & Anonimisering

In de Europese Unie en a fortiori in België is de uitwisseling van gezondheidsgegevens strikt gereglementeerd en omkaderd in de privacywet. In die context is het strikt noodzakelijk om een machtiging te krijgen van het Informatieveiligheidscomité vooraleer tot elk gebruik of uitwisseling van dergelijke gegevens kan worden overgegaan. Op basis van de behoeften zal het IVC een afdoend beveiligingsniveau opleggen.

Hiertoe stelt het eHealth-platform verschillende diensten ter beschikking van zijn partners waardoor de persoonsgegevens m.b.t. de gezondheid omgezet worden naar gecodeerde of anonieme gegevens waaruit de identiteit van de patiënt en/of de zorgverlener niet rechtstreeks of onrechtstreeks kan worden afgeleid.

**Pseudonimisering**

De pseudonimisering bestaat erin de inhoud of de structuur van de gezondheidsgegevens op omkeerbare wijze te wijzigen zodat de personen waarop deze gegevens betrekking hebben, niet meer identificeerbaar zijn.

Verschillende diensten zijn daartoe beschikbaar:

1. De pseudonimisering 'WS SEALS' die via de integratie van een webservice ‘WS Seals’ de volgende functies biedt:
    - ‘Encode’: waarbij gegevens als input kunnen worden ingevoerd om vervolgens in gecodeerde vorm te worden teruggegeven

    - ‘Decode’: waarbij gecodeerde gegevens als input kunnen worden ingegeven om vervolgens als niet-gecodeerde gegevens te worden teruggegeven
2. De pseudonimisering 'Batch codage'
    - waarbij het eHealth-platform als vertrouwensderde (TTP –Trusted Third-Party) optreedt in het codeer- en decodeerproces van de gezondheidsgegevens voor rekening van de partner
3. De pseudonimisering 'Blinded pseudo' (afgeleide dienst)
    - die de mogelijkheid biedt om pseudoniemen aan te passen afhankelijk van de partij die de gegevens verwerkt, zonder deze gegevens te de-pseudonimiseren, zodat de identiteit van de betrokkene beschermd blijft;
    - het gaat strikt genomen niet om een basisdienst maar om een afgeleide dienst die evenwel voldoet aan dezelfde kwaliteits- en veiligheidsstandaarden als de basisdiensten die in de eHealth-wet beschreven zijn;
    - sommige “Blinded pseudocompatibel" diensten kunnen deze pseudonimiseringscategorie integreren

**Anonimisering**

Anonimisering is het woord dat door het eHealth-platform wordt gebruikt om de dienst te beschrijven waarbij de inhoud of de gegevensstructuur wordt gewijzigd zodat de identificatie van de personen waarop de gegevens betrekking hebben, onmogelijk wordt. De anonimisering is onomkeerbaar en vereist de tussenkomst van een TTP.

## In de praktijk

**Wat zijn de implementatievoorwaarden?**

- Een akkoord van het Informatieveiligheidscomité is verplicht
- Neem contact op met de verantwoordelijke van de dienst binnen het eHealth-platform en beschrijf duidelijk de context en het doeleinde van uw project. Hou er rekening mee dat een akkoord van het Informatieveiligheidscomité verplicht is
    - voor de dienst pseudonimisering 'WS SEALS' > nicolas.donnez@ehealth.fgov.be
    - voor de dienst pseudonimisering 'Batch codage' > wolf.wauters@health.fgov.be
    - voor de afgeleide dienst pseudonimisering 'Blinded pseudo' > pseudo@ehealth.fgov.be
    - voor de dienst anonimisering > nicolas.donnez@ehealth.fgov.be
    - bijkomende vragen kunnen worden verstuurd naar TTP@ehealth.fgov.be
- Indien akkoord, dient u te beschikken over een e-Health-certificaat en te voorzien in de implementatie van een versleutelingsdienst

# 7. Systeem voor end-to-endversleuteling

### Wat is de dienst End to End Encryption van het eHealth-platform?

De dienst End to End Encryption (ETEE) (ook wel versleutelings- of encryptiedienst genoemd) van het eHealth-platform is een reeks diensten die toelaten berichten gericht aan zorgverleners (individuele zorgverleners of instellingen) te versleutelen. Deze diensten zijn toegankelijk voor individuele zorgverleners en instellingen en in sommige gevallen ook voor patiënten.

De versleutelingsdiensten worden onder meer toegepast in het kader van het gebruik van de eHealthBox-dienst of de elektronische voorschriften (Recip-e).

De ETEE-diensten zijn de volgende:

- ETKDepot (SOAP & REST) en KeyDepot (REST) voor de versleuteling naar een gekende bestemmeling
- KGSS(SOAP & REST) voor de versleuteling naar een niet-gekende bestemmeling

De ETEE-diensten zijn beschikbaar als webservices (toegankelijk via een medisch softwarepakket of via een externe toepassing).

### Welke functionaliteiten biedt de dienst End to End Encryption?

De webservice ETKDepot is toegankelijk voor iedereen en biedt de volgende functionaliteiten:

- de opzoeking van een ETK, dit wil zeggen de publieke sleutel die verbonden is aan het eHealthcertificaat van een zorgverlener of een instelling waarvan de identificatienummers (INSZ, RIZIV-nummer, KBO-nummer) gekend zijn. Aan de hand van de REST-dienst kan tevens de certificaathouder worden achterhaald.
    - eens verkregen, laat die ETK toe om een bericht te versleutelen ter attentie van een gekende bestemmeling (de zorgverlener of instelling).

De webservice KGSS (Key Generation and Storage System) is toegankelijk voor iedereen en biedt de volgende functionaliteiten:

- de aanmaak van een symmetrische encryptiesleutel die opgeslagen zal worden door het eHealth-platform en die toegankelijk zal zijn volgens de voorwaarden van degene die de sleutel heeft aangemaakt;
- het ophalen van een bestaande sleutel, op voorwaarde dat het identificatienummer van de sleutel gekend is en de toegangsvoorwaarden die vastgesteld werden bij de aanmaak van de sleutel voldaan zijn (bijvoorbeeld: geauthenticeerd zijn als apotheker erkend door het eHealth-platform).

- dankzij de REST-dienst is het tevens mogelijk voor de houder om een bestaande sleutel te verwijderen

Deze functionaliteiten laten toe de dienst KGSS te gebruiken indien de identiteit van de bestemmeling van het versleutelde bericht niet op voorhand gekend is, maar dat bepaalde voorwaarden voldaan moeten zijn om de encryptiesleutel te verkrijgen.

De webservice KeyDepot is voor alle doelgroepen toegankelijk en biedt de volgende functies:

- De aanmaak van een sleutelpaar; de openbare sleutel zal door het eHealth-platform worden opgeslagen en voor alle doelgroepen toegankelijk zijn
- De toevoeging van informatie voor een reeds bestaande openbare sleutel door de houder ervan
- De opzoeking van een openbare sleutel
- De verwijdering van openbare sleutels door de houder ervan
- De opzoeking van alle openbare sleutels met betrekking tot een persoon
- De opzoeking van het 'attestation object' met betrekking tot een openbare sleutel
- De opzoeking van informatie over de houder van een sleutel

## In de praktijk

### Afhankelijkheden, aanbevelingen en waarschuwingen

Om gebruik te maken van de webservice ETKDepot of de webservice KGSS, dient de zorgverlener of de patiënt te beschikken over een medisch softwarepakket waarin deze dienst geïntegreerd is. Beide diensten zijn ook geïntegreerd in globalere oplossingen zoals Recip-e, Hoofdstuk IV, eHealthBox.

Er is een technische bibliotheek beschikbaar ter ondersteuning van uw versleutelingsbewerkingen.

### Wat zijn de voorwaarden voor de integratie van de dienst End to End Encryption van het eHealth-platform?

- Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform Kris Van Aken en schets duidelijk de context, het doeleinde en het geschatte volume van uw project.

Stuur een e-mail om meer informatie te vragen

# 8. eHealthBox

De dienst eHealthBox van eHealth-platform is een beveiligde elektronische brievenbus, die specifiek ontwikkeld werd voor de zorgverleners en instellingen. De bedoeling is om een beveiligde elektronische mededeling van de nodige vertrouwelijke en medische gegevens tussen de Belgische actoren in de gezondheidszorg mogelijk te maken.

De dienst eHealthBox is beschikbaar als **webservice** (toegankelijk via een medisch softwarepakket) en als **webtoepassing** (toegankelijk via een pc en een eID/itsme of TOTP).

### Welke functionaliteiten biedt de dienst eHealthBox?

De dienst eHealthBox biedt de volgende functionaliteiten:

- als **webtoepassing**, een pakket dat het volgende omvat:
  - een dienst voor de raadpleging van berichten,
  - een dienst voor de publicatie van berichten,
  - de dienst ‘eHealth update info’, een toepassing die toelaat om via een e-mailadres (bv. een webmailadres gekozen door de zorgverlener) verwittigd te worden als er nieuwe berichten binnenkomen in de eHealthBox,
  - een dienst voor de raadpleging van algemene informatie over de capaciteit van de mailbox (huidig volume, maximaal toegelaten volume, aantal niet-ontvangen berichten als de mailbox vol zit ...),
  - een notificatiedienst die een overzicht biedt van de status van de berichten (ontvangen en/of gelezen),
  - de mogelijkheid om de berichten te organiseren en te verplaatsen tussen de verschillende dossiers.
- als **webservice**, eenpublicatiedienst voor het verzenden van berichten, die het volgende omvat:
  - een out-of-officedienst die toelaat te verwijzen naar een vervangende zorgverlener:
    - een functionaliteit voor gegroepeerde mailverzending op basis waarvan een of meerdere berichten naar een groep zorgverleners verzonden kunnen worden (bijvoorbeeld een bericht ter attentie van het verplegend personeel van een ziekenhuis),
    - een versleutelingsdienst om de integriteit van de meegedeelde gegevens te waarborgen,
    - de mogelijkheid om bijlagen te verzenden (het volume van de berichten mag niet groter zijn dan 10 MB),

        - de mogelijkheid om berichten van het type 'news' te verzenden, dat zijn berichten die men ongelimiteerd kan actualiseren.
    - een dienst voor de raadpleging van de berichten die het volgende omvat:
        - een dienst voor de raadpleging van algemene informatie over de capaciteit van de mailbox (huidig volume, maximaal toegelaten volume, aantal niet-ontvangen berichten als de mailbox vol zit ...),
        - een notificatiedienst die een overzicht biedt van de status van de berichten (ontvangen en/of gelezen),
        - een dienst voor de raadpleging van een samenvatting van de berichten (geordend op datum),
        - de mogelijkheid om gelijktijdig verschillende mailboxen te raadplegen (bijvoorbeeld de mailbox van een zorgverlener in zijn hoedanigheid van individuele zorgverlener en zijn mailbox in de hoedanigheid van zorgverlener binnen een ziekenhuis),
        - de mogelijkheid om de berichten te organiseren en te verplaatsen tussen de verschillende dossiers.
    - een dienst genaamd 'eHealth Addressbook' die:
        - toelaat een zorgverlener op te zoeken op basis van:
            - het rijksregisternummer (en optioneel zijn beroep),
            - het RIZIV-nummer (en optioneel zijn beroep)
            - het beroep en de naam (en optioneel zijn voornaam)
            - het beroep en de postcode
            - het beroep en de gemeente
            - het e-mailadres
        - toelaat een zorginstelling op te zoeken op basis van:
            - het EHP-nummer (en optioneel het type instelling),
            - het RIZIV-nummer (en optioneel het type instelling),
            - het KBO-nummer (en optioneel het type instelling),
            - de naam en het type instelling,
            - het type instelling en de postcode,
            - het type instelling en de gemeente,
        - toelaat de meest recente contactgegevens van een zorgverlener of een zorginstelling te raadplegen (opgenomen in de authentieke bronnen):
            - voor een actor in de gezondheidszorg: rijksregisternummer / naam / voornamen / taal / geslacht / geboortedatum / eventuele datum van overlijden / adres / contactgegevens / RIZIV-nummer / beroep / beroepscode / specialisatie / specialisatiecode / professioneel adres / eHealthBox,

- voor een zorginstelling: identificatienummer (met type EHP/CBE/NIHII) van de instelling / beschrijving van de instelling / type instelling / benaming / adressen / andere contactgegevens / eHealthBox,
- de teruggestuurde eHealthBox-gegevens omvatten: identificatienummer van de box en typenummer (INSZ, NIHII, CBE), eventueel het subtype (bijvoorbeeld ziekenhuis), de hoedanigheid van de actor in de gezondheidszorg of de instelling.

## In de praktijk

### Afhankelijkheden, aanbevelingen en waarschuwingen

De dienst eHealthBox werd ontwikkeld voor zorginstellingen en de zorgverleners die over een RIZIV-nummer beschikken.

Om de eHealthBox als **webtoepassing** te gebruiken moet de zorgverlener zich aanmelden via een pc aan de hand van een eID, itsme of een TOTP. Het is ook belangrijk om een webbrowser te gebruiken die getest werd door eHealth-platform. Raadpleeg daarvoor de informatie over toegang tot webtoepassingen op eGezondheid.

Om de eHealthBox als **webservice** te gebruiken dient te zorgverlener te beschikken over een medisch softwarepakket dat deze dienst geïntegreerd heeft (dit is het geval voor alle softwarepakketten die geregistreerd werden door eHealth-platform).

### Wat zijn de voorwaarden voor de integratie van de dienst eHealthBox van het eHealth-platform?

- Neem contact op met Wolf Wauters, de verantwoordelijke projectleider binnen het eHealth-platform, via het e-mailadres Wolf.Wauters@ehealth.fgov.be. Beschrijf de context en de doelstelling van uw project en geef een raming op het vlak van volume.
- Indien akkoord, dient u te beschikken over een eHealth-certificaat en te voorzien in de integratie van een versleutelingsdienst.

Om de integratie van de webservice voor publicatie en raadpleging van de eHealthBox te vergemakkelijken, stelt het eHealth-platform connectoren ter beschikking van de actoren in de gezondheidszorg.

Meer informatie via support@ehealth.fgov.be.

# 9. RR Consult

## Wat is RR Consult?

RR Consult omvat een aantal diensten waarmee de gegevens van een persoon in het Rijksregister en in de Kruispuntbankregisters kunnen worden opgezocht en geraadpleegd.

Deze diensten zijn toegankelijk voor de instellingen en de beroepsbeoefenaars in de gezondheidzorg (erkend in het KB 78), die hiertoe op voorhand werden gemachtigd door het Informatieveiligheidscomité (het vroegere 'sectoraal comité van de sociale zekerheid en de gezondheid').

De machtigingen die in het verleden bij het sectoraal comité van het Rijksregister of bij het sectoraal comité van de sociale zekerheid en van de gezondheid werden verkregen, blijven geldig.

Deze machtigingen worden verkregen naargelang:

- het type instelling en/of de verrichtte prestaties (ziekenhuizen, erkende laboratoria, huisartsen);
- het doeleinde van de aanvraag (bv.: controle en bijwerking van de identificatiegegevens van de patiënten in het medisch dossier, ...);
- het type gegevens waarvoor de toegang wordt gevraagd (naam, geboortedatum, geslacht, verblijfplaats, ...).

De beraadslagingen vindt u terug via het tabblad 'Informatieveiligheidscomité'

## Welke diensten worden door RR Consult aangeboden?

**Belangrijk: elke gebruiker krijgt enkel toegang tot de gegevens waarvoor er op voorhand een juridische machtiging werd verleend.**

**PersonService**

Raadpleging van de identificatiegegevens van een persoon

- op basis van het INSZ of het INSZ BIS;
- op basis van fonetische criteria.

**CBSSPersonService**

Aanmaak door de gemachtigde instanties van een INSZ of een INSZ BISnummer.

**PersonInfoService**

Raadpleging van de historiek van bepaalde gegevens uit het Rijksregister en de KSZ-registers op basis van het INSZ en INSZ BIS van een patiënt.

**InscriptionService**

Beheer door de organisaties/instellingen van de inschrijving van een patiënt op de abonnementendienst van de mutaties. Voor een correct gebruik ervan is het nodig om ook de toepassing PersonNotificationService te implementeren.

**PersonNotificationService**

Beheer (ophalen en verwijderen) van de mutaties door een gemachtigde instantie (oude benaming: MutationSender).

**SSINHistory**

Oproepen van de lijst van de unieke identificatienummers (INSZ/INSZ BIS) die een persoon heeft (gehad). Deze dienst wordt gebruikt in het kader van de aanmaak van een INSZ of een INSZ/BIS.

### Wie heeft toegang tot RR Consult?

**De volgende instellingen werden al gemachtigd om krachtens algemene beraadslagingen deze diensten te gebruiken:**

- Ziekenhuizen;
- Erkende laboratoria voor klinische biologie;
- Erkende laboratoria voor pathologische anatomie;
- Erkende rust- en verzorgingstehuizen;
- Psychiatrische verzorgingstehuizen of initiatieven voor beschut wonen.

**Beroepsbeoefenaars in de gezondheidszorg (KB78):**

De beroepsbeoefenaars in de gezondheidszorg werden op juridisch vlak gemachtigd om het rijksregisternummer te gebruiken in het kader van de toepassingen die een beroep doen op de basisdiensten van het eHealth-platform en om hiertoe het rijksregisternummer van de patiënt in het dossier van de patiënt op te slaan. Deze mogelijkheid wordt in een eerste fase aan de huisartsen aangeboden.

**Andere instanties:**

Andere instanties die een dossier hebben ingediend waarin ze het doeleinde en de evenredigheid rechtvaardigen, hebben eveneens een specifieke machtiging gekregen.

**Voor bijkomende inlichtingen of om de stappen te kennen voor het verkrijgen van elke nieuwe beraadslaging verzoeken wij u om contact op te nemen met het eHealth-platform:** RRNConsult@ehealth.fgov.be

### Hoe toegang krijgen tot RR Consult?

Om de diensten eHealth RR Consult te kunnen gebruiken, moet de instelling of de zorgverlener beschikken een eHealth-certificaat en over een medisch softwarepakket waarin deze dienst is geïntegreerd.

**Procedure voor een ziekenhuis, een erkend laboratorium, een psychiatrisch verzorgingstehuis, een initiatief voor beschut wonen, een rust - of een verzorgingstehuis.**

Zie de formulieren onderaan op de pagina.

*Stap 1*: De instanties, die de webservice in een van hun toepassingen wensen te integreren, moeten eerst (bij voorkeur via mail) **alle** hierna vermelde documenten overmaken aan:

**Informatieveiligheidscomité, kamer sociale zekerheid en gezondheid**

Mevrouw Joke Vanderpoorten

Willebroekkaai 38 te 1000 Brussel

ivc@mail.fgov.be

1. een verbintenis waarbij de instelling verklaart de voorwaarden uit de beraadslaging na te leven. U moet het gepast formulier kiezen naargelang het type van de instelling:
    - ziekenhuis;
    - erkende laboratoria voor klinische biologie;
    - erkende laboratoria voor pathologische anatomie;
    - psychiatrisch verzorgingstehuis of initiatief voor beschut wonen;
    - rusthuis of verzorgingstehuis.
2. een akte tot erkenning van uw instelling (bewijs van het statuut of van de erkenning);
3. een evaluatieformulier van de DPO van uw instelling;
4. een conformiteitsverklaringsformulier betreffende de referentieveiligheidsmaatregelen;

5. een aanvraag om de webservices eHealth te mogen gebruiken.

*Stap 2*: Het Informatieveiligheidscomité, kamer sociale zekerheid en gezondheid, zal u zijn beslissing meedelen en u bij akkoord een acceptatie Application ID toekennen. Het zal tegelijkertijd het Rijksregister op de hoogte brengen.

*Stap 3*: U kan vervolgens het technische gedeelte opstarten en aansluitend een testrapport sturen naar integration-support@ehealth.fgov.be. Alle informatie hierover vindt u in de cookbooks op deze pagina.

*Stap 4*: Na de validatie van het testrapport doet het eHealth-platform het nodige om uw toegangen in productie te configureren. U ontvangt een productie Application ID dat u toegang geeft tot de productie-omgeving.

**Bijzondere procedure “Circle of trust” (CoT)**

Zie de formulieren en de informatieve documenten onderaan op de pagina.

Voor de erkende laboratoria voor klinische biologie en de ziekenhuizen die het formulier 'Circle of trust' CoT hebben ingevuld:

1. de CoT-verklaring invullen en terugsturen naar hun voogdij-instantie (zie ook de toelichting bij deze verklaring op eer);
2. het verzoek om toestemming voor gebruik van de webservices eHealth RR Consult voor de toekenning van BIS-nummers opmaken;
3. de minimale veiligheidsnormen naleven;
4. de regels inzake goede businesspraktijken die door de COT-laboratoria of COT-ziekenhuizen moeten worden geïmplementeerd, naleven;
5. testgevallen aanvragen bij het supportteam (integration-support@ehealth.fgov.be) en hen het testrapport sturen.

Na de goedkeuring van het testrapport krijgt u een Application ID voor de toegang in productie.

In het kader van de gezondheidscrisis kunnen de erkende laboratoria voor klinische biologie en de ziekenhuizen die reeds op de dienst RR Consult zijn aangesloten, eveneens een beroep doen op de webservice waarmee, onder bepaalde voorwaarden, INSZ/BIS nummers kunnen worden aangemaakt.

**Uw instelling behoort niet tot de categorieën hiervoor vermeld:**

In dat geval nodigen we u uit om contact op te nemen met het eHealth-platform ( RRNConsult@ehealth.fgov.be) om de context van het project, de wettelijke basis, het doeleinde en een raming van het volume voor te leggen.

We zullen uw aanvraag analyseren en nagaan of er een juridische machtiging bestaat op het niveau van enerzijds het rijksregister en anderzijds de KSZ-registers.

Zodra deze machtigingen verkregen zijn, dient u het aanvraagformulier voor het gebruik van de webservices in te dienen.

Aansluitend ontvangt u een 'acceptatie application ID' waarmee u het technische gedeelte kan aanvatten. Na de validatie van uw testrapport doet het eHealth-platform het nodige om uw toegangen in productie te configureren.

**Opmerking**: Indien de DPO van uw instelling (nog) niet gekend is bij het eHealth-platform, dient het evaluatieformulier van uw DPO te worden verstuurd.

**Aandachtspunten**

- Indien uw organisatie evolueert op juridisch of organisatorisch vlak (fusie, intrekking erkenning, ...) of wanneer er een andere DPO wordt aangesteld, wordt u verzocht contact op te nemen met het eHealth-platform. Deze evolutie kan immers zowel op juridisch als administratief vlak een impact hebben voor wat betreft de toegang tot de diensten van het eHealth-platform via de eHealth-certificaten.
- Voor de artsen: in het kader van de continuïteit van de medische zorgverlening kunnen de artsen met een actief visum die niet over een softwarepakket beschikken gebruikmaken van de webtoepassing eHealthCreaBis om BIS-nummers aan te maken.
- Voor alle vragen m.b.t. het gebruik van de dienst RR Consult kan u ons contacteren via het e-mailadres RRNConsult@ehealth.fgov.be.

# 10. I.AM (Identity & Access Management)

### Wat is de dienst ‘Geïntegreerd gebruikers- en toegangsbeheer’/I.AM (Identity & Access Management)?

De dienst geïntegreerd gebruikers- en toegangsbeheer van het eHealth-platform heeft als doel om de identificatie, de authenticatie en de machtiging van actoren in de gezondheidszorg te vergemakkelijken.

Deze dienst is samengesteld uit verschillende componenten die samenwerken om de (unieke) authenticatie, de machtiging en de identiteitsverspreiding van de gebruikers van de gezondheidszorg mogelijk te maken die toegang vragen tot de diensten (gehost bij de gezondheidszorginstanties en het eHealth-platform).

Deze componenten zijn conform de internationale normen voor de mededelingen tussen bedrijven teneinde de veiligheid en de stabiliteit te garanderen en de integratie te vergemakkelijken.

## Welke functionaliteiten worden door de dienst I.AM aangeboden?

De dienst geïntegreerd gebruikers- en toegangsbeheer biedt de volgende functionaliteiten:

- Authenticatie van de gebruiker
  - via het eHealth-certificaat
  - via een numerieke sleutel die door het eHealth-platform wordt ondersteund
- Identificatie van de gebruiker, keuze van zijn profiel volgens
  - zijn hoedanigheid / het type individuele zorgverlener (op basis van de informatie vervat in de gegevensbank Cobrha)
  - zijn organisatie in naam waarvan hij kan optreden
  - het mandaat waarvoor hij kan optreden
  - zijn kind(eren) (op basis van de gegevens aanwezig in het Rijksregister)
- Unieke authenticatie (single sign-on)
  - in het kader van een webtoepassing moet de gebruiker zich niet opnieuw authenticeren (behalve wanneer dit uitdrukkelijk wordt gevraagd voor een toepassing)
  - in het kader van een webservice maakt de gebruiker een sessie aan die in het kader van verschillende diensten voor een bepaalde duur wordt gebruikt (de duur hangt af van het profiel van de gebruiker)

  Opmerking : de single-sign-on IDP mag niet worden verward met een houding ‘isPassive’ waarin de schermen van de IDP die aan de gebruiker worden getoond, tot het strikte minimum worden beperkt. De isPassive is enkel geldig tussen de webtoepassingen die deze functionaliteit ondersteunen. Hierdoor kan de gebruiker onder meer een profiel selecteren in een toepassing en moet hij niet opnieuw een profiel selecteren wanneer hij overgaat naar een 2de toepassing (die dat profiel ondersteunt) die door onze I.AM IDP wordt beveiligd.

- Delegatie van toegangen tot de toepassingen
  - binnen een instelling
    - het is mogelijk om de gebruikers te bepalen die in naam van een instelling kunnen optreden voor bepaalde beschikbare toepassingen
      - de delegatie gebeurt via de UserManagement
    - bijkomend aan deze toewijzingen aan de gebruikers is het mogelijk om functies te bepalen binnen deze instelling
      - de delegatie gebeurt via de UserManagement en Remaph
      - deze functionaliteit kan in principe niet worden gebruikt in het kader van de webservices > indien deze functionaliteit wordt gebruikt, moet het project vragen om IDP te gebruiken

        - indien een persoon die in de instelling werkt in naam van een andere gebruiker van die instelling mag optreden, kan een hiërarchische relatie tussen die 2 personen worden bepaald
            - de delegatie gebeurt via UserManagement en Remaph
            - deze functionaliteit kan in principe niet worden gebruikt in het kader van de webservices > indien deze functionaliteit wordt gebruikt, moet het project vragen om IDP en AttributeAuthority te gebruiken (waardoor onze partners de authentieke bronnen eHealth kunnen ondervragen)
            - dit systeem werd uitgewerkt om een onderscheid te maken tussen de toegangen tot de toepassingen en de toegangen tot de gegevens.
            - de toepassing is verantwoordelijk voor het weergeven aan de ondergeschikte van de lijst met zijn hiërarchische oversten nadat deze ondergeschikte de toegang tot deze toepassing (vanuit onze IDP) heeft gekregen
    - van een instelling naar een andere instelling
        - de delegatie gebeurt via de webtoepassing Mandaten
            - indien de mandaattypes die in de toepassing beschikbaar zijn niet aan de verwachtingen van de toepassing voldoen, moet de aanmaak van een nieuw type mandaat worden aangevraagd via de verantwoordelijke projectleider binnen eHealth
    - van een natuurlijke persoon naar een andere natuurlijke persoon
        - de delegatie gebeurt via de webtoepassing Mandaten
- Toegang tot de gegevens
    - via de webservice I.AM AA (AttributeAuthority, waardoor onze partners de authentieke bronnen eHealth kunnen ondervragen) kan toegang worden verleend tot bepaalde gegevens (contactadres van een zorgverlener, benaming van een instelling, lijst met hiërarchische verantwoordelijken van een ondergeschikte binnen een instelling, ...) in onze authentieke bronnen (waaronder CoBRHA)
    - de toegang tot deze gegevens is beveiligd
- Beveiliging van de toepassing door middel van een machtigingsmechanisme gebaseerd op de identiteit van de gebruiker

## In de praktijk

### Afhankelijkheden, aanbevelingen en waarschuwingen

De integratie van deze basisdienst houdt nauw verband met de architecturen die door het eHealth-platform worden aangeboden.

In het kader van de ontwikkeling van een webtoepassing (server side) raden wij u aan om de software Shibboleth SP te gebruiken om de integratie van uw toepassing met onze I.AM IDP te vergemakkelijken.

Indien uw systeem de toegang tot bepaalde REST-diensten ( Representational State Transfert) van het eHealth-platform vereist, zal er een integratie met onze I.AM Connect moeten plaatsvinden.

Indien uw toepassing onze token eXchange moet kunnen gebruiken, moeten bepaalde regels worden nageleefd en moet een contract worden ondertekend.

Om de I.AM STS en I.AM AA te kunnen gebruiken is de eID van de actor in de gezondheidszorg of een certificaat afgeleverd door het eHealth-platform vereist.

I.AM mag enkel worden gebruikt voor de gezondheidsactoren die door het eHealth-platform zijn erkend

**Wat zijn de voorwaarden voor de integratie van de dienst I.AM van het eHealth-platform?**

- Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform eHealthppkb@ehealth.fgov.be en beschrijf de context en de finaliteit van uw project en geef een raming op het vlak van volume
- Na afloop en indien akkoord, de nodige documenten voor de configuratie van de gewenste diensten meedelen
    - CAB-I.AM / eDU in te vullen in overleg met uw verantwoordelijke projectleider binnen het eHealth-platform
    - om de functionaliteit van toegang tot de gegevens te gebruiken
        - een eHealth-certificaat verkrijgen per gewenste omgeving
        - het I.AM registration-formulier per omgeving invullen en voorleggen en daarbij het verkregen certificaat vermelden
    - om I.AM Connect te gebruiken
        - het juiste registratieformulier gebruiken afhankelijk van de realm: Healthcare of M2M
    - om de I.AM IDP te gebruiken
        - het I.AM Registration-formulier invullen per omgeving en voorleggen met vermelding van het gekregen certificaat

Om de integratie van de oproep van de STS-webservice te vergemakkelijken, stelt het eHealth-platform ‘connectoren' ter beschikking van de actoren in de gezondheidszorg.

Meer informatie: support@ehealth.fgov.be

# Identity & Access management - Technische organisatie

## Inleiding

Het I.AM-systeem (Identity & Access Management) van het eHealth-platform integreert alle basisdiensten waarvan de functionaliteiten het toegangsbeheer, het gebruikersbeheer en het beheer van de toegang tot de gegevens toelaten.

Naargelang de behoeften van de toepassing, onderscheiden we 4 contexten:

1. De beveiliging van Web App
2. De beveiliging van ‘Simple Object Access Protocol’ (SOAP) Web Service
3. De beveiliging van ‘Representational State Transfert’ (REST) Web Service
4. De Data Access

De authenticatie en de autorisatie zijn belangrijke aspecten van elk van deze contexten.

## De beveiliging van Web App

Om toegang te krijgen tot een toepassing van het type beveiligde Web App, dient men zich te authenticeren en een autorisatie te verkrijgen

- voor de klassieke webapplicaties (typisch voor server-side HTML-applicaties), via het component ‘I.AM IDP’
- voor de mobiele webapplicaties (applicaties die gebruik maken van JavaScript voor het oproepen van REST-diensten bijvoorbeeld) of native applicaties, via het component ‘I.AM Connect’.

In al deze gevallen biedt het systeem de mogelijkheid van ‘single sign-on’ aan de gebruiker, zodat die zich slechts één keer moet identificeren om toegang te krijgen tot verschillende applicaties.

In het geval van klassieke Web Apps gebeurt het beheer van de autorisaties door onze IDP (Identity Provider) (via het User & Access Management - UAM).

In het geval van mobiele Web Apps gebeurt het beheer van de autorisaties door de verschillende opgeroepen diensten.

Nuttige documentatie voor de klassieke Web Apps:

- I.AM overview
- I.AM federation metadata
- I.AM IDP
- I.AM federation attributes

- I.AM logout
- I.AM SP Shibboleth
- I.AM SP Shibboleth upgrade
- I.AM registration
- Geïntegreerd gebruikers en toegangsbeheer - SLA
- UAM

Nuttige documentatie voor ‘mobiele’ Web Apps of native applicaties:

- I.AM Connect - Mobile integration - Technical specifications

### De beveiliging van SOAP Web Service

SOAP (Simple Object Access Protocol) is een objectgeoriënteerd protocol dat de uitwisseling van gestructureerde berichten toelaat (XML-formaat in een SOAP-enveloppe) tussen een WSC (Web Service Consumer) en een WSP (Web Service Provider).

Dit protocol wordt onder meer gebruikt in het kader van SOA-architecturen (Service Oriented Architecture).

De authenticatie van de WSC gebeurt via de dienst I.AM STS (Secure Token Service) aan de hand van een eHealth-certificaat of een elektronische identiteitskaart (eID). De assertion die wordt verkregen door de WSC wordt vervolgens geëvalueerd in het kader van de autorisatie.

De autorisatie wordt, voor elke opgeroepen dienst, hoofdzakelijk verricht door de Service Bus van het eHealth-platform op basis van voorgedefinieerde regels. Voor elke beveiligde SOAP service die beschikbaar is op de ESB van het eHealth-platform worden de gedefinieerde toegangsregels geëvalueerd teneinde al dan niet toegang te verlenen tot de dienst.

Het is voor een gebruiker ook mogelijk over te schakelen van authenticatie/autorisatie van het type Web service naar authenticatie/autorisatie van het type web App, via de ‘I.AM STS to IDP’.

Nuttige documentatie:

- eHealthcertificaat
- I.AM STS
- Coördinatie van processen
- Beveiliging van webservices

### De beveiliging van REST Web Service

De REST-webservices (Representational State Transfert) worden gebruikt in het kader van de REST-architectuur. Deze architectuur is gebaseerd op het HTTP-protocol via de verschillende acties: GET, POST, PUT, DELETE.

Het formaat van de uitgewisselde berichten is niet XML maar JSON.

Dit type diensten is hoofdzakelijk bedoeld voor mobiele applicaties.

De authenticatie en autorisatie van de klanten gebeurt via de dienst ‘I.AM Connect’ die gebaseerd is op de standaard OIDC (OpenID Connect).

‘I.AM Connect’ laat onder mee toe om een ‘Access token’ uit te reiken aan de klant die deze token vervolgens naar de REST-dienst kan sturen.

De REST-dienst controleert vervolgens de inhoud van de ‘Access token’ i.v.m. opgelegde veiligheidsvereisten.

Nuttige documentatie:

- I.AM Connect - Mobile integration - Technical specifications

### De Data Access

Dit systeem doet een beroep op de component ‘I.AM AA’ waarvan de functie erin bestaat verschillende gegevensbronnen te raadplegen om na te gaan of de vastgestelde voorwaarden voor de toegang tot de gegevens vervuld zijn en, in voorkomend geval, al dan niet toegang te verlenen.

### I.AM AA (AttributeAuthority)

I.AM AA laat onze partners toe om de authentieke eHealth-bronnen te raadplegen. Deze bronnen bevatten informatie over de gezondheidszorgactoren (CoBrHA), de mandaten, ....

Dit systeem werd ontworpen om de toegang tot de toepassingen te scheiden van de toegang tot de gegevens.

### I.AM STS (Secure Token Service)

I.AM STS laat een gezondheidszorgactor toe om zich te identificeren via het genereren van een token (in tegenstelling tot de identificatie via eID of username). Dit systeem is bedoeld voor de identificatie voor webservices die geïntegreerd zijn in de softwarepakketten van de artsen en laat toe om zich te identificeren als arts, specialist, verpleegkundige, ...

### I.AM IDP (IDentity Provider)

I.AM IDP is de dienst die toelaat om de identiteitsinformatie te creëren, te onderhouden en beheren voor de gebruikers die zich kunnen authenticeren in een gedistribueerd netwerk of een federatie.

IDP ondersteunt verschillende authenticatiemethoden zodat de gebruiker kan bewijzen dat hij wel degelijk degene is die hij beweert te zijn.

I.AM IDP laat toe de toegang tot de webapplicaties te beveiligen die aangeboden en gehost worden door de Service Providers via UAM.

### I.AM Connect

I.AM Connect is een oplossing voor het beheer van de identiteit en de toegang voor webapplicaties en RESTful-webservices gebaseerd op OIDC (OpenID Connect).

Het laat de klanten toe om informatie te vragen en te verkrijgen over de geauthenticeerde sessies en de eindgebruikers. I.AM Connect laat de klanten ook toe om de identiteit van de eindgebruiker te controleren op basis van de authenticatie die verricht werd door onze autorisatieserver.

Het gaat daarbij om diverse soorten klanten: klanten van webapplicaties, JavaScript-klanten, native applicaties (‘mobiele’ klanten).

Nuttige documentatie:

- I.AM Connect - Mobile integration - Technical specifications

### UAM

UAM = User & Access Management

Het UAM wordt gebruikt in het kader van klassieke Web Apps en webservices via de Service Bus van het eHealth-platform en laat toe om een gebruiker al dan niet toegang te verlenen tot een beveiligde resource.

Het UAM is gebaseerd op het generieke Policy Enforcement Model, dat een Policy Enforcement Point (PEP), een Policy Decision Point (PDP), een Policy Administration Point (PAP) en een Policy Information Points (PIP) omvat.

Informatie over UAM.

# Architectuur

In het kader van de ontwikkeling en het onderhoud van zijn projecten en diensten biedt het eHealth-platform diverse structuren en organisaties van de informaticasystemen of “architecturen” aan.

## 1. Architecturen

## 1. Inleiding

In het kader van de ontwikkeling en het onderhoud van zijn projecten en diensten biedt het eHealth-platform diverse structuren en organisaties van de informaticasystemen of 'architecturen' aan.

Die modellen zijn gebaseerd op de behoeften van de partners, maar beantwoorden ook aan bepaalde kwaliteits- en veiligheidsnormen. Ze evolueren continu in rechtstreekse relatie met de sector.

Bij het opstarten van een project is het dus belangrijk om de verschillende aangeboden systemen goed te begrijpen met het oog op een optimale implementatie van de diverse componenten, maar ook om te anticiperen op mogelijke toekomstige evoluties.

Het eHealth-platform biedt voornamelijk 2 types architectuur aan:

- een architectuur van het type SOAP (Simple Object Access Protocol ) , bestemd voor toepassingen en diensten die bedoeld zijn om te functioneren op één enkel toestel, één enkele computer.
- een architectuur van het type REST (Representational State Transfer) bestemd voor toepassingen en diensten die bedoeld zijn om te functioneren op verschillende toestellen (gelijktijdig op een computer, smartphone, tablet, ...).

Zoals reeds aangestipt, is informatica een domein dat constant evolueert. Bij het opstarten van het eHealth-platform stond het gebruik van mobiele apparaten zoals tablets en smartphones nog in zijn kinderschoenen. Daarom werd dan ook voornamelijk de architectuur van het type SOAP ontwikkeld en bepaalt dat type architectuur ook vandaag nog een groot aantal systemen dat in samenwerking met onze partners geïmplementeerd werd. Het onderhoud en de ondersteuning van dat model blijft ook nu een van onze opdrachten en verantwoordelijkheden, maar voor de ontwikkeling van projecten voor mobiele apparaten is het gebruik ervan niet aanbevolen (laat bv. geen versleuteling van berichten toe) en wordt prioriteit gegeven aan een architectuur van het type REST.

# 2. Ontwikkeling van een project in het kader van de online gezondheid: wat men dient te voorzien, te begrijpen en te definiëren

## 2.1. Het project dient te beantwoorden aan voorwaarden inzake identificatie en toegangsbeheer

Om de mobiele toegang tot de eHealth-diensten mogelijk te maken, dienen we ALLE gebruikers die behoefte hebben aan de diensten van het eHealth-platform te kunnen authenticeren, ongeacht het toestel of het systeem dat gebruikt wordt voor de connectie.

We onderscheiden twee categorieën gebruikers van onze diensten:

- personen (Belgische of buitenlandse burgers, professionals, leden van een organisatie, lasthebbers);
- systemen.

Voor elk van hen moet het mogelijk zijn om een digitale identiteit te construeren.

### 2.1.1. Registratie

Alle gebruikers moeten geregistreerd zijn in een authentieke bron die toegankelijk is voor het eHealth-platform (rechtstreeks of onrechtstreeks).

- de personen aanwezig in het rijksregister met een INSZ (Belgen) of een INSZ bis (vreemdelingen) (tot de doelgroep van het eHealth-platform behoren zowel Belgische burgers als vreemdelingen die in België of in het buitenland wonen).
- de systemen moeten behoren tot een organisatie die eenduidig geïdentificeerd kan worden in een authentieke bron voor het specifieke type organisatie.

Elke gebruiker moet zijn identiteit online kunnen bewijzen met een digitale sleutel. Bij de registratie dient hem minstens één sleutel te worden meegedeeld.

### 2.1.2. Authenticatie

De authenticatie moet worden ondersteund voor alle types van klanten: web (browser), native (mobiele toepassing), desktop, server (backend, batch).

Voor de authenticatie moet de gebruiker een van zijn digitale sleutels gebruiken om te bewijzen dat hij wel degelijk degene is die hij beweert te zijn. Het gefedereerde identiteitsmodel van het eHealth-platform moet herbruikbaar zijn voor alle gebruikers.

Alle digitale sleutels moeten beantwoorden aan minimale veiligheidsvereisten.

Een persoon moet verschillende toestellen kunnen gebruiken voor de authenticatie ten aanzien van onze diensten.

Een persoon moet een toepasselijk gebruikersprofiel (bv. burger, hoedanigheid, lid van een organisatie, mandaat) kunnen kiezen dat gebruikt zal worden voor de authenticatie ten aanzien van onze diensten.

Het moet mogelijk zijn om de gekozen identiteit door te geven aan de gevraagde resources of deze laatste moeten de identiteit kunnen ophalen.

#### 2.1.3 Autorisatie

De autorisaties moeten gebaseerd zijn op de gekozen digitale identiteit voor elk van de gevraagde resources.

Het moet mogelijk zijn de autorisaties te propageren naar de gevraagde resources of deze laatste moeten ze kunnen ophalen.

De gebruiker moet kunnen beslissen of hij al dan niet autorisaties wenst te geven aan de klant-toepassing die deze autorisaties in zijn naam zal gebruiken.

De gebruikers moeten de toegekende autorisaties kunnen herroepen.

### 2.2. Het project dient te beantwoorden aan voorwaarden inzake informatieveiligheid

#### 2.2.1. Vertrouwelijkheid

Elke communicatie tussen de klant en de server moet als vertrouwelijk worden beschouwd en moet worden beveiligd tegen elke mogelijke onderschepping, tenminste als de communicatie over een niet-beveiligd kanaal zoals het internet verloopt.

De medische gegevens moeten worden beveiligd op het niveau van het bericht om de verspreiding van de gegevens te vermijden wanneer ze van één punt naar een ander op het netwerk circuleren. Ook al is end-to-endversleuteling tussen de oorspronkelijke verzender en de eindbestemmeling niet noodzakelijk, de communicatie moet minstens point-to-point geconfigureerd zijn tussen beide partijen zodat medische gegevens nooit onbeveiligd uitgewisseld worden tussen beide partijen. De vraag of point-to-point volstaat dient per project te worden bepaald.

De gebruikers moeten berichten kunnen ondertekenen en versleutelen op verschillende apparaten (laptop, smartphone of tablet) zonder de digitale sleutels tussen deze apparaten te moeten overdragen en blootstellen.

**Integriteit**

Wanneer medische gegevens verstuurd worden van de klant naar de server, dienen ze ondertekend te zijn op het niveau van het bericht om de integriteit van de inhoud te garanderen.

**Het project dient de communicatiestandaarden vast te stellen uit de voorgestelde lijst**

**Identificatie & Toegangsbeheer**

Dit is de lijst van voorgestelde talen/protocollen:

- SAML 2.0
- Oauth 2.0
- OIDC 1.0
- JWT
- Signed JWT Assertion
- PKCE

**Informatieveiligheid**

Dit is de lijst van voorgestelde talen/protocollen:

- TLS
- JWS
- JWE
- JWK
- WebAuthn

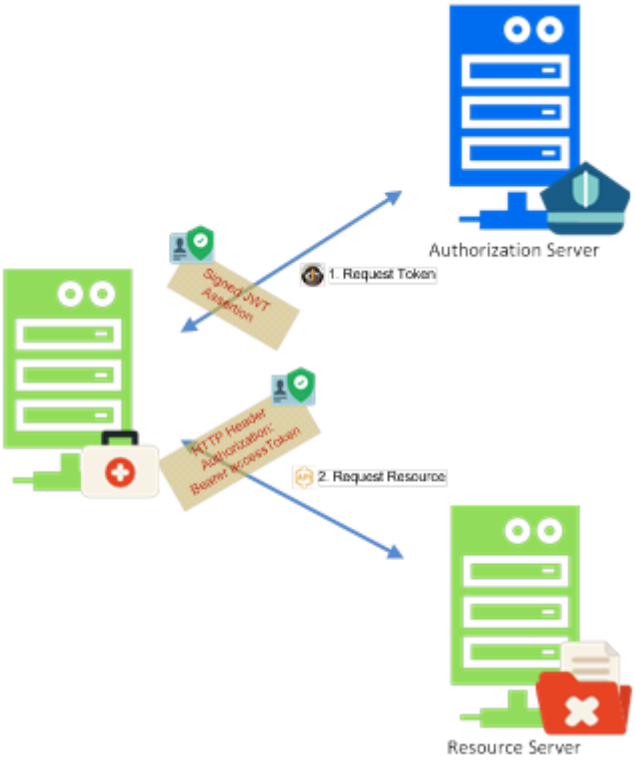
## 2.4. Het project moet één of meerdere types van stromen definiëren uit de voorgestelde lijst

### 2.4.1. Voor het deel 'Identity & Access Management' dient een onderscheid te worden gemaakt tussen:

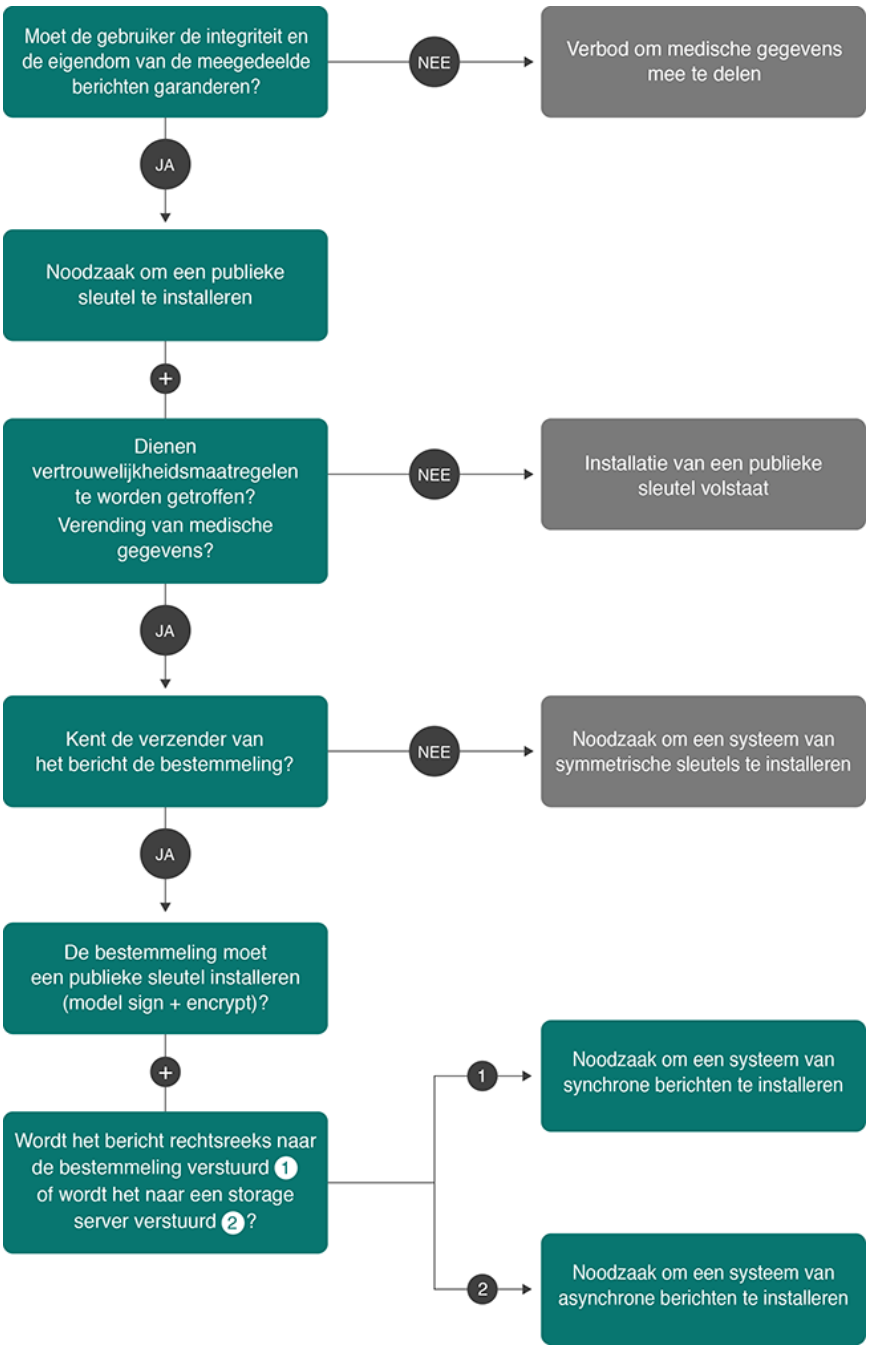
#### 2.4.1.1. een toepassing die bestemd is om te functioneren op het mobiele toestel van de gebruiker (native app/public client)

### 2.4.1.2. een server-based toepassing, die gehost wordt door een partner en opgeroepen wordt door de gebruiker voor gebruik op zijn mobiel toestel (confidential client)

### 2.4.1.3. een toepassing die geen menselijke tussenkomst vereist en die bedoeld is om automatisch te functioneren van server tot server, voor de automatische update van gegevensbanken bijvoorbeeld (system client)

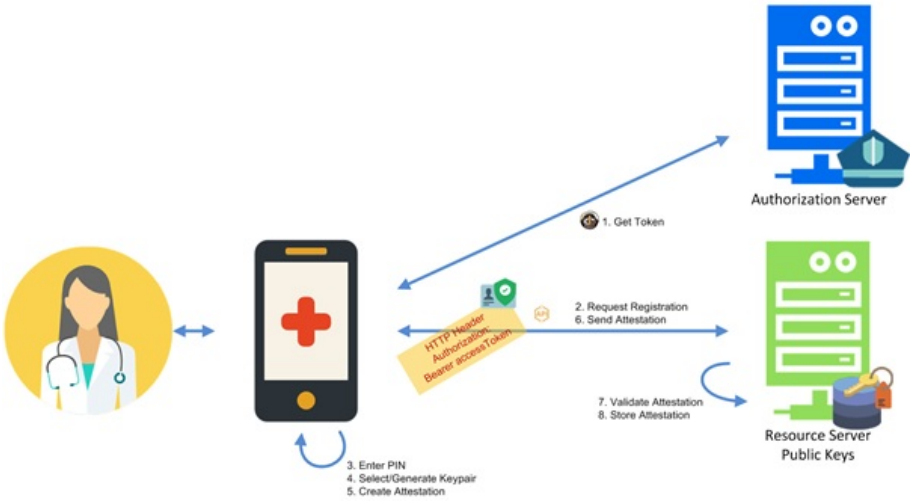


### 2.4.2. Wat betreft het deel 'informatieveiligheid', dient men na te denken over de volgende aspecten:

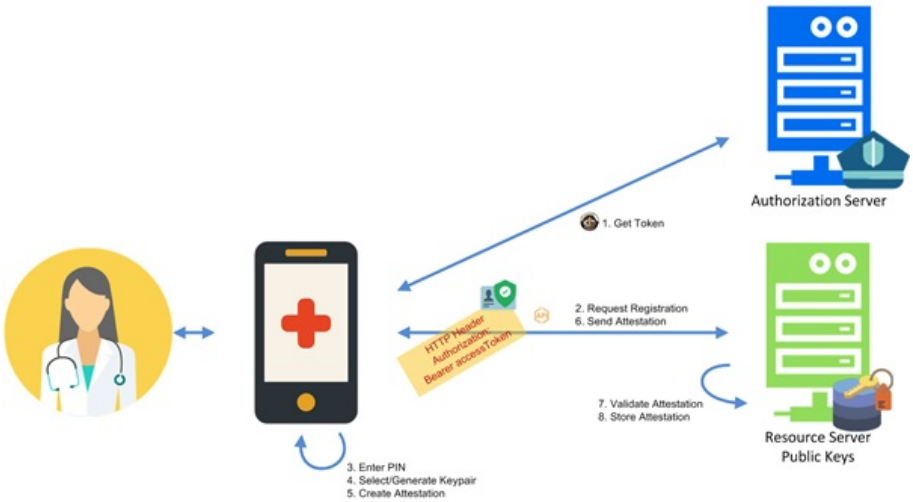


## 3. Schematische voorstelling use cases

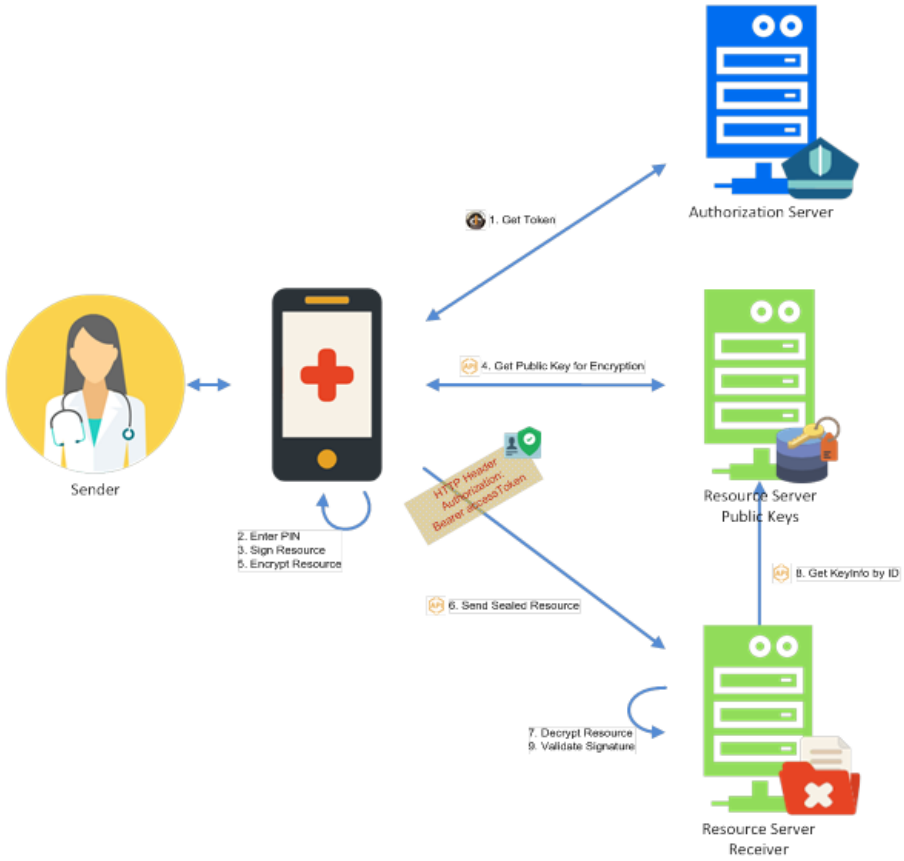
### 3.1. Registratie van een publieke sleutel (use case: registratie van een sleutel in het kader van de aanvraag van een eHealth-certificaat binnen een architectuur van het type SOAP)



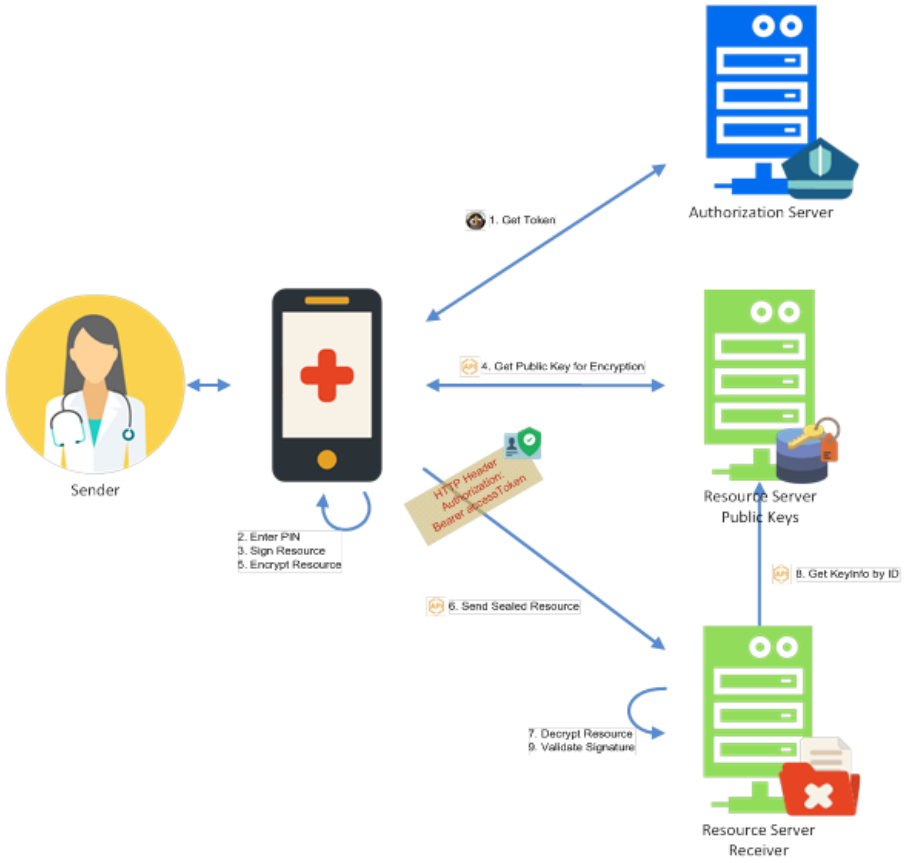

### 3.2. Registratie van een symmetrische sleutel (use case: registratie van een sleutel in het kader van Recip-e)



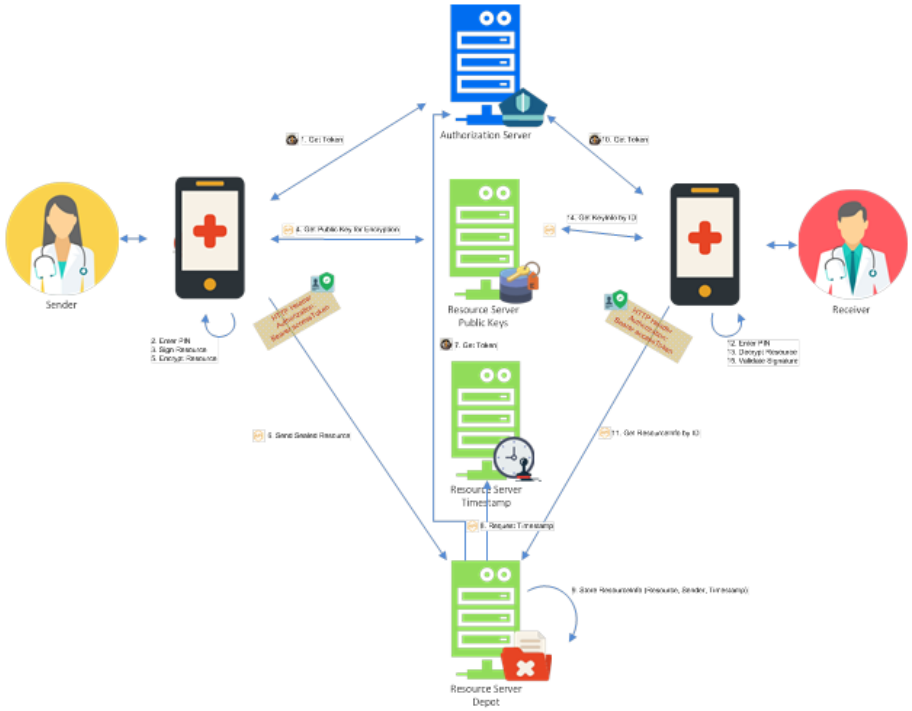
### 3.3. Gekende bestemmeling, synchrone mededeling (meest voorkomende use case: wanneer een klant rechtstreeks een dienst van het eHealth-platform moet contacteren die het versleutelingssysteem vereist)



### 3.4. Gekende bestemmeling, asynchrone mededeling (use case: eHealthBox)



### 3.5. Onbekende bestemmeling (use case: Recip-e)




# Application LiveCycle

## 1. Releases Management

De tabel hieronder bevat de data van de volgende releases, alsook de begindata voor de testen in acceptatie.

Volgende releases

| Naam Release | Type release | Content freeze | Code freeze | In ACC op AZ UP | In ACC op AZ IN en start testen | In PRD op AZ UP | In PRD op AZ IN |
|---|---|---|---|---|---|---|---|
| R2023.2.2 | Minor | 24/11/2023 | 04/01/2024 | 16/01/2024 | 23/01/2024 | 13/02/2024 | 20/02/2024 |
| R2024.1 | Major | 16/11/2023 | 05/02/2024 | 27/02/2024 | 19/03/2024 | 07/05/2024 | 12/05/2024 |
| R2024.1.1 | Minor | 04/04/2024 | 09/05/2024 | 21/05/2024 | 28/05/2024 | 11/06/2024 | 18/06/2024 |
| R2024.1.2 | Minor | 02/05/2024 | 06/06/2024 | 25/06/2024 | 02/07/2024 | 16/07/2024 | 23/07/2024 |
| R2024.2 | Major | 23/05/2024 | 08/07/2024 | 30/07/2024 | 20/08/2024 | 08/10/2024 | 13/10/2024 |
| R2024.2.1 | Minor | 05/09/2024 | 10/10/2024 | 22/10/2024 | 29/10/2024 | 26/11/2024 | 03/12/2024 |
| R2024.2.2 | Minor | 22/11/2024 | 02/01/2025 | 14/01/2025 | 21/01/2025 | 11/02/2025 | 18/02/2025 |
| R2025.1 | Major | 14/11/2024 | 04/02/2025 | 25/02/2025 | 18/03/2025 | 06/05/2025 | 11/05/2025 |
| R2025.1.1 | Minor | 03/04/2025 | 08/05/2025 | 20/05/2025 | 27/05/2025 | 10/06/2025 | 17/06/2025 |
| R2025.1.2 | Minor | 30/04/2025 | 05/06/2025 | 24/06/2025 | 01/07/2025 | 15/07/2025 | 22/07/2025 |
| R2025.2 | Major | 22/05/2025 | 08/07/2025 | 29/07/2025 | 19/08/2025 | 07/10/2025 | 12/10/2025 |
| R2025.2.1 | Minor | 04/09/2025 | 09/10/2025 | 21/10/2025 | 28/10/2025 | 25/11/2025 | 02/12/2025 |

De benaming van een release beantwoordt telkens aan de volgende logica: R.2023 **x.y,** waarbij **x** de ‘Major Release’ (MR) aanduidt en **y** de ‘minor Release’ (mR). Bijvoorbeeld: R.2023.1.2 is de tweede ‘minor Release’ volgend op de eerste ‘Major Release’ van het jaar 2023.

Een MR wordt één jaar op voorhand ingepland. Hieronder vindt u de voornaamste fasen van het proces met X als datum van de Major Release.

Fasen van het proces met X

| Timing | Fasen |
|---|---|
| X - 1 jaar: | Een jaar vóór de release wordt er beslist over de inhoud van de wijzigingen in de nieuwe release ten opzichte van de vorige; |
| X - 6 maanden: | 'content freeze': er wordt niets meer veranderd aan de wijzigingen die zullen gebeuren t.o.v. de vorige release; |
| X - 3 maanden: | 'code freeze': er wordt geen enkele wijziging meer aangebracht aan de code van de major release en de cookbooks worden gepubliceerd; |
| X - 5 weken: | start van de testen van de major release in de acceptatie-omgeving; |
| X - 2 weken: | 'acceptation freeze'; |
| X - 1 week: | evaluatie van de nieuwe versie, m.a.w. Go/noGo; |
| X | inproductiestelling. |

Sinds juni 2021 bestaat onze nieuwe infrastructuur uit twee AZ's ('availability zones'). Het verkeer wordt standaard voor 95 % over 'AZ IN' geleid en voor 5 % over 'AZ UP'.

Elke nieuwe inproductiestelling gebeurt in 'canary release'-modus (*). In de kalender hieronder staan telkens twee data per omgeving (AZ UP en AZ IN). Deze data stemmen overeen met de inacceptatiestelling en inproductiestelling van de release.

**(*) Toelichting 'canary release'-modus**

Onze nieuwe infrastructuur bestaat uit twee AZ's ('availability zones') waarbij we de nieuwe releaseversie op een van beide AZ's (standaard is dit AZ UP) plaatsen om vervolgens het verkeer geleidelijk aan door te laten op die AZ (UP) met de nieuwe release zodat de andere AZ (IN) geüpdatet kan worden met de nieuwe release.

### Modaliteiten voor de inproductiestelling van een minor release (*)

Inproductiestelling minor release

| Timing | Fasen |
|---|---|
| J1 Vrijdag (vóór de inproductiestelling op AZ UP) | *al het verkeer wordt (vanaf 12.30 uur) overgeheveld naar AZ IN zodat de inproductiestelling op AZ UP kan plaatsvinden zonder hinder voor productie* |
| J2 Zaterdag | X |
| J3 Zondag | X |
| J4 Maandag | X |
| J5 Dinsdag | *de inproductiestelling op AZ UP vindt plaats overdag* |
| J6 Woensdag | *het verkeer wordt in 2 fasen teruggebracht naar AZ UP : om 12.00 uur 5% en om 14.00 uur 50%* |
| J7 Donderdag | *95% van het verkeer wordt teruggebracht naar AZ UP om 12.30 uur* |
| J8 Vrijdag | *100% van het verkeer wordt teruggebracht naar AZ UP om 12.30 uur* |
| J9 Zaterdag | X |
| J10 Zondag | X |
| J11 Maandag | X |
| J12 Dinsdag | *de inproductiestelling op AZ IN vindt plaats overdag* |
| J13 Woensdag | *het verkeer wordt in 3 fasen teruggebracht naar AZ IN : om 12.00 uur 5 % en om 14.00 uur 50 % en 95 % om 22.00 uur* |

(*) Deze planning kan lichtjes wijzigen in functie van de uitrol van de release

U vindt deze mogelijke wijzigingen via de volgende link: :
https://status.ehealth.fgov.be/nl/interventions

### Modaliteiten voor de inproductiestelling van een major release (*)

Inproductiestelling major release

| Timing | Fasen |
|---|---|
| J1 Vrijdag (vóór de inproductiestelling op AZ UP) | *al het verkeer wordt (vanaf 12.30 uur) overgeheveld naar AZ IN zodat de inproductiestelling op AZ UP kan plaatsvinden zonder hinder voor productie* |
| J2 Zaterdag | X |
| J3 Zondag | X |
| J4 Maandag | X |
| J5 Dinsdag | X |
| J6 Woensdag | *het verkeer wordt in 2 fasen teruggebracht naar AZ UP: om 012 00 uur 5 % en om 14 00 uur 50 %* |
| J7 Donderdag | *de inproductiestelling op AZ IN vindt plaats overdag* |
| J8 Vrijdag | *100% van het verkeer wordt teruggebracht naar AZ UP om 12.30 uur* |
| J9 Zaterdag | X |
| J10 Zondag | *de inproductiestelling op AZ IN vindt plaats overdag* |
| J11 Maandag | *het verkeer wordt in 3 fasen teruggebracht naar AZ IN : om 12 00 uur 5 % en om 14 00 uur 50 % en 95 % om 22.00 uur* |

(*) Deze planning kan lichtjes wijzigen in functie van de uitrol van de release

U vindt deze mogelijke wijzigingen via de volgende link: :
https://status.ehealth.fgov.be/nl/interventions

De acceptatie-omgeving laat toe de nodige testen uit te voeren voor de implementatie van de release in de productie-omgeving.

We benadrukken dat het belangrijk is om fictieve (persoons)gegevens te gebruiken bij de testen. Het gebruik van reële gegevens is strikt verboden.

Voor elke major release of implementatie van een nieuwe component is het aanbevolen om testen te verrichten om te controleren dat uw componenten compatibel zijn met de (nieuwe) versies van onze diensten die online geplaatst worden.

De eHealth Release Notes zijn documenten waarin de belangrijkste nieuwe ontwikkelingen worden toegelicht, alsook de aanpassingen aan de basisdiensten van het eHealth-platform, het einde van de levenscyclus van diensten en de eventueel gekende problemen.

De Release Notes worden op het portaal van het eHealth-platform gepubliceerd 3 maanden vóór een major release en 1 maand vóór een minor release.

# 2. eHealth Business Continuity Plan

Het Business Continuity Plan van het eHealth-platform heeft tot doel het behoud van onze diensten te garanderen na een groot incident dat het informaticasysteem treft. Het gaat erom de activiteit zo snel mogelijk te hervatten met minimaal gegevensverlies en het behoud van een bepaald veiligheidsniveau. Dat plan is een van de essentiële punten van ons informaticaveiligheidsbeleid.

Ongeacht het verantwoordelijkheidsniveau of de bron van het incident, is het de bedoeling een noodoplossing ter beschikking te stellen wanneer er een impact wordt vastgesteld op het niveau van de beschikbaarheid van de diensten van het eHealth-platform en/of van de eGezondheidsdiensten zodat de voornaamste functies worden gegarandeerd.

De bepaling van de prioritaire functies en van hun prioriteitsniveau en de technische implementatie van de oplossingen gebeuren in nauwe samenwerking met de partnerinstellingen en de softwareleveranciers. Wat de mededeling van de informatie betreft en gelet op de complexe verwachtingen van de verschillende doelgroepen (eindgebruikers/zorgverleners en ICT-integratoren/softwareleveranciers), wordt de informatie die de zorgverleners direct aanbelangt, meegedeeld via de website eHealth Status. Deze site bevat een gedetailleerd overzicht van de geïmplementeerde procedures en van de softwarepakketten die die procedure hebben overgenomen. De informatie en de procedures die specifiek voor de ICT-integratoren zijn bestemd, worden geconsolideerd op die pagina van de website van het eHealth-platform, die specifiek aan die opdracht is gewijd.

De implementatie van een BCP, de integratie van de verschillende interfaces en de noodzakelijke testen nemen tijd in beslag en vergen een continue aanpassing. De prioriteit ging in een eerste fase naar de huisartsen en apothekers. De implementatie van de oplossingen staat reeds gedocumenteerd op de website eHealth Status .

Met de verdere uitrol van de processen zal gelijktijdig het volgende worden gerealiseerd:

- de geconsolideerde deelname van nieuwe partners volgens hun verantwoordelijkheden
- de continuïteit en de validatie van de processen die momenteel bij de partners worden ingevoerd volgens de opgelegde standaarden
- de permanente verbetering van de tools en oplossingen op basis van de vaststellingen op het terrein
- de geleidelijke implementatie van nieuwe oplossingen voor alle eindgebruikers

Het eHealth-platform stelt de nodige informatie ter beschikking van de ICT-integratoren zodat zijn de BCP-oplossing in hun systeem kunnen integreren. Hiertoe worden verschillende documentatiemedia aangeboden:

- een cookbook voor een generieke implementatie van de BCP-oplossing

- een samenvattend document met een concrete, reeds functionele toepassing van het BCP in het kader van de dienst verzekerbaarheid bestemd voor de apothekers
- de cookbooks van bepaalde diensten (STS en ETK depot) bevatten bepaalde BCP-procedures die specifiek zijn voor het gebruik ervan en die een aanvulling zijn op de BCP-oplossing die in het BCP-cookbook wordt beschreven
- de connectoren dienen tevens als ondersteuning bij de integratie

## 3. Serviceniveaus

De serviceniveaus van het eHealth-platform worden in twee verschillende documenten vastgelegd:

- Het 'MSA' (Master Service Agreement) waarin een globaal kader wordt aangeboden;
- Het 'SLA' (Service Level Agreement) dat specifiek is voor elke dienst.

### Het 'MSA'

Het MSA biedt de gebruikers van de diensten van het eHealth-platform een globaal kader aan waarin hoofdzakelijk het incident-, problem- en changemanagement wordt behandeld. In dat document worden de verbintenissen van het eHealth-platform, de verschillende toepasbare procedures en de beschrijvingen van de diensten opgenomen.

### Het 'SLA'

In het SLA worden de verbintenissen bepaald die specifiek zijn voor elke dienst van het eHealth-platform. Dat document omvat onder meer de doelstellingen inzake performantie en/of beschikbaarheid eigen aan elke dienst, ook KPI's (Key Performance Indicators) genoemd. De verschillende SLA's zijn beschikbaar op het portaal in de verschillende hoofdstukken waarin de door het eHealth-platform voorgestelde diensten worden behandeld.

# Connectors

Overzicht van de verschillende connectoren ontwikkeld door het platform eHealth

# 1. eHealth platform services connectors

De “*eHealth platform services connectors*” zijn lokale (en lichte) bibliotheken met de bedoeling om de ontwikkelaars van software voor individuele zorgverleners en apotheken te helpen bij de integratie van de basisdiensten van het eHealth-platform die worden aangeboden via “web service”-interfaces. Deze bibliotheken dienen meer algemeen eveneens ter ondersteuning van de verbindingen met de diensten met toegevoegde waarde die via het eHealth-platform beschikbaar zijn of die gebruik maken van de ICT-standaarden die door het eHealth platform werden vastgesteld (zoals de "hubs" bijvoorbeeld). De ontwikkeling van deze bibliotheken kadert dus in de standaardisering en de ondersteuning bij het gebruik van de basisdiensten van het eHealth-platform.

Deze connectoren zijn opgebouwd uit twee "lagen".

- De eerste laag of “**technische connector**” biedt een algemene API ter ondersteuning van het gebruik van louter technische basisdiensten (hoofdzakelijk in het domein van de beveiliging: authenticatie, vercijfering, …)
- De tweede laag of “**businessconnector**” maakt gebruik van de technische connector om de verbinding met een reeks diensten voor een bepaalde doelgroep binnen éénzelfde sessie te vergemakkelijken.

De connectoren zijn uiteraard afhankelijk van de interfaces van de diensten die zij integreren. De updates van de connectoren ingevolge de wijzigingen aan deze interfaces worden in de mate van het mogelijke ter beschikking gesteld via deze webpagina..

Deze connectoren zijn beschikbaar in JAVA en .NET, maar worden uitsluitend ontwikkeld in JAVA. De .NET-code is dus geen ‘native code’. Deze connectoren worden gegenereerd aan de hand van een versie van de tool IKVM die licht werd aangepast aan onze behoeften. Als u van plan bent om vanuit dezelfde filosofie uw eigen library’s te ontwikkelen op basis van de onze, raden we u aan om diezelfde versie van de tool te gebruiken en de richtlijnen voor de integratie ervan na te leven. De connectoren zijn bibliotheken die verdeeld worden onder vrije licentie. Ze zijn beschikbaar voor iedereen die ze wil gebruiken. Voor ondersteuning bij het gebruik van deze bibliotheken dient er op voorhand een aanvraag te worden ingediend bij het eHealth-platform via het e-mailadres info@ehealth.fgov.be (met als onderwerp "eHealth platform service connectors").

## Wijziging van mei 2024 ten opzichte van de vorige versies

**Release 4.5.4 & 3.26.1**

### Business connectoren

Bug fixes

- eh2ebox en ehboxv3: het MIME-type van de berichttekst is niet langer beperkt tot text/plain of text/html, om het gebruik van andere MIME-types voor eH2eBox mogelijk te maken.
- MyCareNet Registratie: verwijderen van de datum-tijdzone in de xml gegenereerd door de connector (sommige mutualiteiten accepteren geen tijdzones).

**Technische connectoren**

Update van het standaard configuratiebestand van de connector om de configuratiemodule ConfigurationModuleRegisterTransformers te starten, zodat de XAdES optionele-deflate transformatie beschikbaar is.

**Opmerking**: de minor versies van afhankelijkheden zijn ook bijgewerkt voor versie 4.5.4, in het bijzonder het verplaatsen van org.apache.commons:commons-compress naar v1.26.1, die beveiligingsproblemen oplost.

### Diensten die gedekt worden op het niveau van de “business”-lagen

- eHealth-platform services connectors

### Compatibiliteit van de technische connector

- De compatibiliteit van de technische connector versie 4.4.0 met de Recip-e-connectoren is gevalideerd.

### Download

De java-connectoren en een archief-bestand met de “.net”-connectoren zijn beschikbaar via een maven repository. De volgende lijst bevat links naar de business connectoren van de diverse beroepsgroepen en de technische connector.

- Physician
- Physiotherapist
- Nurse
- Pharmacy
- Dentist
- Midwife
- Practical Nurse
- Audiologist
- Dietician
- Occupational Therapist
- Logopedist

- Orthoptist
- Podologist
- Trussmaker
- Technische connector

# Onlinediensten

## 1. Toegang tot de gezondheidskluizen

In België worden de gezondheidsgegevens onder meer opgeslagen in de zogenaamde eerstelijnsgezondheidskluizen. Er bestaan er drie in België, één per gewest.  In Vlaanderen gaat het om Vitalink, in Wallonië om Intermed en in Brussel om Brusafe.  Dankzij de dienst 'Toegang tot de regionale gezondheidskluizen' kunnen de gemachtigde zorgverleners via hun medisch softwarepakket waarin deze dienst is opgenomen, toegang krijgen tot de gezondheidsgegevens die in die kluizen zijn opgeslagen. Die toegang wordt strikt gereglementeerd volgens de voorwaarden van de wet inzake gezondheidsgegevens. Het eHealth-platform heeft in dat kader als opdracht om de uitwisselingen te beveiligen.

## 2. WalCareNet - MemberData

De dienst "Member Data" (MDA) van WalCareNet laat elke gemachtigde instelling of zorgverlener toe om de informatie van de zorggebruiker te raadplegen die nodig is voor een correcte facturatie of zorg- of productverstrekking.

Deze dienst heeft betrekking op verschillende luiken waarvan het eerste, de verzekerbaarheidsgegevens van de patiënt, gemeenschappelijk is voor alle instellingen en zorgverleners.

Elke sector heeft naargelang de beslissingen van het Informatieveiligheidscomité het recht om toegang te krijgen tot een of meerdere luiken.

Naargelang de sector is deze dienst toegankelijk op synchrone en/of asynchrone wijze.

Hieronder alle luiken die voor WalCareNet beschikbaar zijn:

- Verzekerbaarheidsgegevens van de patiënt (toegankelijk voor alle sectoren) = facet insurability
- De huisapotheker = facet ReferencePharmacy;
- Het GMD = facet GlobalMedicalfile;

- De status palliatieve zorg  = facet Palliativestatus.
- Het zorgtraject = facet Carepath

### Voor wie?

- De rust- en verzorgingstehuizen (RVT), de rusthuizen (RH) & de centra voor dagverzorging (CDV)
- De psychiatrische verzorgingstehuizen (PVT).
- De ziekenhuizen
- De IBW (initiatieven voor beschut wonen)
- De OTM (orthopedisch technoloog in mobiliteitshulpmiddelen)
- De CFR (centra voor functionele revalidatie)
- De GTZ (geïntegreerde thuiszorg)

### Hoe invullen/gebruiken ?

Om de dienst “Member Data” te gebruiken, legt de zorgverlener een verzoek voor met daarin, behalve de identificatie van de patiënt (op basis van zijn INSZ of zijn inschrijvingsnummer bij het ziekenfonds), de periode waarvoor de raadpleging van de informatie wordt gevraagd alsook de gegevens die hij/zij wenst te ontvangen: verzekerbaarheidsgegevens en een of meerdere afgeleide rechten waarop zijn sector recht heeft.

Enkel de gegevens waarvoor de sector gemachtigd is kunnen worden opgevraagd.

Dit verzoek wordt naar WalCareNet gestuurd die het verzoek verwerkt en in zijn antwoord de gegevens meedeelt die de sector mag krijgen.

Deze dienst is enkel via webservice op synchrone wijze en op asynchrone wijze beschikbaar.

# Informatieveiligheid & Privacy

Onze regelgeving en diensten inzake veiligheid en informatie omtrent GDPR

# 1. Toolbox

## Awareness

Hoewel het merendeel van de informaticarisico's vermeden kan worden of opgelost kan worden dankzij aangepaste veiligheidstools, blijft het belangrijk dat de medewerkers de risico's en oplossingen ten volle begrijpen, aangezien de "menselijke fout" de zwakke plek is die het vaakst uitgebuit wordt. Daarom stellen de federale instellingen van volksgezondheid didactische en pedagogische tools ter beschikking van de ziekenhuizen om hen te helpen bij hun informatie- en preventie-opdracht op het vlak van informaticaveiligheid. Verschillende informatiedragers zijn beschikbaar, zoals affiches, powerpoint-presentaties, flyers of filmpjes over diverse onderwerpen zoals paswoordbeheer, phishing, malware of veiligheidsmaatregelen bij telewerk.

Alle informatie en materiaal is terug te vinden in volgende fiches, gebundeld per thema:

- Phishing
- Wachtwoorden en multifactor authenticatie
- Social engineering
- Telewerk
- Veilig communiceren
- Het CyZo Project (Helix-groep)

## Continuity

Voor elke organisatie is de controle over de continuïteit van de bedrijfsprocessen heel belangrijk.

De steeds meer doorgedreven cybersecurityaanvallen op de informatiesystemen van ziekenhuizen, laboratoria en andere instellingen binnen de gezondheidszorg, zorgen er voor dat de nodige maatregelen moeten worden genomen om deze systemen en aldus hun processen beter te beschermen.

Aan de hand van een aantal onderwerpen bieden we informatie en hulpmateriaal (zoals controlelijsten) om de continuïteit te verbeteren. U vindt de nodige informatie op volgende informatiefiches, gebundeld per thema.

- Incident response plan
- Business Continuity Plan

Opmerkingen en suggesties zijn steeds welkom via mail: security@ehealth.fgov.be

### Zelfevaluatie

Deze zelfevaluatie heeft als doel om een idee te hebben over de 'aantoonbaarheid' dat je organisatie conform is met bepaalde punten uit de AVG regelgeving.

- Zelfevaluatie – Conformiteit AVG

## Budgettering FOD VVVL

### Toewijzing van het 2024 Cyberbudget van de ziekenhuissector

Dit sectie bevat de instructienota over het individuele en "contributor" financiering, samen met de twee formulieren die vermeld worden in de circulaire van 15/03/2024 "Toewijzing van het budget cyber 2024 voor de ziekenhuissector".

- Instructienota over individuele en "contributor" financiering – te raadplegen voordat u de formulieren invult
- Formulier voor toegang tot individuele financiering - in te vullen **ten laatste op 31 mei 2024**
- Formulier voor toegang tot “contributor” financiering - in te vullen **ten laatste op 1st april 2024**

## 2. Minimale Normen Ziekenhuizen

Er werd voor de instellingen in de gezondheidssector een lijst opgesteld met Minimale Normen (MNM), en Implementatierichtlijnen , geïnspireerd op de ISO 27000-reeks. Die hebben tot doel de veiligheidsregels en de controlemiddelen erop te versterken, teneinde het algemene veiligheidsniveau van alle instellingen die gebruikmaken van het eHealth-platform te verhogen.

De MNM vormen de basis van waaruit de functionaris voor gegevensbescherming het informatieveiligheidsbeleid uitvoert met betrekking tot de hem of haar omringende informatiesystemen en -structuren.

Met dank aan NBN.

## Maturiteitstool

Samen met de ziekenhuizen werd een tool ontworpen om de maturiteit van de ziekenhuizen t.o.v. de minimale normen van de gezondheidssector te bepalen.

Naar het bestand met de tool.

# 3. Opleiding & GDPR

### Veiligheidsconsulent - Opleidingen

Het eHealth-platform biedt jaarlijks een opleiding aan rond informatieveiligheid en gegevensbescherming.

In samenwerking met de erkende gespecialiseerde dienst van Smals werd een opleidingsplan opgesteld. Dit opleidingsprogramma legt de nadruk op de kennis die een DPO of informatieveiligheidsconsulent moet hebben om de opdracht naar behoren te vervullen, ongeacht de grootte van de organisatie waarin deze is tewerkgesteld.

Geïnteresseerden die aan deze opleiding wensen deel te nemen, moeten voldoen aan de volgende voorwaarde:

- de organisatie maakt gebruik van de basisdiensten van het eHealth-Platform

Voor alle praktische inlichtingen (data van de cursussen, inschrijvingen, lokalen, ...) kunt u terecht bij Joëlle Ankaer (02-787.58.62)

Voor inlichtingen in verband met de inhoud van de cursus kunt u contact opnemen met security@ehealth.fgov.be

- Beschrijving Programma
- Inschrijvingsformulier
- Agenda Opleiding 2024

### General Data Protection Regulation

De Europese Algemene Verordening Gegevensbescherming ('European General Data Protection Regulation' afgekort 'EU GDPR') introduceert nieuwe regels rond het beheer en de beveiliging van persoonsgegevens. De Europese Commissie beoogt met deze Verordening om de burgers terug controle te geven over hun persoonsgegevens en het regelgevende kader voor internationale bedrijven te vereenvoudigen door de regels binnen de EU gelijkvormig te maken.

Deze verordening is op 24 mei 2016 in werking getreden. Maar er was in een overgangsperiode van 2 jaar voorzien waardoor alle organisaties tot 25 mei 2018 de tijd kregen om zich aan de nieuwe eisen van de EU GDPR aan te passen. In tegenstelling tot een Richtlijn is er geen omzetting vereist in de Belgische regelgeving.

Het eHealth-platform wenst via deze webpagina de juiste informatie samen te brengen over deze nieuwe verordening.

Hieronder vindt u de links naar relevante bronnen:

- De originele Europese tekst rond de EU GDPR
- Omzendbrief GDPR

Verdere informatie van de Europese Commissie rond de EU GDPR

- EU GDPR factsheets
- Verduidelijking rond de overdraagbaarheid van gegevens
- Verduidelijking rond de functionaris voor gegevensbescherming (DPO)
- Verduidelijking rond identificatie van de 'verwerkingsverantwoordelijke' of 'leidende toezichthoudende autoriteit'
- Publicatie van persoonlijke gegevens voor transparantiedoeleinden in de publieke sector
- Verduidelijking rond de gegevensbeschermingsimpactbeoordeling (DPIA)
- Toolkit van EDPS rond beperkingen omtrent de bescherming van persoonlijke gegevens
- DPO corner

De Gegevensbeschermingsautoriteit (GBA) heeft een specifieke webpagina rond EU GDPR en een stappenplan uitgetekend voor de implementatie van de EU GDPR.

De Gegevensbeschermingsautoriteit (GBA) heeft ook een aanbeveling uit eigen beweging uitgebracht met betrekking tot de gegevensbeschermingseffectbeoordeling ('data protection impact assessment' of 'DPIA').

De KSZ heeft de minimale normen voor informatieveiligheid aangepast en ook in overeenstemming gebracht met de EU GDPR

Deze webpagina zal geregeld aangepast worden op basis van nieuwe teksten en evoluties.

# Standards

Interoperabiliteit tussen de diverse actoren binnen de gezondheidszorg kan pas worden gerealiseerd wanneer duidelijke afspraken gemaakt worden. Afhankelijk van de graad van interoperabiliteit die nagestreefd wordt, dienen afspraken te worden gemaakt over de regels voor gegevensuitwisselingen, de algemene architectuur van het uitwisselingssysteem, de uitgewisselde berichten, de structuur van medische documenten en de codificatie van informatie.

Sinds geruime tijd worden in België standaardisatie-initiatieven ondernomen en projecten opgezet. Hieronder volgt een beknopt en niet-exhaustief overzicht van de standaarden die in meer of mindere mate gebruikt worden in de Belgische gezondheidszorg.

De wetgever heeft aan het eHealth-platform de opdracht meegegeven om nuttige, ICT-gerelateerde functionele en technische standaarden vast te stellen om de elektronische gegevensuitwisseling in de gezondheidszorg te ondersteunen. Deze standaarden zullen verder bouwen op de reeds gebruikte, hieronder vermelde standaarden en zullen worden vastgelegd in nauw overleg met de onderscheiden actoren in de gezondheidszorg. De standaarden die het eHealth-platform zal vastleggen, betreffen enkel de ICT-aspecten en niet de inhoudelijke aspecten van de gezondheidzorg.

# 1. Standards

Interoperabiliteit tussen de diverse actoren binnen de gezondheidszorg kan pas worden gerealiseerd wanneer duidelijke afspraken gemaakt worden. Afhankelijk van de graad van interoperabiliteit die nagestreefd wordt, dienen afspraken te worden gemaakt over de regels voor gegevensuitwisseling, de algemene architectuur van het uitwisselingssysteem, de uitgewisselde berichten, de structuur van medische documenten en de codificatie van informatie.

Sinds geruime tijd worden in België standaardisatie-initiatieven ondernomen en projecten opgezet.

De wetgever heeft aan het eHealth-platform de opdracht meegegeven om nuttige, ICT-gerelateerde functionele en technische standaarden vast te stellen om de elektronische gegevensuitwisseling in de gezondheidszorg te ondersteunen.

Naar de website over de standaarden