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.

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

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)

Basisdiensten

1. Codering, anonimisering en TTP
2. Elektronische datering (timestamping)
3. Systeem voor end-to-end vercijfering
4. Portal
5. Data Attribute Service - Web service
6. Verwijzingsrepertorium (Hubs &Metahub)
7. Webservices ConsultRR
8. Coördinatie van elektronische deelprocessen
9. IAM (Identity & Access Management)
10. eHealth-certificaten
11. Beveiligde elektronische brievenbus (eHealthBox)

Application LiveCycle

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

Standards

1. Standards

Connectors

1. eHealth platform services connectors

Informatieveiligheid & GDPR

1. Informatieveiligheid & General Data Protection Regulation

Architectuur

1. Architectures

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. Codering, anonimisering en TTP

Wat zijn de codering en anonimisering (Trusted Third Parties) van het eHealth-platform?

Deze tools laten toe om de identiteit van een persoon of van de medische gegevens met betrekking tot een persoon te verbergen achter een code, teneinde de privacy van deze persoon te beschermen en het medisch beroepsgeheim na te leven. De codering gebeurt via een synchrone webservice, terwijl de TTP-anonimisering asynchroon gebeurt via een batch die complementair is aan de eHealthBox.

Wat zijn de functionaliteiten van de codering en de TTP-anonimisering?

Codering

De webservice codering (WS Seals) biedt de volgende functionaliteiten:

- ‘Encode’: deze methode laat toe gegevens als input in te geven, waarna deze gegevens in gecodeerde vorm teruggegeven worden. Er zijn verschillende algoritmes beschikbaar waarmee de codering kan worden uitgevoerd
- ‘Decode’: deze methode laat toe om gecodeerde gegevens als input in te geven, waarna de niet-gecodeerde gegevens teruggegeven worden

TTP-anonimisering

De TTP-anonimisering, ook “batch TTP codering” genoemd, laat toe aan een instelling of zorgverlener die over medische gegevens beschikt om zijn gegevens in anonieme vorm naar een gekende bestemmeling te versturen, d.w.z. dat de informatie die toelaat om de betrokken persoon (op wie de medische gegevens betrekking hebben) te identificeren gecodeerd wordt. De anonimisering gebeurt ook op het niveau van de verzender van het bericht zodat de bestemmeling niet weet van wie de medische gegevens die hij ontvangen heeft afkomstig zijn en het niet mogelijk is hieruit af te leiden op wie de gegevens betrekking hebben.

De TTP laat de bestemmeling ook toe de medische gegevens die hij ontvangen heeft te verrijken en ze terug te sturen naar de oorspronkelijke verzender (zonder dat hij de identiteit van de verzender te weten komt). In dat geval worden de gegevens gedeanonimiseerd zodat de oorspronkelijke verzender kennis kan nemen van alle informatie.

Concreet gebeurt de verzending en ontvangst van de berichten via de eHealthBox, terwijl de batch TTP Codering deze berichten verwerkt teneinde ze te anonimiseren/deanonimiseren en te verzenden naar de juiste instelling of persoon. Zodra het bericht verwerkt en afgeleverd is, krijgt de verzender een ontvangstbewijs zodat hij weet dat het bericht ontvangen werd, ofwel krijgt hij een melding met de reden waarom het niet verwerkt kon worden. Een bericht wordt binnen de 2 uur na verzending verwerkt en doorgestuurd naar de eindbestemmeling.

In de praktijk

Wat zijn de voorwaarden voor de integratie van de dienst codering en TTP van het eHealth-platform ?

- Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform

  Wolf.Wauters@ehealth.fgov.be

  en beschrijf duidelijk de context en het doeleinde van uw project

- In het kader van het gebruik van de batch TTP codering zijn drie elementen vereist:
  - Akkoord van het Sectoraal Comité:
    - opstellen van een machtigingsaanvraag voor het gebruik van de batch codering en indienen bij het Sectoraal Comité. U vindt de lijst van de verschillende sectorale comités alsook nuttige informatie over de machtigingsaanvraag via de volgende link
    - voor verdere vragen over de aanvraag kunt u terecht bij TTP@ehealth.fgov.be
  - Elektronische ondertekening van het document TTP_GlobalDoc
    - zodra het Sectoraal Comité zijn akkoord heeft verleend, dient een document “TTP_GlobalDoc” te worden opgesteld door het team TTP Service van het eHealth-platform (contact: TTP@ehealth.fgov.be). Dit document vat de procedure van uitwisseling van medische gegevens samen (verzenders, bestemmelingen, details van de doorgave, ...) overeenkomstig de beraadslaging van het Sectoraal Comité. Dit document dient elektronisch te worden ondertekend door alle partijen die betrokken zijn bij het project
    - na de ondertekening van dit document zal het team TTP Service van het

eHealth-platform aan de verzenders de nodige informatie bezorgen omtrent het gebruik van de batch TTP (bijvoorbeeld de naam van het TTP-project die in de berichten moet worden gebruikt)

- Toegang tot eHealthBox
  - zoals reeds vermeld, veronderstelt het gebruik van de batch TTP codering het gebruik van de eHealthBox. Dit betekent dat de verzenders en de ontvangers in het bezit moeten zijn van een eHealth-certificaat

- In het kader van het gebruik van de dienst codering
  - Beschikken over een eHealth-certificaat om de webservice te kunnen gebruiken
  - Akkoord van het Sectoraal Comité in geval van gebruik van de methode “Decode"

    Aangezien de methode “Decode” toelaat om de gegevens te decoderen, moet hiervoor een machtiging bestaan van het Sectoraal Comité. U vindt de lijst van de verschillende sectorale comités alsook nuttige informatie over de machtigingsaanvraag via de volgende link

    Verdere vragen over de aanvraag kunnen via mail worden gericht aan Wolf.Wauters@ehealth.fgov.be

2. Elektronische datering (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

  Emmanuel de Hemricourt de Grunne

  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 (te certificeren document) op 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.

Alle 5 minuten worden de cijfercodes samengebracht in een pakket, de zogenaamde ‘TimeStampBag’. Dit pakket wordt naar het eHealth-platform verstuurd zodat zijn ‘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 archief van het ziekenhuis. Het eHealth-platform bewaart van zijn kant een kopie van het « pakket » met zijn 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

3. Systeem voor end-to-end vercijfering

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

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

De vercijferingsdiensten 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 voor de vercijfering naar een gekende bestemmeling
- KGSS voor de vercijfering naar een niet-gekende bestemmeling

De ETEE-diensten zijn beschikbaar als webservices (toegankelijk via een medisch softwarepakket of via een derde 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 eHealth-certificaat van een zorgverlener of een instelling waarvan de identificatienummers (INSZ, RIZIV-nummer, KBO-nummer) gekend zijn;
    - eenmaal verkregen laat deze ETK toe om een bericht te vercijferen 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 vercijferingssleutel 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: geauthentiseerd zijn als apotheker erkend door het eHealth-platform).

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

In de praktijk

Afhankelijkheden, aanbevelingen & 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 meer globale oplossingen zoals Recip-e, Hoofdstuk IV, eHealthBox.

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

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.

Meer informatie: support@ehealth.fgov.be

4. Portal

Het portaal www.ehealth.fgov.be 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 (eHealth-platform: www.ehealth.fgov.be/ehealthplatform). 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 linken 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 & waarschuwingen

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

- over een fall-back-scenario te beschikken in geval van onbeschikbaarheid van het CMS
- niet telkens het CMS te moeten oproepen bij elke request (belastingsherverdeling vermijden) bijvoorbeeld en de CMS maximum 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

  eHealthppkb@ehealth.fgov.be

  en geef een duidelijke beschrijving van de context van uw project

5. Data Attribute Service - Web service

In uitvoering van artikel 5, 4°, a), van de wet tot oprichting van het eHealth-platform van 21 augustus 2008 heeft het eHealth-platform als opdracht om een samenwerkingsplatform te zijn voor een veilige elektronische gegevensuitwisseling.

Nieuwe projecten, onder meer in het kader van de administratieve vereenvoudiging, vereisen het gebruik van een contactengids voor een juiste routering van de berichten. Het doel is om te kunnen bepalen naar welke instantie(s) een bericht met betrekking tot een patiënt moet worden gestuurd (bijvoorbeeld: preventiedienst, controlearts, werkgever, ...).

DAAS is dus een generieke dienst die door het eHealth-platform werd ontwikkeld om te kunnen antwoorden op verschillende vragen tot identificatie van de bestemmeling(en) van een bericht in de gezondheidszorgsector.

Deze generieke dienst volgt het voorbeeld van de Attribute Authority (AA).

Om de bestemmeling te kunnen identificeren, raadpleegt deze dienst ofwel de authentieke bronnen ofwel de residuaire routeringsgids en maakt het resultaat van de opzoeking over aan de softwareprovider van de zorgverlener.

Afhankelijk van het project zal het gebruik van deze dienst onderhevig zijn aan de goedkeuring door het Beheerscomité van het eHealth-platform en door het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid.

Voor wie?

In een eerste fase wordt deze dienst in het kader van het project “back to work” gebruikt door de softwareproviders van de huisartsen alsook door de oplossing die wordt gebruikt door de verzekeringsinstellingen en de diensten voor preventie en bescherming op het werk.

“Back to work” heeft tot doel de re-integratie te bevorderen van de langdurig zieke werknemer die het overeengekomen werk niet meer kan uitvoeren door

- hem tijdelijk aangepast of ander werk aan te bieden in afwachting van het opnieuw uitoefenen van het overeengekomen werk,
- hem definitief aangepast of ander werk te geven.

Dit reïntegratietraject wordt opgesteld in overleg tussen verschillende artsen (behandelende arts, medische dienst voor het beheer van de arbeidsongeschiktheden en de arbeidsgeneesheer).

Hiervoor moet onder andere de elektronische communicatie tussen de verschillende partijen mogelijk gemaakt worden. In dit project gaat het meer bepaald om het uitwisselen van medische gegevens tussen de behandelende arts, de controlearts van het ziekenfonds en de arbeidsgeneesheer.

DAAS wordt in dit project gebruikt om eHealthBox-berichten correct te routeren naar deze verschillende betrokken artsen.

Deze generieke dienst zal later tevens worden gebruikt in het kader van het Mult-eMediatt-project (informatisering van de arbeidsongeschiktheidsattesten).

Hulp nodig?

Het contactcentrum kan de softwareproducenten helpen bij vragen hieromtrent.

Tel: 02 788 51 55

Mail: support@ehealth.fgov.be

6. Verwijzingsrepertorium (Hubs &Metahub)

De doelstelling van het systeem van hubs en metahub in zijn geheel bestaat erin om regionale en lokale uitwisselingsystemen van medische gegevens, de zogenoemde "hubs", onderling te verbinden om aan een zorgverlener de mogelijkheid te bieden de beschikbare elektronische medische documenten met betrekking tot een bepaalde patiënt terug te vinden en te raadplegen, ongeacht de plaats waar deze documenten opgeslagen zijn en ongeacht de plaats vanwaar de zorgverlener op het systeem inlogt.

7. Webservices ConsultRR

Wat is ConsultRR?

ConsultRR 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 van de gezondheid.

Deze machtigingen (“Beraadslagingen”) worden verkregen naargelang:

- het type instelling en/of de verrichte prestaties (ziekenhuizen, erkende laboratoria, huisartsen)
- het doeleinde van de aanvraag (bv.: het nummer van dit register gebruiken voor de controle en bijwerking van de identificatiegegevens van de patiënten, de controle en bijwerking van de identificatiegegevens van hun patiënten, hun eenduidige identificatie in het medisch dossier, ...)
- het type gegevens waartoe toegang wordt gevraagd (naam, geboortedatum, geslacht, verblijfplaats, ...)

De beraadslagingen vindt u in detail terug via het tabblad “Informatieveiligheidscomité”.

Welke diensten worden door ConsultRR aangeboden?

IdentifyPerson

waarmee bepaalde gegevens van een patiënt in het rijksregister en in de Kruispuntbankregisters kunnen worden geraadpleegd op basis van een INSZ (identificatienummer van de sociale zekerheid) en de patiënt kan worden ingeschreven in het opvolgingsregister van zijn mutaties.

PhoneticSearch

waarmee het geldend uniek identificatienummer van een patiënt binnen het rijksregister en de Kruispuntbankregisters op basis van fonetische criteria (bv. naam en geboortedatum) kan worden opgezocht.

PersonHistory

waarmee de historiek (naam, geboorteplaats en -datum, geslacht, adres) van de gegevens van een patiënt in het rijksregister en de Kruispuntbankregisters kan worden geraadpleegd op basis van een INSZ (identificatienummer van de sociale zekerheid)

ManageInscription

waarmee een instantie de inschrijving van een patiënt op de abonnementendienst van mutaties kan beheren om op de hoogte te blijven van de wijzigingen van diens gegevens (bv.: adreswijziging).

MutationSender

waarmee de wijzigingen (aanpassing, toevoeging of verwijdering) van de gegevens (bv. adreswijzigingen) van een patiënt kunnen worden verkregen. De patiënt moet op voorhand zijn ingeschreven op de abonnementendienst van de mutaties (ManageInscription).

SsinHistory

waarmee de historiek van de unieke identificatienummers (INSZ/BISS) van een patiënt op basis van het laatste INSZ kan worden verkregen.

ManagePerson

waarmee bis-INSZ-nummers kunnen worden aangemaakt en waarmee in het kader van de integratietesten van de dienst ConsultRN een patiënt met fictieve rijksregistergegevens kan worden aangemaakt.

In de praktijk

De webservices van ConsultRN werden ten behoeve van de verzorgingsinstellingen en de zorgverleners ontwikkeld.

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

Ziekenhuis

- Beraadslaging RN nr. 21/2009 van 25 maart 2009
- Beraadslaging RN nr. 60/2009 van 7 oktober 2009
- Beraadslaging nr. 9/039 van 7 juli 2009

Erkend laboratorium voor klinische biologie

- Beraadslaging RN nr. 35/2010 van 6 oktober 2010
- Beraadslaging nr. 10/078 van 9 november 2010

Rusthuis of erkend verzorgingstehuis

- Beraadslaging RN nr. 41/2011 van 20 juli 2011
- Beraadslaging nr. 11/084 van 8 november 2011

Psychiatrische verzorgingstehuizen of initiatieven voor beschut wonen

- Beraadslaging RN nr. 40/2011 van 20 juli 2011
- Beraadslaging nr. 11/083 van 8 november 2011

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

De beroepsbeoefenaars in de gezondheidszorg (KB78) 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 staat in een eerste fase open aan de huisartsen.

- Beraadslaging RN nr. 77/2009 van 23 december 2009, nr. 11/2018 van 21 februari 2018 en nr. 20/2018 van 28 maart 2018
- Beraadslaging nr. 18/039 van 6 maart 2018

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: valerie.forton@ehealth.fgov.be

Hoe toegang krijgen tot Consult RR?

a) Op voorhand

Om de diensten van eHealth ConsultRN te gebruiken, moet de instelling of de zorgverlener

- over een medisch softwarepakket beschikken waarin deze dienst is geïntegreerd;
- over een eHealth-certificaat beschikken (meer informatie om een certificaat in acceptatie en in productie te verkrijgen)

b) Te volgen integratieprocedure indien uw instelling een ziekenhuis, een laboratorium, een psychiatrisch verzorgingstehuis, een initiatief voor beschut wonen, een rusthuis of een verzorgingstehuis is

Stap 1: De hierboven vermelde 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

Ter attentie van Mevrouw Joke Vanderpoorten

E-mail : ivc@mail.fgov.be

Postadres: Willebroekkaai 38 te 1000 Brussel

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 uw instelling:
    - formulier voor een ziekenhuis
    - formulier voor een laboratorium
    - formulier voor een psychiatrisch verzorgingstehuis of een initiatief voor beschut wonen
    - formulier voor een rusthuis of een 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

Voor vragen in verband met de in te vullen formulieren kan u contact opnemen met Valérie Forton, verantwoordelijke projectleider voor het eHealth-platform.

Stap 2: Het Informatieveiligheidscomité, kamer sociale zekerheid en gezondheid, zal u zijn beslissing meedelen (en bij akkoord uw APPLICATIONID) en zal tegelijkertijd het Rijksregister op de hoogte brengen.

Stap 3: U moet vervolgens het technische gedeelte opstarten (zie de cookbooks hieronder) en uw testgevallen in acceptatie opsturen naar integration-support@ehealth.fgov.be

Het hiertoe in te vullen document is beschikbaar via deze link.

Stap 4: Bij validatie van de testgevallen doet het eHealth-platform het nodige om uw toegangen in productie te configureren.

c) Te volgen integratieprocedure indien uw instelling niet tot de bovenvermelde categorie behoort

We nodigen u uit om contact op te nemen met de verantwoordelijke projectleider voor het eHealth-platform en hiertoe duidelijk de context, het doeleinde van uw aanvraag en een raming van het volume van uw project mee te delen. We zullen samen met u uw aanvraag analyseren.

Wat de huisartsen betreft, zal het beroep op bepaalde diensten van “eHealth Consult RN” opgenomen worden in de registratiecriteria van de softwarepakketten voor huisartsen.

d) Belangrijke 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: valerie.forton@ehealth.fgov.be

Deze evolutie kan immers een impact hebben zowel op juridisch als administratief vlak (bijvoorbeeld toegang tot de diensten van het eHealth-platform via de eHealth-certificaten).

8. 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
- Dienstenregister (Registry)
    - het register omvat alle diensten die aangeboden worden door het eHealth-platform en zijn partners en vermeldt ook technische en functionele informatie
    - het register is toegankelijk in acceptatie en productie

In de praktijk

Afhankelijkheden, aanbevelingen & 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

Waarschuwingen

- de diensten die asynchroon gegevens uitwisselen mogen geen gebruik maken 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

  eHealthppkb@ehealth.fgov.be

  en geef een duidelijke beschrijving van de context en de finaliteit 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

9. IAM (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 IAM 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 & waarschuwingen

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

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 diensten REST (Representational State Transfert) van het eHealth-platform vereist, zal er een integratie met onze IAM 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-IAM / 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 IAM registration formulier per omgeving invullen en voorleggen daarbij het verkregen certificaat vermelden
    - om IAM connect te gebruiken
    - het te gebruiken realm aanduiden of het formulier voor de aanmaak van realm invullen
    - het klantregistratieformulier invullen en voorleggen
  - om de IAM IDP te gebruiken
    - het IAM Registration formulier invullen en voorleggen per omgeving en daarbij het verkregen certificaat vermelden

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 IAM-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 authentiseren en een autorisatie te verkrijgen

- voor de klassieke webapplicaties (typisch voor server-side HTML-applicaties), via het component 'IAM 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 hebben tot verschillende applicaties.

Het is ook mogelijk voor een gebruiker om over te schakelen van een authenticatie/autorisatie van het type Web App naar een authenticatie/autorisatie van het type Web Service via de functionaliteit 'SSO IDP to fat client'.

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 Wep Apps gebeurt het beheer van de autorisaties door de verschillende opgeroepen diensten.

Nuttige documentatie voor de klassieke Web Apps:

- IAM overview

- IAM federation metadata
- IAM IDP
- IAM federation attributes
- IAM logout
- IAM 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 Technical specifications
- I.AM Connect - Client registration
- I.AM Connect - Realm registration

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 IAM 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.

Net zoals het mogelijk is om over te schakelen van een authenticatie/autorisatie van het type Web App naar een authenticatie/autorisatie van het type Web Service, is het omgekeerde ook mogelijk via de dienst ‘IAM STS to IDP’.

Nuttige documentatie:

- eHealthcertificaat
- IAM STS

- Coördinatie van processen

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 ‘IAM Connect’ die gebaseerd is op de standaard OIDC (OpenID Connect).

‘IAM 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 Technical specifications
- I.AM Connect - Client registration
- I.AM Connect - Realm registration

De Data Access

Dit systeem doet een beroep op de component ‘IAM 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.

IAM AA (AttributeAuthority)

IAM 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.

IAM STS (Secure Token Service)

IAM 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, ...

IAM IDP (IDentity Provider)

IAM IDP is de dienst die toelaat om de identiteitsinformatie te creëren, te onderhouden en beheren voor de gebruikers die zich kunnen authentiseren 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.

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

IAM Connect

IAM 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 geauthentiseerde sessies en de eindgebruikers. IAM Connect laat de klanten ook toe om de identiteit van de eindgebruiker te controleren in functie 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 Technical specifications
- Definitie van realm
- Definitie van klanten

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.

10. 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.

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 toegangsjeton 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.

11. Beveiligde elektronische brievenbus (eHealthBox)

De dienst eHealthBox van het 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:een publicatiedienst voor het verzenden van berichten, die het volgende omvat:
  - een “out-of-office”-dienst die toelaat te verwijzen naar een vervangende zorgverlener
    - een functionaliteit voor gegroepeerde mailverzending op basis waarvan één of meerdere berichten naar een groep zorgverleners verzonden kunnen worden (bijvoorbeeld een bericht ter attentie van het verplegend personeel van een ziekenhuis)
    - een vercijferingsdienst 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, d.w.z. 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
        - zijn rijksregisternummer (en optioneel zijn beroep)
        - zijn RIZIV-nummer (en optioneel zijn beroep)
        - zijn beroep en zijn naam (en optioneel zijn voornaam)
        - zijn beroep en zijn postcode
        - zijn beroep en zijn gemeente
        - zijn e-mailadres
    - toelaat een zorginstelling op te zoeken op basis van
        - haar EHP-nummer (en optioneel het type instelling)
        - haar RIZIV-nummer (en optioneel het type instelling)
        - haar KBO-nummer (en optioneel het type instelling)
        - haar 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 type nummer (INSZ, NIHII, CBE), eventueel het subtype (bijvoorbeeld ziekenhuis), de hoedanigheid van de actor in de gezondheidszorg of de instelling

In de praktijk

Afhankelijkheden, aanbevelingen & waarschuwingen

De dienst eHealthBox werd ontwikkeld ten behoeve van de 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 het eHealth-platform.

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 het eHealth-platform).

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

- Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform

  Wolf WAUTERS

  en beschrijf de context en de finaliteit 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 vercijferingsdienst

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: support@ehealth.fgov.be

Application LiveCycle

1. eHealth Business Continuity Plan

Het Business Continuity Plan van het eHealth-platform heeft tot doel om het behoud van onze diensten te garanderen na een belangrijke ramp die het informaticasysteem treft. Het gaat erom om de activiteit zo snel mogelijk te hervatten met een minimaal verlies aan gegevens 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 om 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 het prioriteitsniveau ervan 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 https://www.status.ehealth.fgov.be/. Deze site bevat een gedetailleerd overzicht van de geïmplementeerde procedures en van de softwarepakketten die deze procedure hebben overgenomen De informatie en de procedures die specifiek voor de ICT-integratoren zijn bestemd, worden geconsolideerd op deze 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 site https://www.status.ehealth.fgov.be/.

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 de BCP-cookbook wordt beschreven
- de connectoren dienen tevens als ondersteuning bij de integratie

2. 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 dit specifiek zijn voor elke dienst van het eHealth-platform. Dit document omvat onder meer de doelstellingen inzake performantie en/of beschikbaarheid eigen aan elke dienst, ook PKI (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.

3. Releases Management

In de tabel hieronder zijn de data van de volgende geplande MR's (Major Releases) en de begindata van de tests in acceptatie opgenomen.

Naam Release	Soort release	Content freeze	Code Freeze	Begin tests ACC	Release
R.2018.2.2	Minor	28/11/2018	03/01/2019	15/01/2019	03/02/2019
R.2019.1	Major	04/10/2018	03/01/2019	18/03/2019	05/05/2019
R.2019.1.1	Minor	03/04/2019	09/05/2019	21/05/2019	16/06/2019
R2019.1.2	Minor	30/05/2019	27/06/2019	09/07/2019	28/07/2019
R.2019.2	Major	03/04/2019	27/06/2019	02/09/2019	20/10/2019
R.2019.2.1	Minor	25/09/2019	31/10/2019	12/11/2019	08/12/2019
R.2019.2.2	Minor	28/11/2019	19/12/2019	04/02/2019	23/02/2020
R.2020.1	Major	03/10/2019	19/12/2019	09/03/2020	26/04/2020
R.2020.1.1	Minor	22/04/2020	21/05/2020	02/06/2020	28/06/2020
R.2020.1.2	Minor	28/05/2020	25/06/2020	04/08/2020	23/08/2020
R.2020.2	Major	06/05/2020	25/06/2020	31/08/2020	18/10/2020
R.2020.2.1	Minor	23/09/2020	21/10/2020	03/11/2020	13/12/2020

De benaming van de releases volgt de volgende logica: R.2015.x.y, waarbij x staat voor het volgnummer van de Major Release (MR), y voor dat van de minor Release (mR). Bijvoorbeeld, R.2015.1.2 staat voor de 2de minor Release die volgt op de eerste Major Release van het jaar 2015.

Een MR wordt een jaar vóór de implementatie gepland. Het schema hieronder geeft de belangrijkste stappen van het proces weer waarbij X = dag van de major release

X - 1 jaar:	er wordt beslist wordt welke wijzigingen de nieuwe release zal bevatten ten opzichte van de vorige;
X - 6 maanden:	“content freeze”: er worden geen verdere wijzigingen aanvaard ten opzichte van de vorige release;
X - 3 maanden:	“code freeze” plaats: er worden geen wijzigingen meer aangebracht aan de code en de cookbooks worden gepubliceerd
X - 5 weken:	begin van de tests in de acceptatie-omgeving;
X - 2 weken:	“acceptation freeze”;
X - 1 week:	functionele evaluatie van de nieuwe versie: Go/noGo;
X	major release.

De acceptatie-omgeving wordt vóór de productie-omgeving overgeheveld. Hierdoor is het mogelijk om in de acceptatie-omgeving de noodzakelijke tests te verrichten voor de implementatie van de release in de productie-omgeving.

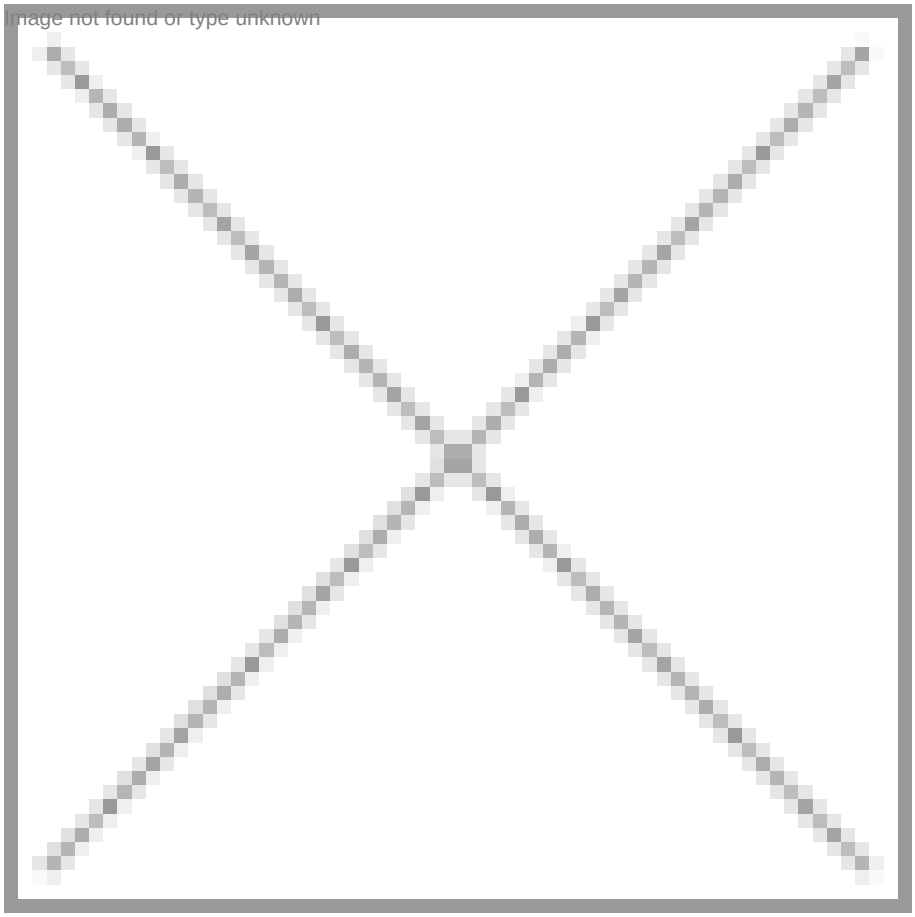
Tijdens de overgang, is het belangrijk dat uw DNS en firewall correct zijn geconfigureerd. U vindt hier een document waarin wordt uitgelegd hoe u deze kunt configureren.

Gelieve eveneens op te merken dat het noodzakelijk is gebruik te maken van fictieve gegevens bij testprocedures, het gebruik van werkelijke persoonsgegevens is strikt verboden.

Het is raadzaam om testen te verrichten zodat u bij elke release of integratie van een nieuwe component kan nagaan of uw componenten compatibel zijn met de (nieuwe) onlineversies van onze diensten. Het is bovendien mogelijk om een demonstratie te krijgen van onze diensten in de acceptatieomgeving. Het volstaat in beide gevallen om het ad hoc formulier in te vullen en het twee weken op voorhand door te mailen naar ehealth_service_management@ehealth.fgov.be.

De eHealth Release Notes zijn documenten waarin de belangrijkste nieuwe ontwikkelingen, aanpassingen aan de eHealth-basisdiensten van, End Of Live van diensten en eventueel gekende problemen worden gedocumenteerd.

Release Notes verwijzen steeds naar een eHealth Major Release en worden 3 maanden vóór een Major Release op het eHealth-portaal gepost.



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 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.

Communicatiestandaarden

Voor de communicatie tussen zorgsystemen en de definiëring van communicatieberichten wordt de in België ontwikkelde communicatiestandaard Kmehr (Kind messages for Electronic Healthcare Record) gebruikt.

Naar de website over deze standaard

Patientsummary - Sumehr

Voor het opstellen van een patient summary wordt in België gebruik gemaakt van de Belgische standaard Sumehr (Summarized Electronic Health Record). Sumehr is een Kmehr-gebaseerde standaard waarin de minimale set aan gegevens wordt bepaald die een arts nodig heeft om zicht te krijgen op de medische toestand van een patiënt.

Codificatiestandaarden

De gebruikte codificatiestandaarden zijn sterk afhankelijk van de diverse t oepassingsdomeinen. Voor rapporterings- en statistiekdoeleinden wordt in België voornamelijk gebruik gemaakt van het internationale WHO-codificatiesysteem ICD (International Classification of Diseases). Afhankelijk van de te rapporteren gegevens wordt zowel gebruik gemaakt van ICD-9 als ICD-10. Een aantal gezondheidszorgdomeinen of gebruikersgroepen werken met codificatiesystemen die van ICD-10 zijn afgeleid. Voorbeelden hiervan zijn ICD-O (International Classification of Diseases for Oncology) die gebruikt wordt door het Kankerregister. ICPC-2 (International Classification of Primary Care) is een codering die specifiek is voor de huisartsgeneeskunde. Ook de Belgische thesaurus, gebaseerd op de IBUI (Identificateur Belge Unique / Belgische Unieke Identificator), vertrekt vanuit de ICD-10- en ICPC-2-codificatie. De eerder aangehaalde standaarden zijn vrij generiek van opzet.

Specifieke standaarden

Specifieke domeinen binnen de gezondheidszorg beschikken over eigen (technische) standaarden en codificatiesystemen. DICOM (Digital Imaging and Communications in Medicine) is een voorbeeld van een technische standaard ontwikkeld voor de opslag, beheer en communicatie van medische beelden. Domeinspecifieke codificatiestandaarden zijn bijvoorbeeld ICF (International Classification of Functioning, Disability and Health) voor onder andere kinesitherapie of Loinc (Logical Observation Identifiers Names and Codes) voor de codificatie van laboresultaten.

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 .NETcode 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").

Wijzigingen van oktober 2019 tegenover de vorige versies

- Beschikbaarstelling van de dienst MemberData in de businessconnector MemberData v2 voor de nieuwe doelgroepen (zie tabel). De bestaande packages voor artsen kunnen verder gebruik blijven maken van de businessconnector MemberData v1.
- Toevoeging van een nieuwe dienst MemberData Asynch (asynchroon) voor de verpleegkundigen, vroedvrouwen, bandagisten en orthopedisten.
- Toevoeging van nieuwe acties MOHM in de businessconnector VSBnet Async (consultSupportAndRepairList, getConsultSupportAndRepairList, cancelApplication, getCancelApplication).
- Beschikbaarstelling van de dienst Mediprima Consult v2 voor de artsen en apothekers.
- Beschikbaarstelling van de dienst Therlink voor de nieuwe doelgroepen (zie tabel).
- Wijziging van de XSD’s MyCareNet voor de dienst MedAdmin.
- De gebruikers van de businessconnector eAttest v2 dienen te migreren naar versie 3.18.0 (zie bugfixes en verbeteringen in de release notes).

De “Release notes” bevatten meer informatie.

Betrokken diensten op het vlak van de "business"-lagen

- eHealth-platform services connectors Business services

Een generieke connector, die de dienst eHealthBox v3 aanbiedt, is op aanvraag ook beschikbaar voor andere beroepen.

Compatibiliteit van de technische connector

De compatibiliteit van de technische connector versie 3.18 met de Vitalink en Recip-e connectors is gevalideerd. Opgelet, om de technische connector van het eHealth-platform te integreren in de businessconnector van Recip-e, raden wij u aan om gebruik te maken van de API's die in deze connector beschikbaar zijn voor de diensten van Recip-e. De vroegere Recip-e API's die beschikbaar waren in de connector "physician" zijn verwijderd.

Download

De java-connectoren en een archief-bestand met de ".net"-connectoren zijn beschikbaar via een maven repository (repo.ehealth.fgov.be). De volgende lijst bevatten 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

Informatieveiligheid & GDPR

Onze regelgeving en diensten inzake veiligheid en informatie omtrent GDPR

1. Informatieveiligheid & General Data Protection Regulation

Veiligheidsconsulent - Opleidingen

Doel van de basisopleiding informatieveiligheid georganiseerd door het eHealth-platform

Het eHealth-platform biedt jaarlijks een basisopleiding aan rond het thema informatieveiligheid. Deze basisopleiding heeft als voornaamste doel een brede kennis te verwerven in de verschillende domeinen van informatiebeveiliging.

Het programma omvat verschillende, onafhankelijke modules. Het is dus mogelijk om in te schrijven voor afzonderlijke modules, zonder het geheel te volgen. In totaal duurt de opleiding 7 dagen.

De opleiding wordt zowel in het Nederlands als het Frans gegeven (verschillende sessies).

- Programma en inschrijvingsmodaliteiten

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 is in een overgangsperiode van 2 jaar voorzien waardoor alle organisaties tot 25 mei 2018 de tijd krijgen 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 een roadmap uitgetekend voor de implementatie van de EU GDPR.

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.

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. Architectures

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.

Deze 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 van architectuur aan:

- Een architectuur van het type SOA (Service Oriented Architecture), 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 SOA ontwikkeld en bepaalt dit type architectuur ook vandaag nog een groot aantal systemen dat in samenwerking met onze partners geïmplementeerd werd. Het onderhoud en de ondersteuning van dit model blijft ook nu één van onze opdrachten en verantwoordelijkheden, maar voor de ontwikkeling van projecten voor mobiele apparaten is het gebruik ervan niet aanbevolen (laat bv. geen vercijfering 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 authentiseren, ongeacht het toestel of het systeem dat gebruikt wordt voor de connectie.

We onderscheiden twee categorieën van 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 één 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, ten minste als de communicatie over een niet-beveiligd kanaal zoals 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-end vercijfering 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 vercijferen 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

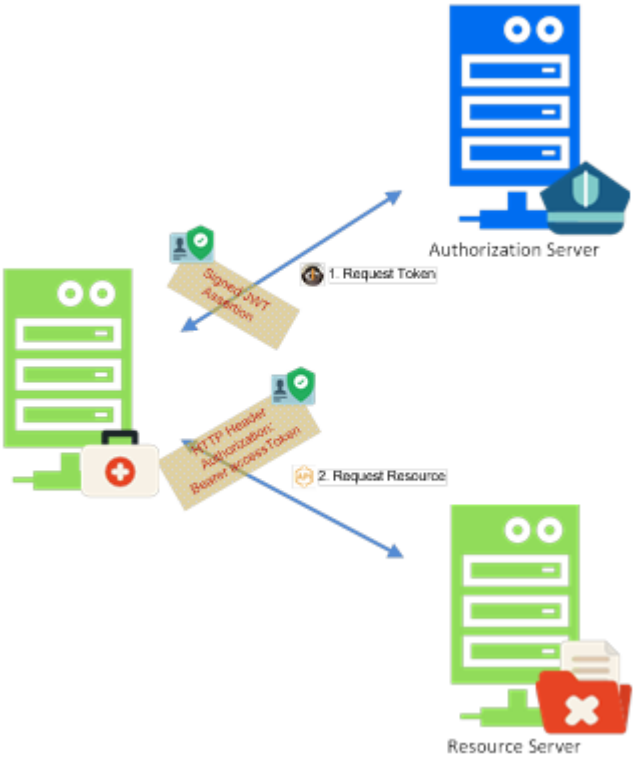
2.4. Het project moet één of meerdere types van stromen definiëren uit de voorgestelde lijst

2.4.1. Voor het luik “Identity & Access Management” dient een onderscheid te worden gemaakt tussen:

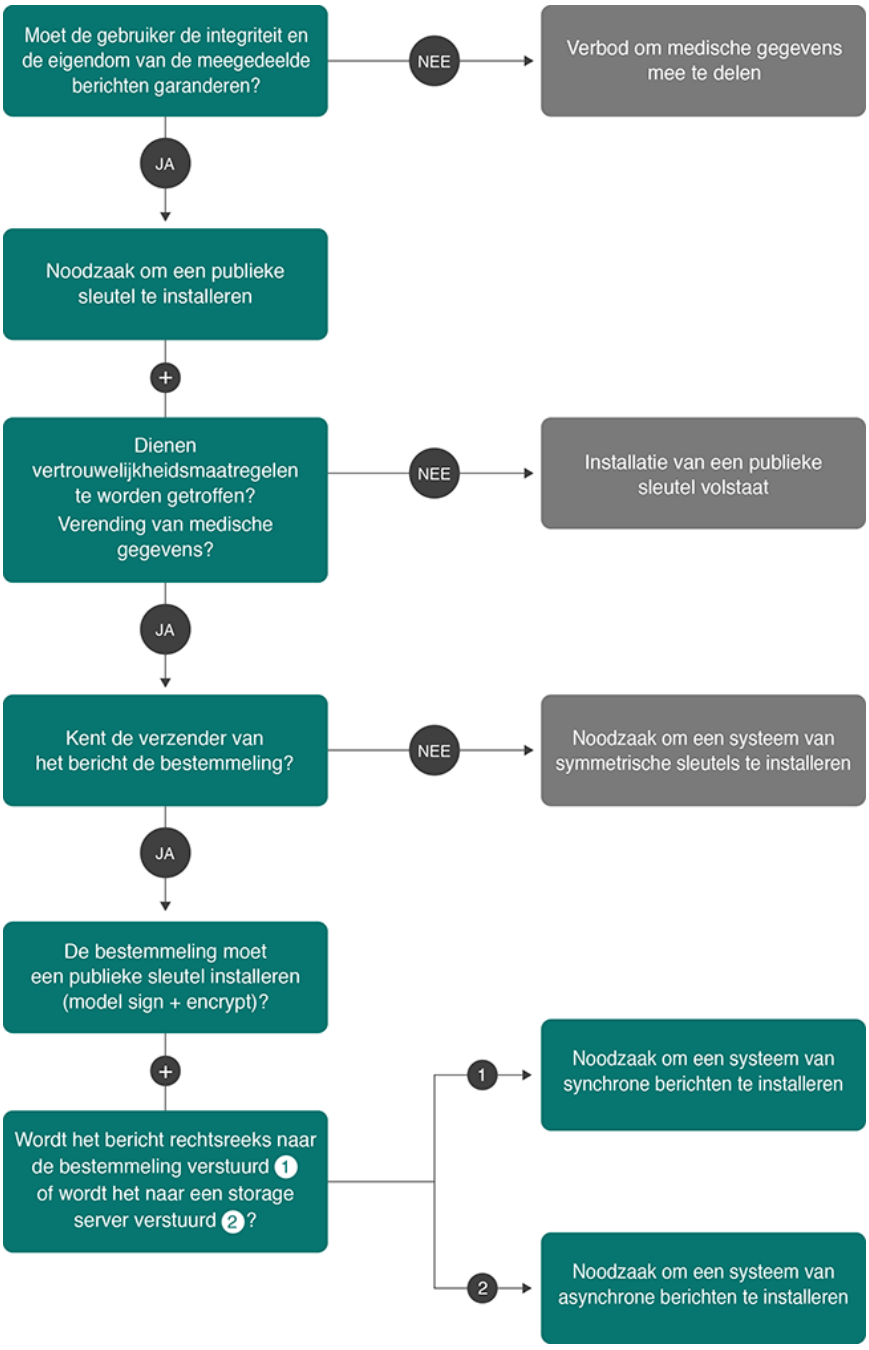
2.4.1.1. een toepassing die bestemd is om te functioneren op het mobiele toestel van de gebruiker (native app/public client)

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)

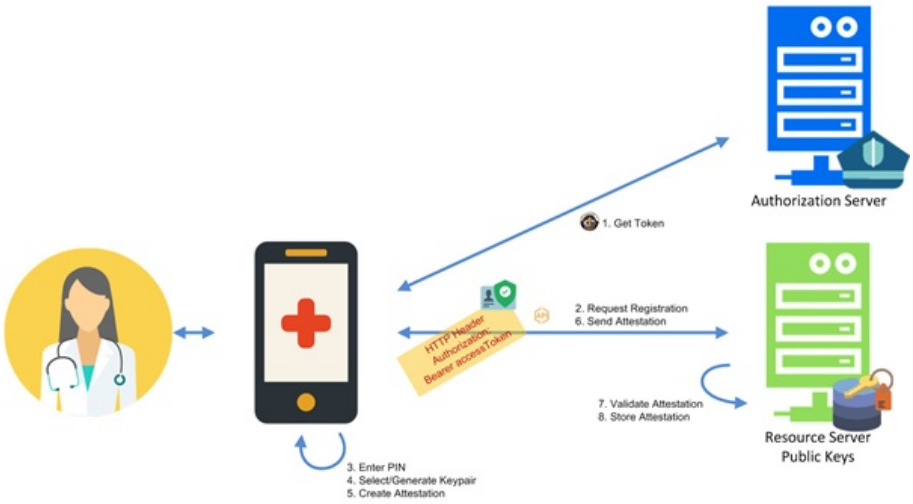


2.4.2. Wat betreft het luik “informatieveiligheid”, dient men na te denken over de volgende aspecten:

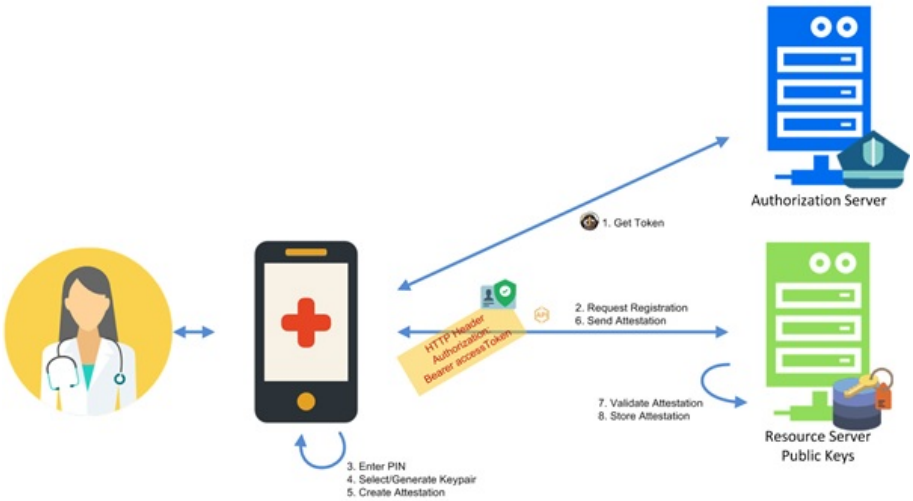


3. Schematische voorstelling use cases

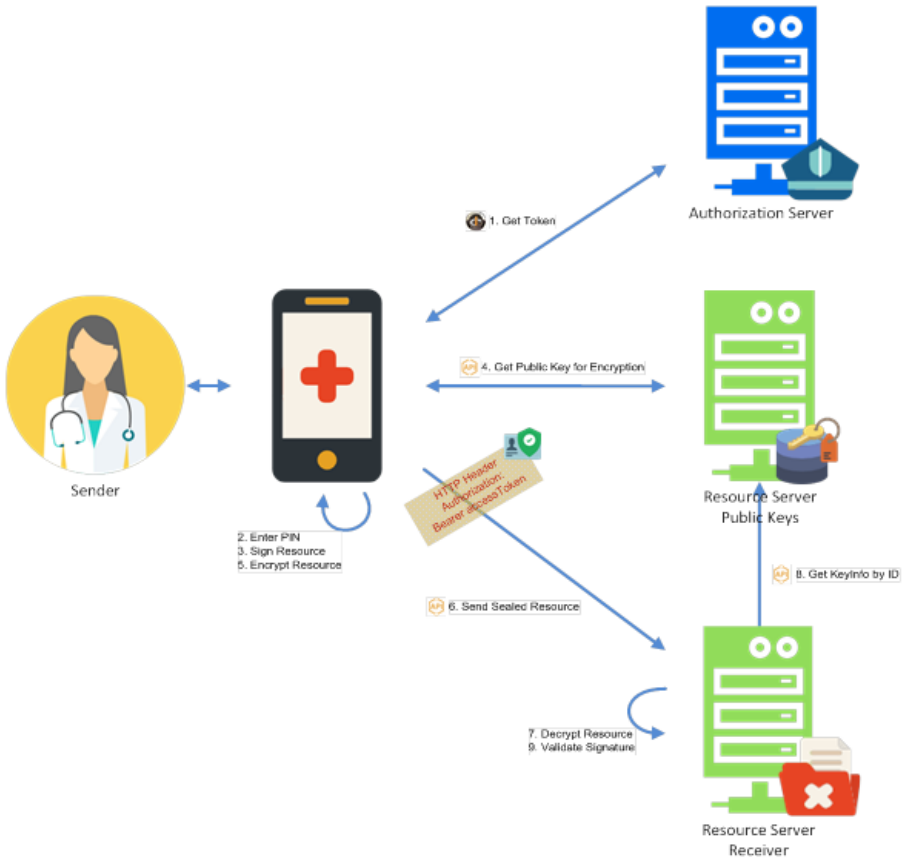
3.1. Registratie van een publieke sleutel (use case: registratie van een sleutel in het kader van de aanvraag van een eHealth-certificaat binnen een architectuur van het type SOAP)



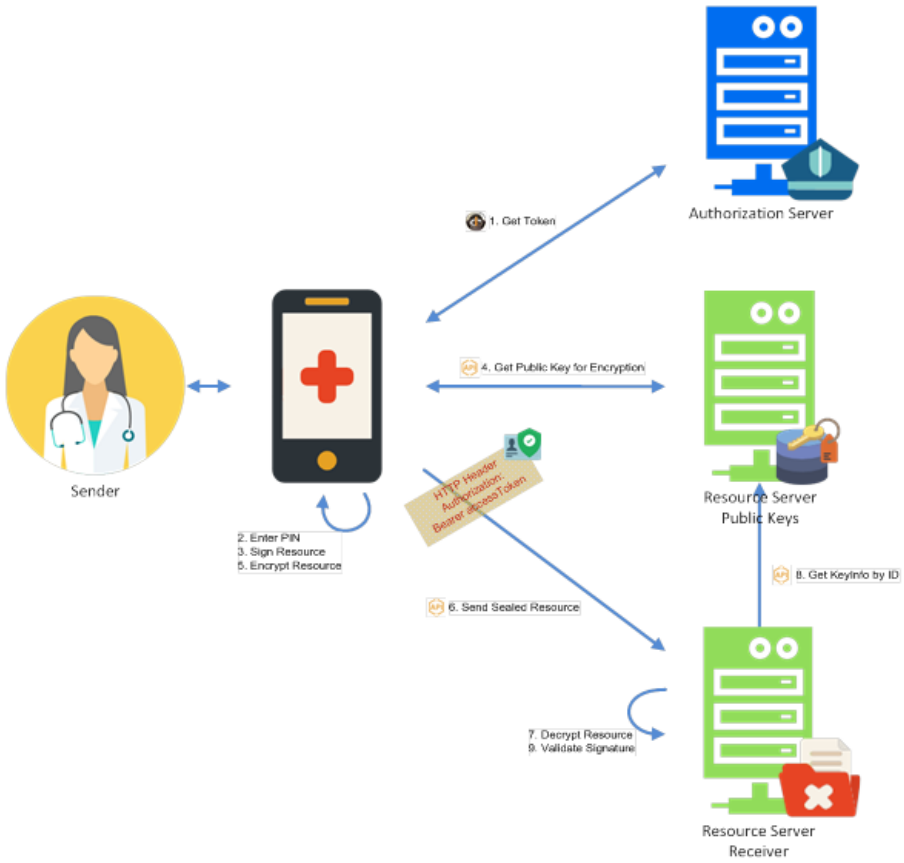
3.2. Registratie van een symmetrische sleutel (use case: registratie van een sleutel in het kader van Recip-e)



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



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



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