# 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

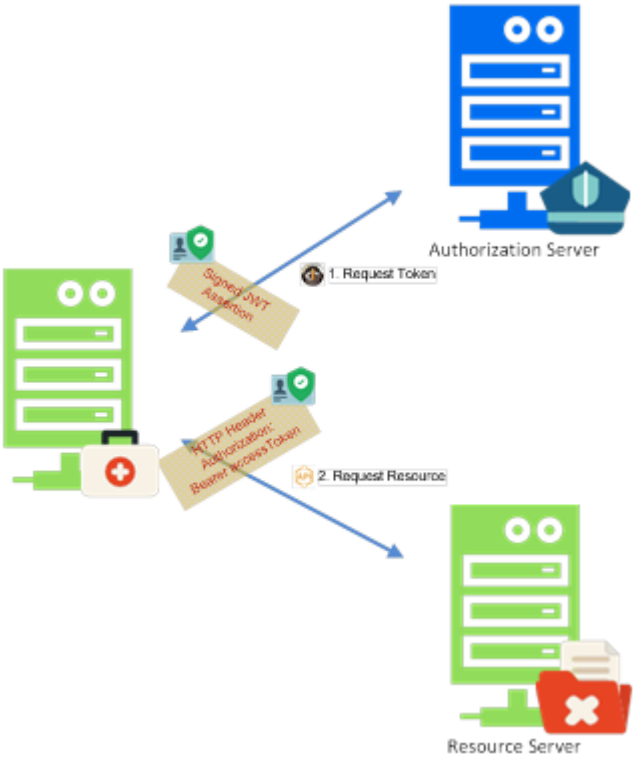
## 2.4. Het project moet één of meerdere types van stromen definiëren uit de voorgestelde lijst

### 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)

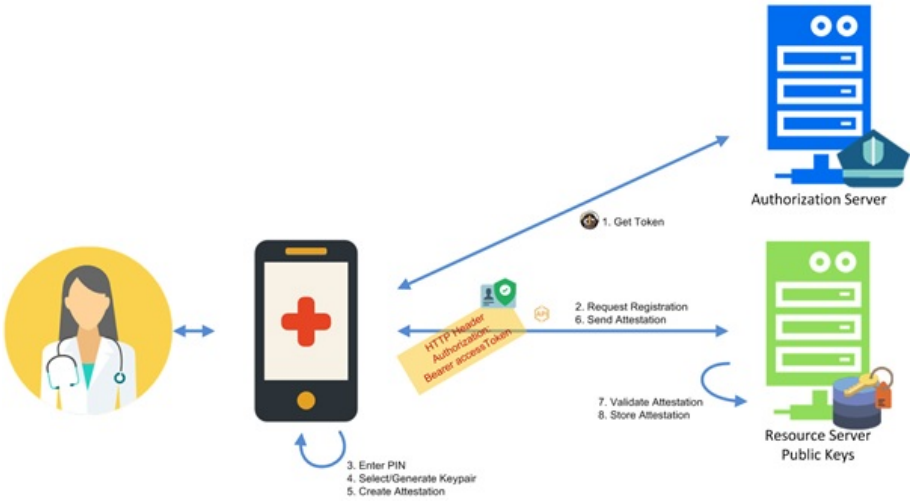
### 2.4.1.3. een toepassing die geen menselijke tussenkomst vereist en die bedoeld is om automatisch te functioneren van server tot server, voor de automatische update van gegevensbanken bijvoorbeeld (system client)



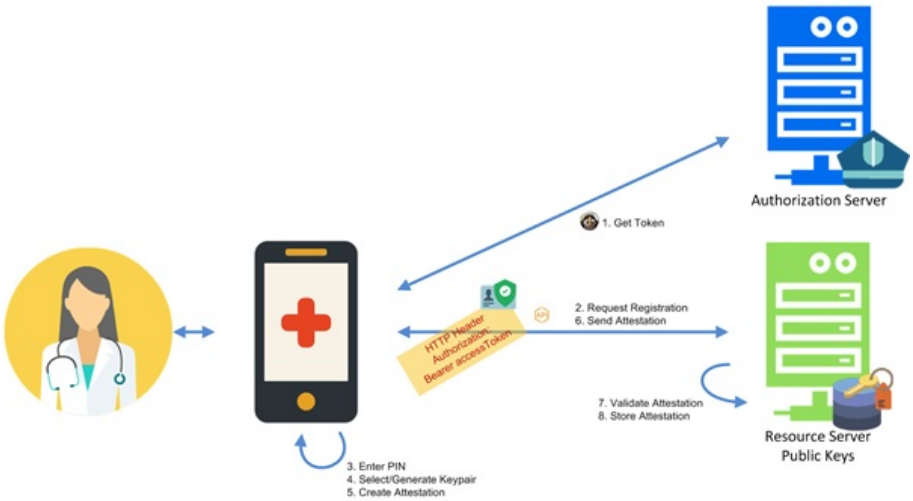
### 2.4.2. Wat betreft het deel 'informatieveiligheid', dient men na te denken over de volgende aspecten:

## 3. Schematische voorstelling use cases

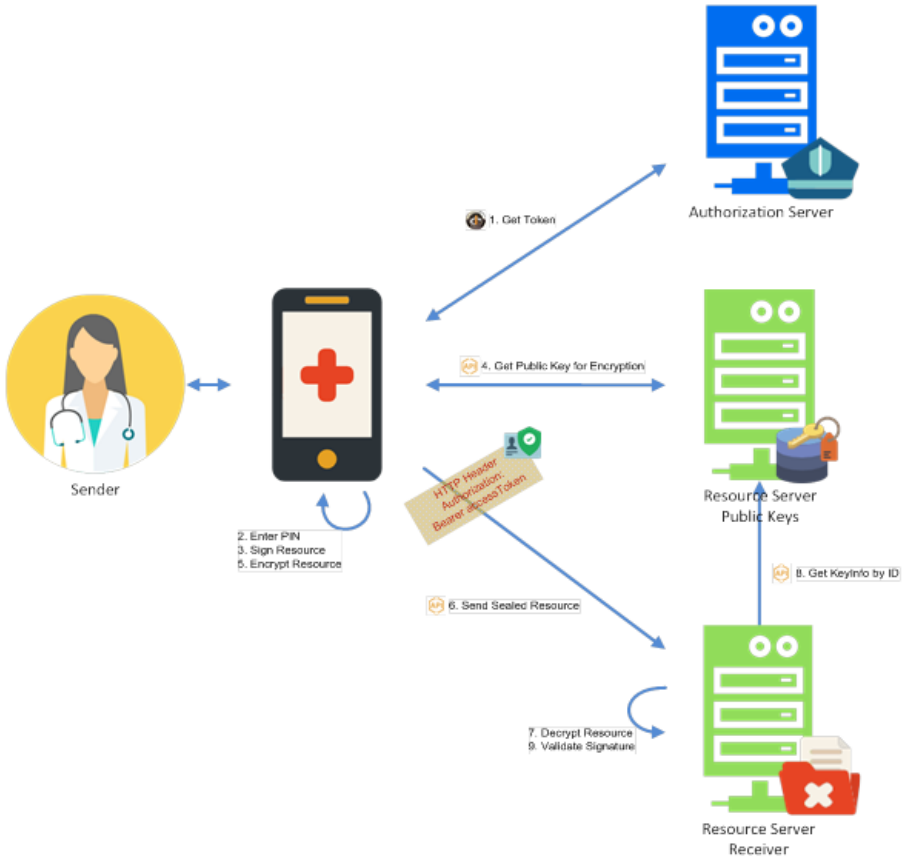
### 3.1. Registratie van een publieke sleutel (use case: registratie van een sleutel in het kader van de aanvraag van een eHealth-certificaat binnen een architectuur van het type SOAP)



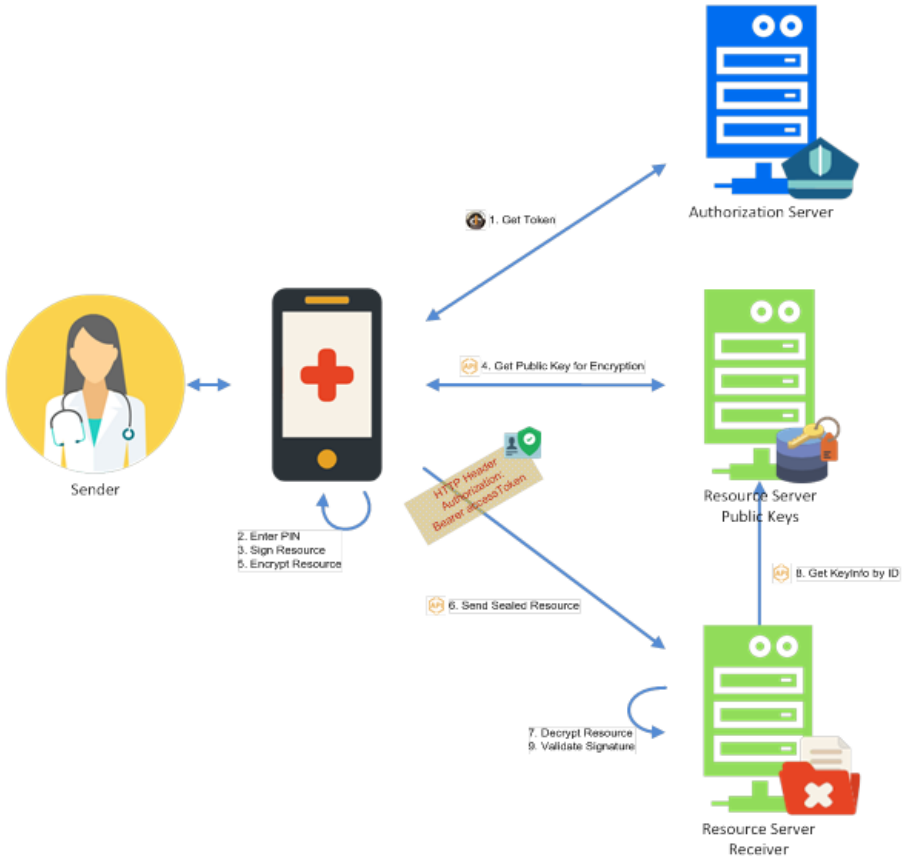

### 3.2. Registratie van een symmetrische sleutel (use case: registratie van een sleutel in het kader van Recip-e)



### 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)