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 juiste registratieformulier gebruiken in functie van de realm:
      Healthcare
      of M2M
  - om de IAM IDP te gebruiken
    - het IAM Registration formulier invullen per omgeving en voorleggen met vermelding van het gekregen certificaat.

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

Meer informatie: support@ehealth.fgov.be

Identity & Access management - Technische organisatie

Inleiding

Het 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.

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

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
- Beveiliging van webservices

De beveiliging van REST Web Service

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

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

Dit type diensten is hoofdzakelijk bedoeld voor mobiele applicaties.

De authenticatie en autorisatie van de klanten gebeurt via de dienst ‘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

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

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.