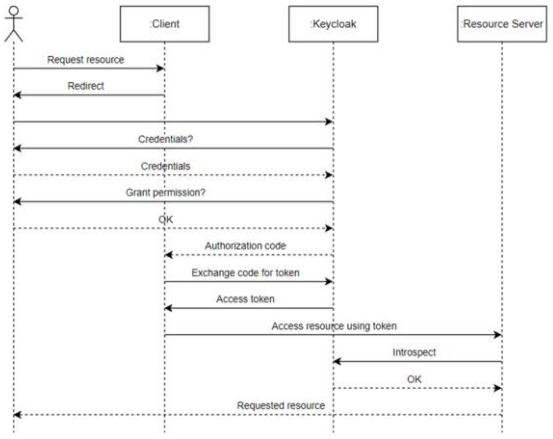
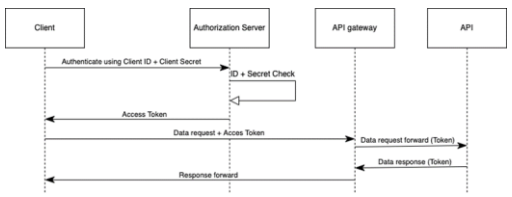
# IAM met OAuth 2.0

## Identity and access management voor microservice-architecturen

Finn Alberts, Lorenzo Clermonts, Giorgio Peerboom, Bram Verheijen en Erik Wingers – studenten te Zuyd Hogeschool Heerlen – Minor Cyber Security




Authorization code flow




Client credentials flow

*Dit project is uitgevoerd binnen de minor Cyber Security van Zuyd Hogeschool, Heerlen in samenwerking met CGI Maastricht.*

**Procesbegeleider:** Daniël Heynen
**Opdrachtgever en inhoudelijke begeleiders:** Marcel Perdok en Maurice Wollersheim

**Zuyd Hogeschool**
Nieuw Eyckholt 300, 6419 DJ Heerlen
T +31 (0)45 400 6400
www.zuyd.nl

**AANLEIDING**
Steeds meer systemen worden gedistribueerd ontwikkeld met microservices. Deze manier van ontwikkelen brengt nieuwe uitdagingen met zich mee op gebied van identity and access management (IAM). Waar voorheen een perimeter-based aanpak geschikt was, wordt tegenwoordig gewerkt met een zero-trust model.

Vanuit CGI Maastricht is de wens om meer kennis en ervaring op dit gebied te vergaren. Om dit op een praktijkgerichte manier uit te voeren, wordt hierbij een vaccinatieregister als voorbeeld genomen.

**DOELSTELLING**
Het doel van dit project is het vergaren van kennis en ervaring over IAM met een zero-trust model en de implementatie hiervan.

**AANPAK**
Er is gewerkt met een iteratieve, op agile gebaseerde, werkwijze.

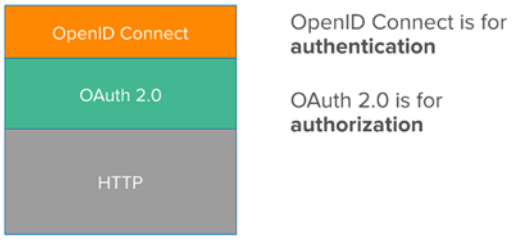
Hierbinnen zijn eerst requirements verzameld voor een vaccinatie-register om hiermee een context te schetsen. Deze zijn geprioriteerd met de MoSCoW-methode.

Vervolgens is een uitgebreid ontwerp gemaakt middels Kruchten 4 + 1. Hierin is ook een security view opgesteld met daarin de cross-cutting security concerns.

Tot slot is een zeer versimpeld prototype van een vaccinatie-register gerealiseerd om hands-on met IAM te kunnen experimenteren.

**RESULTATEN**
Op basis van de requirements is het systeem ontworpen. De belangrijkste view voor dit project is de security view.

Het hoofdpunt van de security view zijn de twee te gebruiken flows binnen OAuth 2.0 en OpenID Connect. OAuth 2.0 en OpenID Connect zijn open protocollen voor IAM.




De gebruikte flows zijn de authorization code flow voor de autorisatie van gebruikers en de client credentials flow voor de autorisatie van microservices. De flows zijn aan de linkerkant te zien.

Deze flows leveren uiteindelijk een access token op. Voor de vorm van deze token is gekozen voor een Opaque Token. Deze token is slechts een simpele code en bevat niet de rechten van de gebruiker. De eindapplicatie kan met deze token terug naar de autorisatieserver om de rechten op te halen.

In het prototype wordt aangetoond hoe met een access token de rechten worden verleend en hoe toegang wordt geblokkeerd als een actor geen rechten heeft.

**CONCLUSIE**
Middels het prototype en het ontwerp is meer kennis verzameld over IAM met microservices als uitgangspunt. Er zijn nog verschillende mogelijkheden voor vervolgonderzoek, voornamelijk om meer praktijkervaring op te doen.

Zuyd Research