Afstemming team Haal Centraal – team NLX

Aanwezig	Eelco Hotting Arnoud Quanjer Timen Olthof Bart Jeukendrup Bert Oldenburger André van den Nouweland Jascha Gregorowitsch Kevin Rijs Melvin Lee Johan Boer Cathy Dingemanse Brenda de Graaf
Datum	25 april 2019
Onderwerp	Autorisatie

Afspraken en afstemming NLX Haal Centraal

Introductie en voorstellen

- Eelco Hotting, Strateeg VNG-Realisatie en CISO gemeente Haarlem
- Arnoud Quanjer, informatiearchitect VNG Realisatie
- Timen Olthof, IT Strateeg Common Ground
- Bart Jeukendrup, Founder Delta10
- Brenda de Graaf , Programmamanager Haal Centraal & Concernadviseur CIO Gemeente Den Haag
- Cathy Dingemanse, Product Owner Haal Centraal & Concernadviseur CIO Gemeente Den Haag
- Melvin Lee, software developer Haal Centraal
- Johan Boer, API designer VNG-Realisatie
- Bert Oldenburger, security expert gemeente Den Haag
- Jascha Gregorowitsch, technisch directeur Enable-U
- Kevin Rijs, developer Enable-U

Aanleiding

Naar aanleiding van de vorige Expertmeeting op 30 januari in Den Haag was nog onduidelijkheid rondom autorisatie. Deze meeting is de follow up en gaat over hoe autorisatie zou moeten werken in een service georiënteerde architectuur met gebruik van NLX, en de impact daarvan op de API's van Haal Centraal.

Aanleiding voor de meeting is de suggestie van Eelco uit het NLX team om autorisatie te laten uitvoeren door de validatie van het request door een autorisatieserver (bijvoorbeeld van een gemeente). N.a.v. deze suggestie worden twee scenario's besproken.

Scenario 1: request validatie in een peer-to-peer architectuur

Hierbij wordt gecontroleerd of de applicatie/gebruiker (bijv. een binnengemeentelijke afnemer) de vraag mag stellen die m.b.v. fields en expand parameters zo is samengesteld dat het antwoord binnen de autorisatie zou moeten vallen. Dit gevalideerde request zou dan over organisaties heen kunnen worden verstuurd naar de provider (bijv. een landelijke registratie) die dit verzoek kan beantwoorden. Daarbij is het uitgangspunt dat NLX is gebaseerd op een “peer tot peer” architectuur, waarbij de NLX Inway van een landelijke registratie rechtstreeks communiceert met de NLX Outway van een binnengemeentelijke consumer. Voordeel hiervan is dat er nooit meer gegevens worden opgevraagd dan de eindgebruiker nodig heeft/ waarvoor de eindgebruiker doelbinding heeft.

Scenario 2: response filtering conform REST architectuurstijl Layered System constraint

Cathy licht toe dat de Haal Centraal API’s zich zo veel mogelijk conformeren aan de REST architectuurstijl. Uitgangspunt zijn de REST constraints, waaronder “Layered System”. Dit houdt in dat er een “message path” is gedefinieerd met intermediaire end points die ieder binnen hun eigen stuk van de keten een eigen taak uitvoeren. Zo ook in de afhandeling van autorisatie. Geen enkele laag (met end point) kan over de volgende laag heen kijken. Lagen kunnen worden toegevoegd, weggehaald, vernieuwd etc. naar gelang de ontwikkeling van de implementatie, zonder impact voor andere lagen (zoals afnemersapplicaties). Een van de voordelen van deze architectuur is dat voor het afhandelen van bepaalde, meestal security gerelateerde taken, standaard producten kunnen worden ingezet (en ingewisseld voor andere!) zoals de NLX of een API Gateway van een grote leverancier. Een dergelijk product kan als intermediate endpoint worden ingezet tussen provider en consumer, zodat de laatsten worden ontzorgd.
Zo kan ook de binnengemeentelijke autorisatie voor de Haal Centraal API’s via een intermediate endpoint worden afgehandeld, waarbij de gemeente met een gemeentelijke autorisatie gegevens opvraagt bij een landelijke registratie, en een gemeentelijke provider (intermediate endpoint) de landelijke response filtert voor binnengemeentelijke consumers o.b.v. de rechten van eindgebruiker of applicatie. Voordeel hiervan dat de (binnengemeentelijke en landelijke) provider binnen de eigen verantwoordelijkheid volledige regie heeft op de autorisatie, weliswaar beperkt tot het eigen deel van de keten.

Afwegingen

- Nadeel van een binnengemeentelijk intermediate endpoint is dat er bij de landelijke registratiemeer informatie kan worden opgevraagd dan dat de eindgebruiker nodig heeft. Dit is met name het geval wanneer een consumer applicatie meerdere autorisaties van eindgebruikers moet ondersteunen. Wanneer voor een taakapplicatie voor alle eindgebruikers dezelfde gegevens moet opvragen, is het eenvoudig om het request m.b.v. fields en expand parameters exact af te stemmen op de eindgebruikersbehoefte.
  Opgemerkt wordt dat het teveel aan opgevraagde gegevens niet door personen wordt gezien.
- Nadelen van het request validatie scenario zijn:
  - dat voor iedere nieuw rechtenprofiel een nieuw request moet worden ontwikkeld, hetgeen voor complexiteit bij de consumer zorgt (deployments, request generatoren

etc..). Dit is in tegenspraak met de doelen van Haal Centraal. Haal Centraal wil consumers ontzorgen door complexiteit bij voorkeur bij de provider te beleggen (hefboomwerking), in dit geval door de introductie van een binnengemeentelijk intermediate endpoint waarbij de autorisatie centraal i.p.v. decentraal wordt afgehandeld.
    - dat 'landelijke registraties een secure relatie moeten hebben met alle gemeentelijke autorisatieservers, bijvoorbeeld om OAuth tokens te valideren (zie OAuth 2.0 specs)
    - dat er bij de aanwezigen geen standaard producten bekend zijn die autorisatie afhandelen m.b.v. request validatie. Daarnaast heeft deze voorziening dezelfde kennis van het domein nodig als een provider die autorisatie uitvoert.

Conclusies autorisatie

- Het is een misverstand dat de NLX volledig is gebaseerd op een "peer to peer" architectuur. Layered System wordt wel degelijk ook met NLX toegepast.
- Door consumers moet altijd worden gestreefd om het request af te stemmen op de informatiebehoefte/autorisatie van de binnengemeentelijke afnemer, tenzij dit voor complexiteit en beheerlast zorgt in de afnemende applicatie omdat meerdere en wisselende rechten van eindgebruikers moeten worden ondersteund. Hierdoor worden in verreweg de meeste gevallen niet meer gegevens opgevraagd dan nodig is. Het gebruik van een binnengemeentelijk endpoint voor autorisatie doet hier niets aan af. Wanneer wel meer gegevens bij een landelijke voorziening worden opgevraagd dan de eindgebruiker nodig heeft, komen deze de gebruiker niet onder ogen door filtering op het intermediate endpoint.
- De introductie van een binnengemeentelijk intermediate endpoint die autorisatie afhandelt lijkt een werkbare methode voor gemeenten.

Logging

- Logging van request, response en doelbinding wordt door NLX zowel in de inway als de outway gefaciliteerd.
- Cathy geeft aan dat het voor de Haal Centraal BRP API voldoende is om in de inway te loggen (aan providerzijde) mits eindgebruiker credentials in het request worden meegegeven. De provider legt zowel het request van de consumer met daarbij de credentials van de eindgebruiker als de daadwerkelijke verstrekking vast. Alles wat je centraal logt hoef je niet decentraal te loggen (efficiënter, goedkoper).
  De consumerapplicatie zal alleen zelf moeten loggen of protocolleren als door de consumer applicatie geen eindgebruiker credentials worden meegegeven, maar gebruik maakt van een service account (legacy applicaties).
- Arnoud geeft aan dat de outway ook verplicht logging moet bijhouden gedurende de migratieperiode naar een service georiënteerde architectuur.

Communicatie

Het Haal Centraal team heeft de mogelijkheid gehad om drie expertsessies met het NLX team bij te wonen. Brenda merkt dat voor veel mensen in overheidsland de NLX uiteenlopende wensdromen

lijkt te vervullen en raadt aan om aan verwachtingenmanagement te doen. Communiceer wat NLX is, wat het niet is, waar het gemeenten in ontzorgt en wat zij zelf nog moeten organiseren. Het NLX team geeft aan dat er vier communicatie experts van Osage zijn ingehuurd, o.a. om de verwachtingen rondom NLX af te stemmen op de realiteit. Daarnaast werk Arnoud Quanjer aan een stuk over NLX.