



Aansluitvoorwaarden WS Gateway Externe Consumer

Auteur:	André van den Nouweland / Michiel Jaeger
Datum:	4 december 2018
Versie:	2.7



1. Inleiding

1.1. Doel en omschrijving

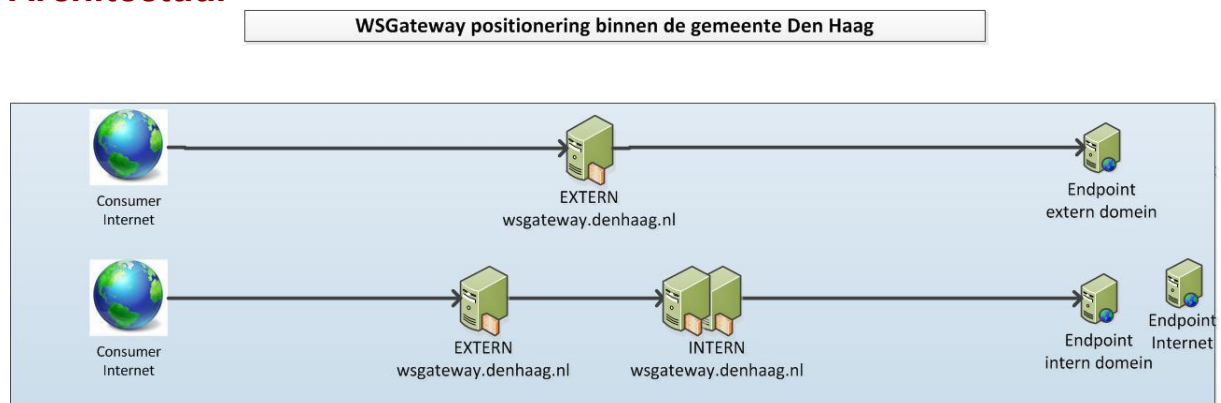
Vaststellen van voorwaarden waaraan een “*externe consumer*” moet voldoen om te kunnen koppelen aan een webservice via de WS Gateway.

1.2. Doelgroep

We onderscheiden de volgende doelgroepen:

- Leveranciers afnemende applicaties buiten de gemeente (*externe consumer*)
- Functioneel beheerders
- Projectleiders.

2. Architectuur



Bij het aansluiten van een webservice wordt er door Team Applicatie Integratie en IDC/TAB gekeken aan welke WS Gateway de webservice wordt gekoppeld. Dit is afhankelijk van de locatie waar zowel de afnemende applicatie als de webservice zich bevinden. Deze informatie wordt in het aanvraagformulier opgenomen.

*) Voor meer informatie over de Haagse architectuur verwijzen we naar document [Aansluitvoorwaarden E-infrastructuur](#) (Alleen interne medewerkers)

3. Scope

Dit document beschrijft de aansluitvoorwaarden voor het openstellen van gepubliceerde webservices op de WS Gateway aan “*externe consumers*”, waarbij de afnemende applicatie buiten de gemeente staat. In de paragraaf “Architectuur” staat een korte impressie hoe de WS Gateway is gepositioneerd binnen de gemeente. De uitgebreide architectuur van de WS Gateway en de gemeente zijn geen onderdeel van dit document. De aansluitvoorwaarden gaan over het ontsluiten van een webservice via de WS Gateway. Hoe webservices inhoudelijk werken, hoe de WS Gateway gebruikt kan worden bij foutmeldingen, het gebruik van *polities* en het gebruik van test tool *SoapUI* valt buiten de scope van dit document.



4. Beveiliging

Een security richtlijn binnen de gemeente is een SSL (https) koppeling naar de WS Gateway (SSL tenzij...). Voor deze SSL koppeling moet het (SHA-2) server certificaat van de WS Gateway op de server van de *consumer* vertrouwd worden. In alle omgevingen is dit een “*certificaat chain*”.

Er is een **externe/interne** beveiliging nodig: een *externe consumer* roept een *provider* binnen de gemeente aan.

Dit is een koppeling met risico's. Dat is de reden waarom de webservice door de externe WS Gateway wordt ontsloten. De locatie van de externe WS Gateway binnen de gemeentelijke architectuur zorgt al voor extra beveiliging. Daarnaast MOET een SSL verbinding met SHA-2 “client-certificaat” worden gebruikt. In alle gevallen waarbij er sprake is van een applicatie-applicatie koppeling wordt de webservice beveiligd op Source-IP. Alleen bij end-user applicaties via bijvoorbeeld mobiele telefoons of in het bijzondere geval dat een publieke webservice wordt aangeroepen, hierbij staat de server van de webservice in het *publieke domein* en zijn de gegevens die worden opgehaald of gemuteerd voor iedereen toegankelijk, kan hiervan eventueel worden afgeweken. Voor de minimale systeemeisen om gebruik te kunnen maken van SHA-2: zie de bijlage Technische voorwaarden.

5. Berichtgrootte

Elke aanbiedende webservice is op de WS Gateway begrensd met een maximale grootte. Bij berichten die deze grens overschrijden zal de WS Gateway een foutmelding geven. De standaard waarde bedraagt 10MB. Het kan zijn dat deze waarde op verzoek van de eigenaar van de betreffende service is verhoogd.

6. Stappenplan aansluiten externe consumer

6.1. Benodigheden

Source-IP van de *consumer* applicatie.

Bij een Soap service zijn de WSDL en schema's in het bezit gebracht van Kenniscentrum Bedrijfsvoeringssystemen/Applicatiekoppelingen.

Formulier consument met toelichting (Alleen interne medewerkers) is bij Team Applicatie Integratie beschikbaar om de *consument* aan te sluiten.

Voor mensen met geen of weinig ervaring met de WSG wordt het aangeraden om eerst een intakegesprek bij Team Applicatie Integratie te plannen.

6.2. TOPdesk melding

Een gemandateerde van de dienst of, indien het een IDC project betreft, IDC/AUT/P&A (hierna: *contactpersoon*) maakt een melding aan in TOPdesk van het Kenniscentrum Bedrijfsvoeringssystemen, URL: <https://aut.topdesk.denhaag.nl>. Het ingevulde formulier wordt aan de melding gekoppeld. De melding wordt dan uitgezet bij Team Applicatie Integratie.

Team Applicatie Integratie neemt bij eventuele vragen contact op met de *contactpersoon* voor deze melding.

6.3. Controle, publicatie

Team Applicatie Integratie bepaalt het resolution path, gaat na of de aanvraag is toegestaan bij de contactpersoon van deze webservice, geeft opdracht aan E-Infra tot publicatie op de WS Gateway en meldt de aanvraag na realisatie af bij de aanvrager.

6.4. Test

De contactpersoon kan de koppeling testen. Team Applicatie Integratie kan hierbij op aanvraag assisteren.



7. Begrippen en afkortingen

Deze sectie beschrijft veel voorkomende begrippen en afkortingen.

7.1. WS Gateway

Dit is de Web Services Gateway (WSG). Het ontkoppelt alle webservices binnen de gemeente van de *consumers* die er gebruik van maken.

7.2. Policy, Policies

Set van regels voor toegang en beveiliging van de WS Gateway. Hierin staan onder andere regels voor gebruik van username/wachtwoord, client certificaat, welke *consumers* wel/niet toegang krijgen, etc.

7.3. Endpoint

Volledige url (adres) om de webservice te benaderen, bijvoorbeeld [https://10.0.0.1/\[webservicepath\]/\[versie\]/webservice.asmx](https://10.0.0.1/[webservicepath]/[versie]/webservice.asmx)

7.4. Resolution path

URL om de webservice via de WS Gateway te benaderen, bijvoorbeeld [http\(s\)://wsgateway-extern.denhaag.nl/\[applicatie\]/\[webservice\]/V\[majorversie\]](http(s)://wsgateway-extern.denhaag.nl/[applicatie]/[webservice]/V[majorversie]). In de WSG heet dit geen endpoint, maar resolution path.

7.5. Majorversie

Linkerdeel van het versienummer (V1.1). Dit deel wijzigt als een nieuwe update de consumer verplicht tot applicatiewijzigingen. Bij webservice wijzigingen waarbij de consumer met de oude wsdl kan blijven koppelen wijzigt alleen de minor versie.

7.6. Minorversie

Rechterdeel van het versienummer (V1.1). Dit deel wordt met 1 verhoogd bij elke kleine webservice update waarbij de consumer met de oude WSDL ongewijzigd kan blijven. De major versie wordt met 1 verhoogd en de minorversie wordt op 0 gezet bij een grote webservice update waarbij alle consumers hun applicatie moeten wijzigen.

7.7. Consumer, Consument, Afnemer

De afnemer van de webservice. Meestal wordt hier de applicatie bedoeld die de webservice benadert.

7.8. Provider, Aanbieder

De webservice. Soms kan ook de server bedoeld worden waar de webservice op geïnstalleerd is.

7.9. Klant

De perso(n)en die op het aanvraagformulier staan als *Contact*.

7.10. Interne consumer, Interne afnemer

De afnemende applicatie staat binnen de gemeente en heeft te maken met de Haagse Architectuur.

7.11. Externe consumer, Externe afnemer

De afnemende applicatie staat buiten de gemeente.

7.12. WS Gateway intern

De interne WS Gateway ontsluit webservices binnen het koppelvlak interne *consumers* / *providers*.

7.13. WS Gateway extern

De externe WS Gateway ontsluit webservices voor het koppelvlak externe *consumers* / *providers*.

7.14. Source-IP

Dit is het IP-nummer van de server waar de webservice daadwerkelijk wordt aangeroepen.

7.15. Publieke domein

Ook wel anonieme domein genoemd. Dit is een omgeving binnen de gemeente waar niet-kritische servers staan. De beveiliging is minder zwaar. Voor koppelingen zijn de beveiligingseisen minder en deze zijn makkelijker en sneller te implementeren.



7.16. SoapUI

Tool om webservices te benaderen via request/response berichten. Het kan gebruikt worden bij nieuwe en bestaande webservices voor een eerste koppeling, voor fouten zoeken, performance testen, integratietesten, etc.

7.17. Architectuur

Beschrijft alle belangrijke componenten en legt het verband ertussen.

7.18. Certificaat chain

Een boom van certificaten, waarbij het 1^e certificaat (root) door een erkende partij is uitgegeven en wordt gebruikt voor het *tekenen* (signen) van het volgende certificaat, enz. De boom bestaat over het algemeen uit 3 of 4 certificaten: root certificaat, 1 of 2 intermediate certificaten en het te gebruiken certificaat.

7.19. Intern certificaat

Certificaat dat binnen de gemeente (self-signed) is aangemaakt voor een specifieke toepassing.



Bijlage Technische voorwaarden

De consumer moet het endpoint via de Web Services Gateway (het resolution path) kunnen benaderen, hieronder een voorbeeld hoe dit getest kan worden:

OT omgeving vanuit consumer:

- telnet wsgateway.ot.denhaag.nl 443

A+P omgeving vanuit consumer:

- telnet wsgateway-extern(.acc).denhaag.nl 443

Om een connectie met de Web Services Gateway te maken met een SHA2 certificaat is het volgende nodig:

- Certificaten van de Web Services Gateway (deze worden op aanvraag toegezonden)
- Systeemeisen aan de server;
 - Windows Server 2003 SP2 (met hotfix KB 938397 of KB 968730)
 - Windows Server 2008
 - Unix/Linux: Java versie 1.5.0_08

Alternatieve methode

Naast telnet kan het volledige resolution path ook via de browser benaderd worden: Bijvoorbeeld via <https://wsgateway.ot.denhaag.nl/<relatieve resolution path>?wsdl>

Als er een UNAUTHORIZED melding komt ("This request requires HTTP authentication") dan is de service actief. Een browsermelding dat de pagina niet gevonden kan worden houdt in dat de service nog niet actief is.

Het is mogelijk via de browser het servercertificaat te exporteren. Bij de UNAUTHORIZED melding kunnen in de browser het certificaat of de certificaten worden weergegeven. Indien de beveiliging van de browser het toelaat kunnen certificaten naar een bestand geëxporteerd worden.

Cliënt certificaten

Als een consument buiten Den Haag wil aansluiten op de WS Gateway *OF* dat vanwege hoge data classificatie de aanbieder partij een cliënt certificaat vereist, zal deze door de consument moeten worden gemaakt. Het certificaat moet voldoen aan de volgende voorwaarden:

- SHA256 hashing-algoritme
- RSA 2048 sleutellengte

Zie de [URL](#) van Logius voor meer informatie over certificaten: welke hiërarchie heeft PKI-overheid en aan welke eisen moet een certificaat voldoen. Het wordt aangeraden om een PKI-overheid-certificaat te gebruiken.

<https://logius.nl/diensten/pkioverheid>