



# Aansluitvoorwaarden WS Gateway Provider

|         |                                          |
|---------|------------------------------------------|
| Auteur: | André van den Nouweland / Michiel Jaeger |
| Datum:  | 2-10-2017                                |
| Versie: | 3.5                                      |



## Inhoud

|         |                                                                       |    |
|---------|-----------------------------------------------------------------------|----|
| 1       | Inleiding .....                                                       | 3  |
| 1.1     | Doel en omschrijving .....                                            | 3  |
| 1.2     | Doelgroep .....                                                       | 3  |
| 2       | Architectuur.....                                                     | 3  |
| 3       | Scope .....                                                           | 4  |
| 4       | Welke WS Gateway ? .....                                              | 4  |
| 5       | Berichtgrootte .....                                                  | 4  |
| 5.1     | Standaard berichten.....                                              | 4  |
| 5.2     | Grote XML berichten (zonder bijlages) .....                           | 4  |
| 5.3     | Grote berichten met bijlages.....                                     | 5  |
| 5.4     | Matrix berichtgrootte.....                                            | 5  |
| 5.5     | Matrix restricties grote bestanden webservice provider/afnemers ..... | 6  |
| 6       | Beveiliging .....                                                     | 7  |
| 6.1     | Algemeen.....                                                         | 7  |
| 6.2     | Soorten beveiliging.....                                              | 7  |
| 6.2.1   | algemeen .....                                                        | 7  |
| 6.2.2   | custom intern/intern publiek (anoniem).....                           | 7  |
| 6.2.3   | standaard intern/intern beveiligd .....                               | 7  |
| 6.2.4   | custom intern/intern beveiligd .....                                  | 7  |
| 6.2.5   | extern/intern .....                                                   | 7  |
| 7       | Stappenplan Provider .....                                            | 8  |
| 7.1     | Benodigdheden .....                                                   | 8  |
| 7.2     | TOPdesk melding.....                                                  | 8  |
| 7.3     | Controle, publicatie en test .....                                    | 8  |
| 8       | Web API -RESTful services .....                                       | 9  |
| Bijlage | Begrippen en afkortingen.....                                         | 10 |
| Bijlage | Technische voorwaarden .....                                          | 12 |



## 1 Inleiding

### 1.1 Doel en omschrijving

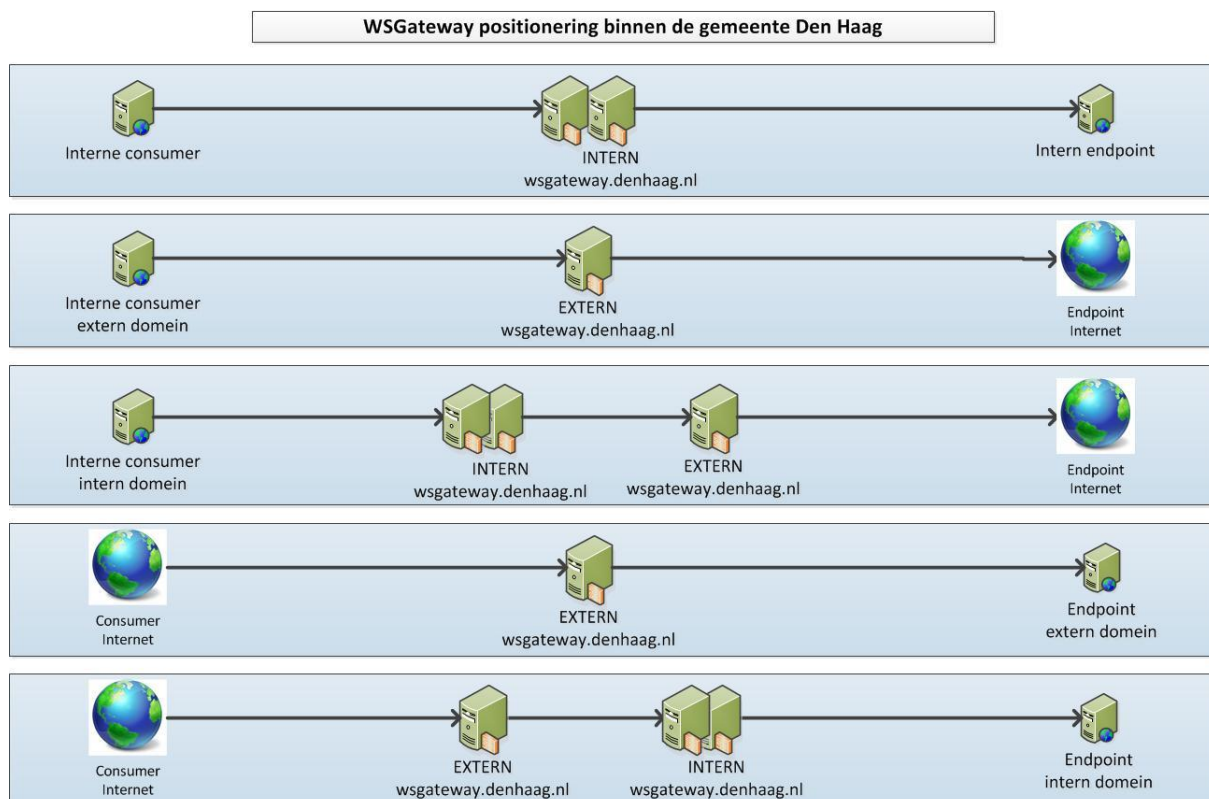
Vaststellen van voorwaarden waaraan een webservice “*provider*” moet voldoen om een webservice ontsloten te krijgen op de *WS Gateway*.

### 1.2 Doelgroep

Dit document is primair geschreven voor de volgende doelgroepen:

- Applicatie-bouwers en -beheerders (in de tekst verder aangeduid als “leveranciers” van webservice)
- Functionele beheerders
- Projectleiders van de diensten
- Projectleiders en adviseurs van IDC-A/P&A

## 2 Architectuur





Bij het aansluiten van een webservice wordt er door Applicatiekoppelingen (A.k.) 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

[ICT Architectuur](#)

## 3 Scope

Dit document beschrijft de aansluitvoorwaarden voor de publicatie van webservices op de WS Gateway (provider). 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 *polices* en het gebruik van test tool *SoapUI* valt buiten de scope van dit document.

## 4 Welke WS Gateway ?

Er zijn meerdere WS Gateways, zoals beschreven in de paragraaf “Architectuur”.

Applicatiekoppelingen helpt mee te bepalen waar de webservice staat en of de ontsluiting mag op de juiste WS Gateway.

## 5 Berichtgrootte

De WS Gateway staat zo ingesteld dat de maximale totale grootte van het bericht wat van en naar de WS Gateway wordt gestuurd 10MB bedraagt. Dit houdt in dat een request inclusief eventuele bijlages (MTOM) maximaal 10MB mag zijn en een response inclusief eventuele bijlages (MTOM) ook maximaal 10MB mag zijn. Bij berichten die deze grens overschrijden zal de WS Gateway een foutmelding geven. A.k. kan niet uit de definities halen hoe groot het grootste bericht zal zijn en stelt dus mogelijk geen vraag hierover. Het beste kunt u zelf even de matrix berichtgrootte van paragraaf 5.4 raadplegen om te kijken of uw berichtenverkeer voldoet aan de voorwaarden. Als ‘streamed’ niet specifiek staat aangegeven is het de standaard ‘Buffered’ variant.

### 5.1 Standaard berichten

Als u berichten heeft die, eventueel inclusief bijlages, nooit groter zullen zijn dan 10MB hoeft u zich geen zorgen te maken en kunt u verder naar paragraaf 6.

### 5.2 Grote XML berichten (zonder bijlages)

Heeft u het zeldzame geval dat u berichten groter dan 10MB moet versturen of ontvangen en het betreft een bericht zonder bijlages (inline), dan zal TAI u conform de tabel van paragraaf 5.4, doorverwijzen naar de Toetsingscommissie. Hiervoor zal door de klant een onderbouwing moeten



worden aangeleverd. A.k. zal hieraan restricties volgens de tabel van paragraaf 5.5 toevoegen, dit om de resources van de WS Gateway te beschermen.

### 5.3 Grote berichten met bijlages

TAI geeft altijd het advies om bij berichten met bijlages de standaard MTOM te gebruiken. Bij berichten van 10MB tot 1GB wordt de z.g. 'MTOM streamed' variant gevraagd. Anders zult u bij berichten tot 100MB door TAI worden doorverwezen naar de toetsingscommissie en uw verzoek zal vanwege de technische beperkingen worden afgewezen bij berichten groter dan 100MB.

### 5.4 Matrix berichtgrootte

| <b>Bericht/Grootte</b>                                     | <b>0-10MB</b>         | <b>10-100MB</b>           | <b>100MB-1GB</b>        | <b>&gt; 1GB</b>         |
|------------------------------------------------------------|-----------------------|---------------------------|-------------------------|-------------------------|
| <i>Zonder bijlages – standaard (buffered)<sup>1)</sup></i> | Akkoord               | Toetsing <sup>6)</sup>    | Afgekeurd <sup>7)</sup> | Afgekeurd <sup>7)</sup> |
| <i>Met bijlages inline <sup>3)</sup></i>                   | Akkoord <sup>5)</sup> | Toetsing <sup>5) 6)</sup> | Afgekeurd <sup>7)</sup> | Afgekeurd <sup>7)</sup> |
| <i>Met bijlages inline streamed <sup>2)</sup></i>          | Akkoord <sup>5)</sup> | Toetsing <sup>6)</sup>    | Afgekeurd <sup>8)</sup> | Afgekeurd <sup>8)</sup> |
| <i>Met bijlages MTOM <sup>4)</sup></i>                     | Akkoord               | Toetsing <sup>6)</sup>    | Afgekeurd <sup>7)</sup> | Afgekeurd <sup>7)</sup> |
| <i>Met bijlages MTOM streamed <sup>2)</sup></i>            | Akkoord               | Akkoord                   | Akkoord                 | Toetsing <sup>6)</sup>  |

**Legenda:**

- 1) Buffered: standaard zal het hele bericht worden verzameld en in zijn geheel worden verstuurd. Effect zal zijn dat het volledige bericht zowel in het geheugen van de client als van de WS Gateway wordt opgeslagen.
- 2) Streamed: het bericht wordt in pakketjes verdeeld en direct doorgestuurd. Deze methode zorgt ervoor dat het geheugengebruik minimaal blijft.
- 3) Inline: de bijlage(s) zitten in de request en worden samen met de rest van de XML verstuurd.
- 4) MTOM: de bijlage(s) zitten apart van de XML request in een aparte 'Mime'. Het bericht wordt nog via de standaard 'Buffered' methode verstuurd.
- 5) A.k. zal voor pakketten adviseren MTOM als standaard te volgen. Voor maatwerk is het dringende advies MTOM als standaard te volgen.
- 6) Hierbij is een goede onderbouwing nodig waarom deze specifieke aansluiting nodig is en de andere alternatieven niet voldoen. Bij goedkeuring zijn WS Gateway restricties nodig.
- 7) Deze is technisch en dus permanent afgekeurd. De WS Gateway heeft te weinig resources om dit aan te kunnen.
- 8) Vanwege security afgekeurd. Het risico van bijvoorbeeld per ongeluk aanzetten logging met als gevolg gebufferde request logging inclusief inline bijlage en een instabiele WS Gateway tot gevolg is te groot.



## 5.5 Matrix restricties grote bestanden webservice provider/afnemers

De volgende tabel bevat restricties die A.k. tijdens publicatie van de service aan de webservice provider moet opleggen en waar afnemers rekening mee moeten houden bij het versturen van grote bestanden via buffered of streamed methode. MTOM is hier niet van belang. MTOM is de standaard die A.k. voorschrijft om bijlages te versturen of te ontvangen. Daarnaast geeft MTOM de mogelijkheid om de WS Gateway met behulp van extra 'policies' beter te configureren voor maximale grootte van het XML bericht en de bijlages. Het heeft géén invloed op de gevolgen als er grote bestanden worden getuurd.

Note: de WS Gateway kan via policy assertions begrensd worden ter voorkoming van instabiel gedrag bij grotere berichten. Op het moment van schrijven is nog geen definitieve configuratie bekend. Zodra de exacte instellingen bekend zijn, wordt dit document hierop aangepast.

| Bericht/Grootte     | Restricties                                                              | Gevolgen/Opmerkingen                                                                                                                                                                                                                                   |
|---------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Buffered tot 10MB   | NVT                                                                      | NVT                                                                                                                                                                                                                                                    |
| Buffered 10MB-100MB | 1-WSG direct buffering (via schijf)<br>2-Begrensd via policy assertions. | 1-Responsetijd neemt toe<br>2-Via policy assertions wordt de WS Gateway zodanig ingesteld dat deze service geen of weinig invloed heeft op resources en het gebruik van de andere services door andere consumenten. Dit kan performance verlies geven. |
| Buffered >100MB     | NVT                                                                      | WSG heeft te weinig resources om dit aan te kunnen                                                                                                                                                                                                     |
| Streamed tot 10MB   | NVT                                                                      | NVT                                                                                                                                                                                                                                                    |
| Streamed 10MB-1GB   | 1-WSG direct streaming                                                   | Berichten > 1GB worden bij bereiken van 1GB geweigerd.                                                                                                                                                                                                 |
| Streamed >1GB       | 1-WSG direct streaming<br>2-Begrensd via policy assertions               | 2-Via policy assertions wordt de WS Gateway zodanig ingesteld dat deze service geen of weinig invloed heeft op resources en het gebruik van de andere services door andere consumenten. Dit kan performance verlies geven.                             |



## 6 Beveiliging

### 6.1 Algemeen

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 de testomgeving is dit 1 self signed certificaat. In de Acceptatie en Productie omgeving is dit een “*certificaat chain*” (PKI-overheid).

Zie de bijlage “*Technische voorwaarden*” voor verdere informatie hierover.

### 6.2 Soorten beveiliging

#### 6.2.1 algemeen

Afhankelijk van de locatie van de consumer en de provider (binnen de gemeente, buiten de gemeente) en van of de webservice gevoelige informatie ontsluit, zoals de kernregistraties doen, onderscheiden we de volgende typen beveiliging

- custom intern/intern publiek;
- standaard intern/intern beveiligd;
- custom intern/intern beveiligd;
- extern/intern beveiligd.

#### 6.2.2 custom intern/intern publiek (anoniem)

De WS Gateway webservice mag wat betreft de *architectuur* door iedereen binnen de gemeente worden aangeroepen. Dit kan een koppeling zonder beveiliging zijn. De WS Gateway hoeft dan geen extra beveiliging in te stellen. De gegevens die de webservice ontsluit kunnen echter wel extra beveiliging nodig hebben, dit ter beoordeling van de klant. In dat geval wordt het een intern/intern beveiligde koppeling.

#### 6.2.3 standaard intern/intern beveiligd

De WS Gateway webservice kan alleen door *consumers* die over de juiste beveiliging beschikken binnen de gemeente worden aangeroepen. Er is gekozen voor minimaal een SSL verbinding en beveiliging op basis van het alleen toestaan van connectie vanaf een of meer bepaalde source-IP adressen.

#### 6.2.4 custom intern/intern beveiligd

De WS Gateway webservice kan ook hier alleen door *consumers* die over de juiste beveiliging beschikken binnen de gemeente worden aangeroepen. De gekozen beveiliging wijkt af van de standaard. Er kan gekozen worden uit intern certificaat, WS-Security (incl. UserNameToken en/of Kerberos ticket en/of SAML token) of andere soorten beveiliging. Applicatiekoppelingen kan hierin adviseren en zal de gekozen beveiliging toetsen.

#### 6.2.5 extern/intern

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 wordt de webservice beveiligd op Source-IP.

Alleen 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.

## 7 Stappenplan Provider

### 7.1 Benodigdheden

- 1) *Endpoint webservice*. Deze moet beschikbaar en benaderbaar zijn.
- 2) Webservice interface bestanden - WSDL en schema's (SOAP) of eventueel WADL (RESTful),
- 3) Het IP-adres van de server waarop de webservice draait.
- 4) Source-IP *consumer* OF inschatting waar de consumer applicatie draait. Zie ook paragraaf [Beveiliging](#).
- 5) [Formulier webservice](#) met [toelichting](#) (*Alleen interne medewerkers*) is bij *Applicatiekoppelingen* beschikbaar om de webservice aan te sluiten. Voor mensen met geen of weinig ervaring met de WSG wordt het aangeraden om eerst een intakegesprek bij *Applicatiekoppelingen* te plannen.

### 7.2 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://kc.topdesk.denhaag.nl>.

Het ingevulde formulier wordt aan de melding gekoppeld. De XML-bestanden, zowel WSDL(s) als XSD(s), worden bijgevoegd. De melding wordt dan uitgezet bij *Applicatiekoppelingen*.

*Applicatiekoppelingen* neemt bij eventuele vragen contact op met de *contactpersoon* voor deze melding.

### 7.3 Controle, publicatie en test

*Applicatiekoppelingen* bepaalt en controleert resolution path, geeft opdracht aan E-Infra tot publicatie op de WS Gateway, test de koppeling zodra de publicatie is uitgevoerd en meldt de aanvraag af.

Het is mogelijk de import niet in Test maar direct in de WS Gateway Acceptatie uit te voeren, dit op aangeven van de *contactpersoon*. De import in Productie wordt pas uitgevoerd als de import in de WS Gateway Acceptatie is uitgevoerd EN na akkoord van de *contactpersoon*.



### 8 Web API -RESTful services

Dit document gaat uit van het gebruik van het Simple Object Access Protocol (SOAP) voor webservices. De WS Gateway kan naast SOAP ook overige Web API's ontsluiten. Het ondersteunt RESTful services (Representational state transfer). Voor services hanteert de gemeente Den Haag het principe "SOAP, tenzij...". Een ander principe is dat alle webservices via de WS Gateway aangeboden worden, ook die op basis van REST.

Bij de aanvraag voor een RESTful webservice moet een schrijven komen van de leverancier, waarin staat waarom ze voor REST gekozen hebben. De redenen voor de 'tenzij' dus.

Het mandaat om te bepalen of REST in een specifiek geval is toegestaan ligt bij Applicatiekoppelingen. Als het schrijven voldoende geldige redenen bevat om REST te gebruiken dan kan de service door. Bij twijfel zal Applicatiekoppelingen vragen voor onderbouwing en deze eventueel extra laten toetsen binnen de gemeente.

Het is een pré als de leverancier van een RESTful service een WADL bestand kan meeleveren als equivalent van WSDL +XSD's. Dit geeft inzicht in de webservice en vereenvoudigt de publicatie van de service op de WS Gateway. Als alternatief kan ook een swagger document meegeleverd worden.



## **Bijlage      Begrippen en afkortingen**

Deze sectie beschrijft veel voorkomende begrippen en afkortingen.

### **WS Gateway**

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

### **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.

### **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)

### **Resolution path**

De volledige URL om de webservice te benaderen, bijvoorbeeld:

[http\(s\)://wsgateway.denhaag.nl/\[applicatie\]/\[webservice\]/V\[majorversie\]](http(s)://wsgateway.denhaag.nl/[applicatie]/[webservice]/V[majorversie]).

In de WSG heet dit geen endpoint, maar resolution path.

### **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.

### **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.

### **Consumer, Consument, Afnemer**

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

### **Provider, Aanbieder**

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

### **Klant**

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

### **Interne consumer, Interne afnemer**

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

### **Externe consumer, Externe afnemer**

De afnemende applicatie staat buiten de gemeente.

### **WS Gateway intern**

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



### **WS Gateway extern**

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

### **Source-IP**

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

### **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.

### **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.

### **Architectuur**

Beschrijft alle belangrijke componenten en legt het verband ertussen.

### **Certificaat chain**

Een boom van certificaten, waarbij het 1<sup>e</sup> certificaat (root) bij een erkende partij in beheer is.

Dit wordt gebruikt voor het *tekenen* (signen) van het volgende certificaat dat wordt uitgegeven, enz.

De boom bestaat over het algemeen uit 3 of 4 certificaten: root certificaat, 1 of 2 intermediate certificaten en het te gebruiken certificaat.

### **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.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 en hoger
  - Unix/Linux: Java vanaf versie 1.5.0\_08

### **Alternatieve methode**

Naast via 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 mogelijk 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.

Zie voor verdere informatie: de [URL](#) van Logius waar de PKI-Overheid certificaten beschreven staan:

<https://cert.pkioverheid.nl/>