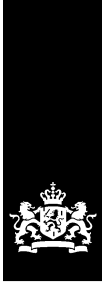


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Servicebeschrijving

Digipoort WUS 2.0 Machtigingraadpleegservice

Versie 1.1

Datum 22 april 2015
Status Definitief

Colofon

Projectnaam	Digipoort
Versienummer	1.1 (Definitief)
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Bijlage(n)

Inhoud

1 Inleiding

1.1 Doel en doelgroep

Dit document beschrijft het ophalen van de informatie over de toestand van opgevoerde machtigingen bij de overheid via Digipoort.

Dit document is bestemd voor ontwikkelaars van programmatuur voor het ophalen van toestandsinformatie van een machtiging bij Digipoort. Het beschrijft hoe gebruik kan worden gemaakt van de betrokken webservice: de Machtigingraadpleegservice.

Verschillen met voorgaande versies

- Oude endpoints/adressen vervangen door nieuwe endpoints
- Toestand "Ontvangen" toegevoegd aan toestandsverloop machtigingen

1.2 Leeswijzer

Dit document maakt onderdeel uit van een reeks documenten die inzicht geven in het gebruik van Digipoort. Dit document beschrijft een service die onderdeel is van het koppelvlak WUS 2.0 van Digipoort.

Deze servicebeschrijving is als volgt opgebouwd:

- Het eerste hoofdstuk bevat algemene informatie als versiehistorie en contactgegevens;
- Het tweede hoofdstuk bevat een globale beschrijving van de werking van het raadplegen van de toestand van een machtiging;
- Het derde hoofdstuk beschrijft de structuur en inhoud van het SOAP-bericht;
- Het vierde hoofdstuk beschrijft de webservice in meer detail.

Als losse bijlagen zijn voorbeelden van SOAP-requests, responses en de detailspecificatie van de webservice (de WSDL) beschikbaar

1.3 Status

Dit document beschrijft een service binnen het WUS 2.0 koppelvlak van Digipoort. De verwachting is dat de gebruikte open standaarden zich de komende jaren verder zullen ontwikkelen en dat de communicatiebehoefte ook aan verandering onderhevig zal zijn. Het gevolg hiervan is dat de komende jaren nieuwe releases van Digipoort in gebruik zullen worden genomen. Dat kan gevolgen hebben voor de koppelvlakken. Logius streeft ernaar om nieuwe releases in nauw overleg met de markt te realiseren. Om het voor marktpartijen snel en eenvoudig mogelijk te maken om gebruik te maken van Digipoort, is er voor gekozen zoveel mogelijk open standaarden en bestaande voorzieningen te gebruiken. Voorbeelden daarvan zijn het gebruik van het SOAP protocol en de toepassing van PKIOverheid certificaten.

1.4 Ondersteuning

Informatie met betrekking tot ondersteuning bij het gebruik van de services van Digipoort is beschikbaar op de website: www.logius.nl/digipoort.

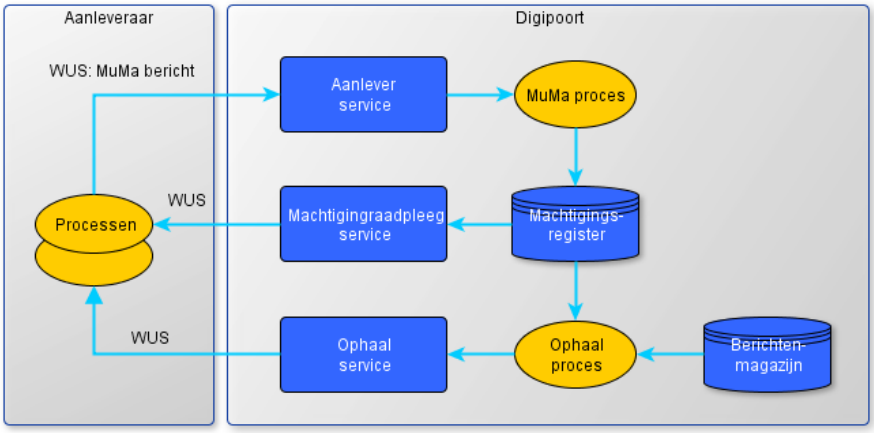
2 Raadplegen van (toestand van) machtigingen

2.1 Inleiding

Dit hoofdstuk geeft een overzicht van het raadplegen van de toestand van machtigingen bij Digipoort. Het opvoeren van een machtiging gebeurt via de Aanleverservice, welke in een apart document is beschreven.

De aanleveraar kan deze informatie opvragen via de machtigingraadpleegservice.

2.2 Overzicht



Figuur 1 Positie Machtigingraadpleegservice binnen Digipoort

Bovenstaand figuur toont een overzicht van de aanroep van de Machtigingraadpleegservice binnen de context van de verwerking van machtigingen op Digipoort. De Aanleveraar is in dit geval de intermediair die aanleveringen voor vertegenwoordigde wil (gaan) uitvoeren.

2.3 Sessiebeschrijving

Via het systeem van de Aanleveraar worden machtigingsmutaties (opvoeren of intrekken) aangeboden aan de Aanleverservice van Digipoort. In een machtigingsmutatie geeft de Aanleveraar aan voor welke dienst en welke vertegenwoordigde hij als gemachtigde wil gaan optreden (opvoeren machtiging) of wil ophouden als gemachtigde op te treden (intrekken machtiging).

De machtigingraadpleegservice ondersteunt een tweetal verzoeken waarmee informatie verkregen kan worden over de toestand van opgevoerde machtigingen, namelijk *getMachtigingToestand* en *getNieuweToestanden*.

Het systeem van de Aanleveraar gebruikt het machtigingsraadpleeg-verzoek *getMachtigingToestand* om op enig moment de toestand van een specifieke machtiging te raadplegen. Dit is alleen mogelijk voor machtigingen die door hem zelf zijn aangeleverd.

Het systeem van de Aanleveraar gebruikt het machtigingsraadpleeg-verzoek *getNieuweToestanden* om een lijst van machtigingstoestanden op te halen waarop mutaties hebben plaatsgevonden die nog niet eerder zijn geselecteerd met hetzelfde verzoek. Een machtigingsmutatie treedt bijvoorbeeld op bij activatie van een machtiging door een succesvolle afronding van het verificatieproces. In dit voorbeeld zijn twee machtigingstoestanden van belang. De eerste machtigingstoestand betreft de toestand voor de mutatie, namelijk "In behandeling". Deze toestand wordt namelijk voorzien van een einddatum. De tweede machtigingstoestand betreft de nieuwe toestand "Actief". De begindatum van deze toestand komt overeen met de einddatum die de eerste machtigingstoestand heeft gekregen.

Als de toestand van de machtiging "Actief" is voor bepaalde combinatie van gemachtigde, vertegenwoordigde en dienst (een zogenaamde "triple") in het machtigingsregister kan er voor deze dienst via Digipoort inhoudelijke gegevensuitwisseling plaatsvinden namens de vertegenwoordigde tussen aangesloten overheidsorganisaties en het systeem van de Aanleveraar.

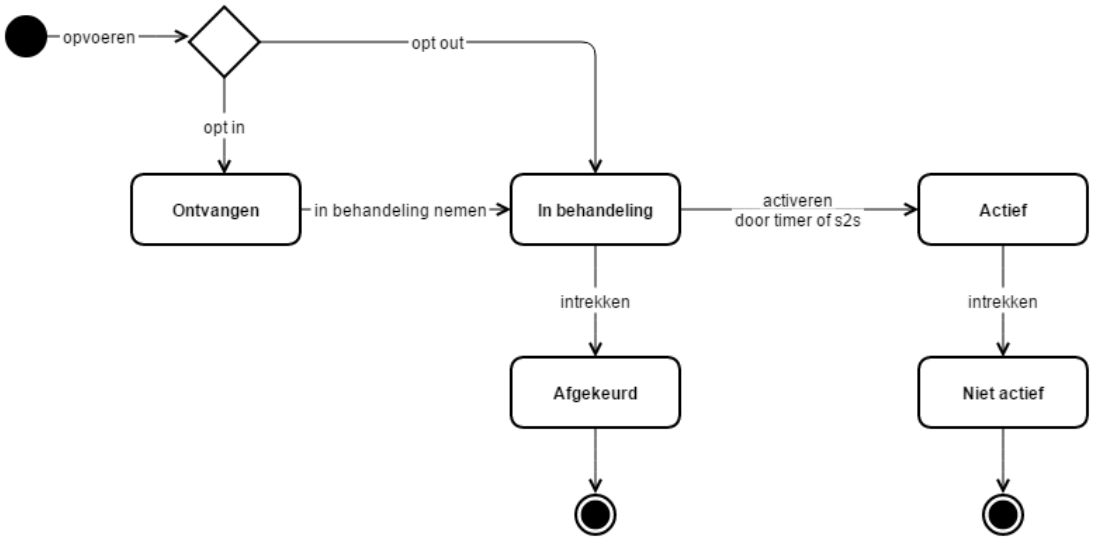
2.4 Beschrijving van actoren

In onderstaande tabel bevindt zich een overzicht van de actoren die een rol spelen in bovenstaande sessiebeschrijving.

Actor	Beschrijving
Aangesloten overheidsorganisatie	Een overheidsorganisatie die bij Digipoort is aangesloten (ontvangende partij).
Aanleveraar	Een intermediair (of bedrijf) die is aangesloten op Digipoort (aanleverende partij).
Gemachtigde	Een partij die optreedt als intermediair en namens één of meerdere vertegenwoordiger(s) berichten kan aanleveren die bestemd zijn voor overheidsorganisaties.
Vertegenwoordigde	Een persoon of organisatie die zich laat vertegenwoordigen door een gemachtigde voor één of meerdere (overheids)diensten.

2.5 Beschrijving toestandsverloop machtigingen

In onderstaande figuur bevindt zich een illustratie van de mogelijke toestandsovergangen.



Figuur 2 Toestandsverloop machtiging

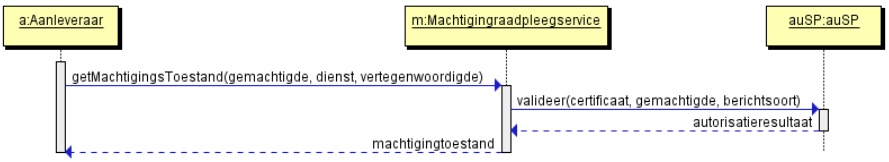
De initiële toestand na het opvoeren van de machtiging is: "Ontvangen" (in het geval van opt in) of "In Behandeling" (in geval van opt out). Een intrekverzoek dat plaatsvindt terwijl de machtiging nog in de toestand "In Behandeling" is, leidt tot de eindtoestand "Afgekeurd".

Als de verificatieprocedure met succes is afgesloten wijzigt de toestand van de machtiging na de zogenaamde opt-out periode van "In behandeling" naar "Actief".

Machtigingen kunnen ook ingetrokken worden en/of diensten kunnen verlopen. Als dit gebeurt terwijl de machtiging in de toestand "Actief" is, treedt de-activatie van de machtiging op. Dit houdt in dat de toestand gewijzigd wordt van "Actief" naar de eindtoestand "Niet actief".

2.6 Aanroep en uitvoering van Machtigingraadpleegservice

In het figuur hieronder is weergegeven hoe de Aanleveraar de Machtigingraadpleegservice aanroept met het verzoek *getMachtigingToestand*.



Figuur 2 Sessieverloop raadplegen van machtigingtoestand

De machtigingraadpleegservice stelt vast of een verzoek voor het raadplegen van de machtiging van een aanleveraar voldoet aan vastgestelde koppelvlakspecificaties.

Indien het verzoek voldoet aan de specificaties, dan haalt de Machtigingraadpleegservice de machtigingstoestand op. De service geeft in een synchroon proces antwoord op dit verzoek. Dit antwoord bevat de gevraagde informatie (SOAP-response) of het bevat de melding dat het verzoek is mislukt (SOAP fault).

De Machtigingraadpleegservice bestaat uit de volgende onderdelen:

- Controleren structuur machtigingsraadpleegverzoek;
- Verwerken van het machtigingsraadpleegverzoek;
- Versturen antwoord van het machtigingsraadpleegverzoek.

Voor het verzoek *getNieuweToestanden* is een overeenkomstig sessieverloop van toepassing.

2.7 Controleren structuur machtigingsraadpleegverzoek

Om gestructureerde berichten aan Digipoort aan te kunnen bieden wordt gebruik gemaakt van een machtigingtoestandverzoek met een voorgedefinieerde structuur. Deze structuur is vastgelegd met de Web Service Definition Language (WSDL). De WSDL voor de Machtigingraadpleegservice is als apart bestand bij de servicebeschrijving bijgevoegd.

Als het bericht niet voldoet aan de eisen gesteld in de WSDL wordt er een SOAP-fault terug gezonden. Als het bericht voldoet aan de eisen, dan wordt het verwerkt.

2.8 Verwerken van het machtigingsraadpleegverzoek

Als een machtigingtoestandverzoek voldoet aan de gestelde eisen, wordt op basis van het certificaat waarmee de elektronische handtekening heeft plaats gevonden bepaald of de informatie door de betreffende aanleveraar mag worden opgehaald.

Er zijn twee SOAP-request van toepassing:

- getMachtigingToestandRequest(identiteitGemachtigde, dienst, identiteitVertegenwoordigde);
- getNieuweToestandenRequest(identiteitGemachtigde, dienst, tijdstempelVanaf, tijdstempelTot).

Aan deze SOAP-requests wordt de endpoint van de AuSP meegegeven die gebruikt dient te worden voor de autorisatie.

In de volgende paragrafen wordt de functionaliteit van de betreffende machtigingsraadpleegverzoeken uitgewerkt.

2.8.1 Verwerken van het verzoek getMachtigingToestand

Op basis van een combinatie van "gemachtigde", "dienst" en "vertegenwoordigde" wordt het machtigingsregister geraadpleegd om de toestand vast te stellen.

2.8.2 Verwerken van het verzoek getNieuweToestanden

Het verzoek bestaat bevat de volgende informatie "gemachtigde", "dienst", "tijdstempel vanaf" en "tijdstempel tot". Hierbij is alleen "dienst" verplicht. Het machtigingsregister wordt geraadpleegd om een machtigingtoestandlijst te bepalen met daarin alle machtigingen die voldoen aan de volgende criteria:

- gemachtigde komt overeen met "gemachtigde";
- dienst komt overeen met "dienst" (indien verzoek deze informatie bevat);
- de machtigingstoestand is geldig geweest in de periode "tijdstempel vanaf" t/m "tijdstempel tot" (voor zover verzoek deze informatie bevat);
- de machtingstoestand is nog niet eerder verwerkt door het *getNieuweToestanden* verzoek.

De machtingstoestandlijst wordt oplopend gesorteerd op de begindatum, zodat de oudste mutaties die voldoet aan de criteria boven in de lijst komen te staan.

Voor de lijst is een maximaal aantal van 100 van toepassing. In de situatie dat de machtigingstoestandlijst dit aantal overschrijdt, wordt geen foutmelding teruggegeven, maar het maximaal aantal machtigingstoestanden. In deze situatie worden alleen de oudste meegegeven. De service kan daarna opnieuw gebruikt worden om opvolgende, nog niet meegegeven, machtigingstoestanden op te halen. Dit gaat zo door totdat de machtigingstoestandlijst leeg is.

De machtigingstoestandlijst wordt vervolgens gebruikt om het antwoord van het machtigingsraadpleegverzoek op te bouwen.

2.9 Versturen antwoord machtigingsraadpleegverzoek

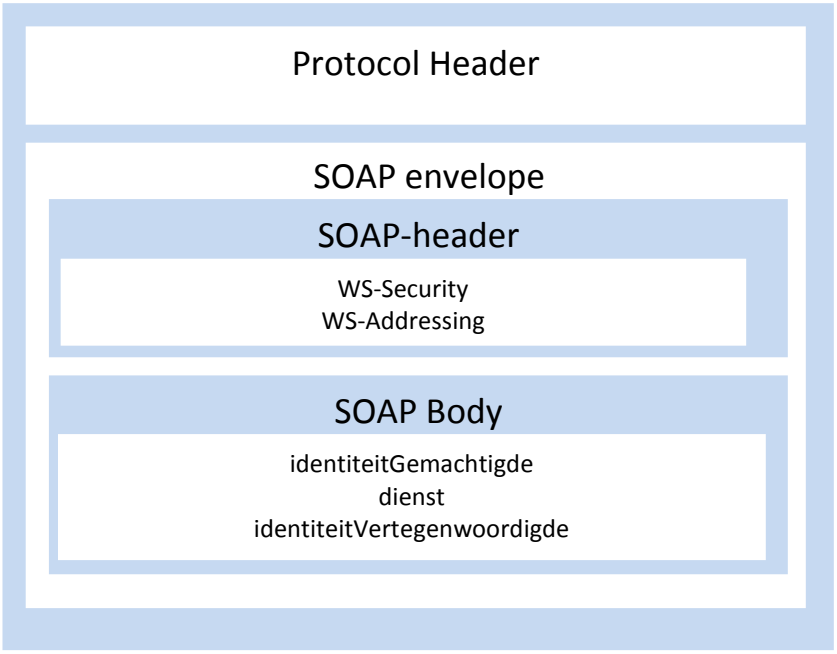
Als het machtigingsraadpleegverzoek met succes is opgehaald, wordt een antwoord (een SOAP-response) verstuurd. De volgende SOAP-responses zijn van toepassing:

- getMachtigingToestandResponse;
- getNieuweToestandenResponse.

3 SOAP-bericht

3.1 Structuur SOAP-request

Het SOAP-request bevat het machtigingtoestandverzoek. In onderstaande figuur wordt de opbouw van de mogelijke SOAP-requests getoond. Op basis van de combinatie de gemachtigde, de dienst en de vertegenwoordigde wordt de toestand van de machtiging opgehaald.



Figuur 3 SOAP-requests voor Machtigingraadpleegservice

Het SOAP-bericht bestaat uit:

- De transportprotocolheader;
- De SOAP-envelope met daarbinnen:
  - De SOAP-header;
  - De SOAP-body.

De SOAP-header bevat de WS-Security, WS-Addressing elementen en de tijdstempel waarop het bericht is gemaakt. Dit is verder uitgewerkt in het document "Koppelvlakbeschrijving Digipoort WUS 2.0".

3.2 Structuur getMachtigingToestandResponse

De SOAP-response bevat het toestandinformatie-antwoord. Deze bevat precies één "getMachtigingToestandResponse"-element.

Dit element bevat de volgende elementen:

Element	**Toelichting**
toestand	De naam van de huidige toestand van de machtiging, bijvoorbeeld "In behandeling".
datum	Tijdstempel van het begin van de huidigde toestand.
actor	De actor die verantwoordelijk is voor de huidige toestand, bijvoorbeeld "S2S".
reden	De reden van de huidige toestand, bijvoorbeeld "Machtigingsclaim ingediend".

3.3 Structuur getNieuweToestandenResponse

De SOAP-response bevat het antwoord van het verzoek *getNieuweToestanden*. Dit antwoord bevat precies één "getMachtigingNieuweToestandenResponse"-element met precies één "getNieuweToestandenReturn"-element.

Het element "getNieuweToestandenReturn" bevat nul of meer "machtigingToestand"-elementen. Ieder "machtigingToestand"-element bevat de volgende elementen:

Element	**Toelichting**
identiteitVertegenwoordigde	De identiteit van de vertegenwoordige bestaat uit twee elementen "type" en "nummer" waarmee de vertegenwoordigde kan worden geïdentificeerd. Bijvoorbeeld: type "PersNr" en nummer: "111111111"
dienst	De dienst van de machtiging, bijvoorbeeld "SBA_IH_2012".
toestand	De naam van de toestand van de machtiging, bijvoorbeeld "In behandeling".
datum	De datum en het tijdstip waarop de toestand ingaat, bijvoorbeeld "2013-05-11T21:30:47.0Z".
actor	De actor die verantwoordelijk is voor de huidige toestand, bijvoorbeeld "S2S".
reden	De reden van de huidige toestand, bijvoorbeeld "Machtigingsclaim ingediend".

3.4 Header-elementen

De elementen WS-Security en WS-Addressing zijn uitgewerkt in het document "Koppelvlakbeschrijving Digipoort; Webservices Bedrijven - WUS 2.0".

In aanvulling op dit document geldt dat het element **wsa:MessageID** moet voldoen aan:

http://www.w3.org/TR/2007/REC-ws-addr-metadata-20070904/

Tevens geldt dat er geen eigen header velden toegevoegd mogen worden aan het bericht.

3.5 Berichtelementen getMachtigingToestand

De SOAP body bevat de inhoudelijke gegevens. De volgende elementen zijn voor het verzoek *getMachtigingToestand* van toepassing:

3.5.1 *identiteitGemachtigde*
De identiteit van de gemachtigde is een combinatie van het identiteitstype en het identiteitsnummer van de gemachtigde.
Verplicht: Ja

3.5.2 *dienst*
De dienst waarvoor de toestand van de machtiging wordt opgevraagd. Dit is de dienst zoals deze voorkomt in de Dienstencatalogus.
Verplicht: Ja

3.5.3 *identiteitVertegenwoordigde*
De identiteit van de belanghebbende is een combinatie van het identiteitstype en het identiteitsnummer van de vertegenwoordigde waarvoor de toestand van de machtiging wordt opgevraagd.
Verplicht: Ja

3.6 Berichtelementen getNieuweToestanden

De SOAP body bevat de inhoudelijke gegevens. De volgende elementen zijn voor het verzoek *getNieuweToestanden* van toepassing:

3.6.1 *identiteitGemachtigde*
De identiteit van de gemachtigde is een combinatie van het identiteitstype en het identiteitsnummer van de gemachtigde.
Verplicht: Ja

3.6.2 *dienst*
Als dit element aanwezig is, worden alleen machtigingstoestanden geselecteerd die betrekking hebben op deze dienst. Dit is de dienst zoals deze voorkomt in de Dienstencatalogus.
Verplicht: Nee

3.6.3 *tijdstempelVanaf*
Als dit element aanwezig is, worden alleen machtigingstoestanden geselecteerd waarvoor de begindatum en tijd na dit moment ligt.
Verplicht: Nee

3.6.4 *tijdstempelTot*
Als dit element aanwezig is, worden alleen machtigingstoestanden geselecteerde waarvoor geen einddatum en tijd van toepassing is.
Verplicht: Nee

3.7 Beveiliging transportniveau

Beveiliging vindt plaats op transportniveau via tweezijdige TLS of SSLv3. In het document "Koppelvlakbeschrijving Digipoort WUS 2.0" is dit nader uitgewerkt.

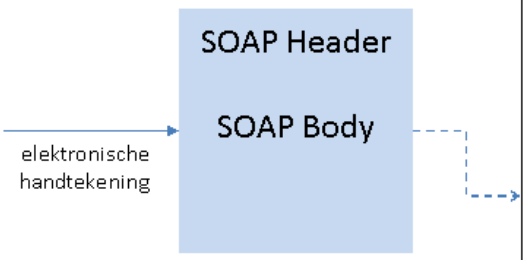
In aanvulling op dit document geldt dat de onderstaande TLS/SSL encryptie-algoritmen en sleutellengtes minimaal ondersteund moeten worden:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_AES_128_CBC_SHA

3.8 Ondertekening bericht (WS-Security)

De aanleveraar dient de body en de header elementen van een verzoek te tekenen. Digipoort zal daarop de body en header elementen van het antwoord tekenen. Dit tekenen dient te geschieden met behulp van een elektronische handtekening en aan de hand van een door een CSP uitgegeven PKIOverheid certificaat. Het certificaat, de handtekening en de gebruikte algoritmes dienen als WS-Security element in de header opgenomen te worden. Dit is nader uitgewerkt in het document "Koppelvlakbeschrijving Digipoort WUS 2.0".

Voorbeeld:




```
<soapenv:header>
   <wsse:security>
      …
      <ds:signature>
         …
         <ds:reference URI="#body">
         <ds:reference URI="#wsa-message-id">
            …
         <ds:reference URI="#timestamp">

            …
      </ds:signature>
      <wsu:timestamp wsu:Id="#timestamp">
   </wsse:security>
   <wsa:MessageID wsu:Id="#wsa-message-id">
         …
</soapenv:Header>
<soapenv:Body Id="body">
   …
</soapenv:Body>
```

Voor de machtigingraadpleegservice moet het *serialnumber* van het certificaat dat gebruikt is voor de elektronische handtekening overeen komen met het identiteitsnummer van de gemachtigde zoals opgenomen in het verzoek.

4 Details Machtigingraadpleegservice WUS 2.0

4.1 Type berichten

De Machtigingraadpleegservice kent drie type berichten:

Onderdeel	Toelichting
SOAP-request	het verzoekbericht aan de Machtigingraadpleegservice waarmee machtigingtoestand kan worden opgevraagd.
SOAP-response	een antwoordbericht waarmee informatie over de machtigingtoestand wordt teruggegeven.
SOAP fault	een foutbericht dat wordt verstuurd wanneer door de Machtigingraadpleegservice een fout wordt geconstateerd.

De structuur van de berichten is beschreven in de bijgeleverde wsdl.

4.2 Adres Machtigingraadpleegservice

Het adres van de Machtigingraadpleegservice is:

https://dgp.procesinfrastructuur.nl/wus/2.0/machtigingraadpleegservice/1.2

4.3 SOAP-request

Zie bijlage:

- *getMachtigingToestandRequest.xml*
- *getNieuweToestandenRequest.xml*

4.4 SOAP-response

Zie bijlage:

- *getMachtigingToestandResponse.xml*
- *getNieuweToestandenRespons.xml*

4.5 SOAP Fault

Zie bijlage:

- *Voorbeeld_MachtigingRaadpleegServiceFault.xml*

Als er fouten in het bericht aanwezig zijn, bijvoorbeeld wanneer de handtekening ontbreekt of wanneer er informatie ontbreekt, wordt er een SOAP fault gegenereerd. De foutmeldingen zijn beschreven in het document "Foutmeldingen en Statusmeldingen Digipoort".