



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Koppelvlakbeschrijving Digipoort Webservices Bedrijven - WUS 2.0

Versie 1.1

Datum	10 juli 2012
Status	Definitief

Colofon

Projectnaam	Digipoort
Versienummer	1.1
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	Servicebeschrijving Aanleverservice Servicebeschrijving Statusinformatieservice Foutmeldingen en Statusmeldingen

Inhoud

Colofon	2
Inhoud	3
Inleiding	4
<i>Doel en doelgroep</i>	<i>4</i>
<i>Leeswijzer</i>	<i>4</i>
<i>Status</i>	<i>4</i>
<i>Ondersteuning</i>	<i>4</i>
1 Berichtenverkeer	5
1.1 <i>Inleiding</i>	<i>5</i>
1.2 <i>Beveiliging</i>	<i>5</i>
1.2.1 <i>Transportniveau</i>	<i>5</i>
1.2.2 <i>Berichtniveau</i>	<i>6</i>
1.2.3 <i>Autorisatie</i>	<i>7</i>
2 Sessieverloop	8
2.1 <i>Controleren structuur verzoek</i>	<i>8</i>
2.2 <i>Ontvangen verzoek</i>	<i>9</i>
2.3 <i>Versturen antwoord</i>	<i>9</i>
3 WS-Security	10
3.1 <i>Tekenen van het bericht</i>	<i>10</i>
3.2 <i>Tijdstempel Aangemaakt</i>	<i>11</i>
4 WS-Addressing	12
5 Algemene afspraken	13
5.1 <i>Communicatiestandaarden</i>	<i>13</i>
5.2 <i>Prefixen</i>	<i>13</i>
5.3 <i>Karaktercodering en karakterset</i>	<i>14</i>
5.4 <i>Datum en tijd</i>	<i>14</i>
5.5 <i>Gebruikte standaarden</i>	<i>14</i>

Inleiding

Doel en doelgroep

Dit document beschrijft de afspraken met betrekking tot het elektronische berichtenverkeer bij de overheid via Digipoort (voorheen Overheidstransactiepoort).

Dit document is bestemd voor ontwikkelaars van programmatuur voor het aanleveren en opvragen van berichten aan en van de overheid via deze infrastructuur.

Leeswijzer

Deze koppelvlakbeschrijving vormt de basis van een reeks servicebeschrijvingen die inzicht geven in het gebruik van de services van Digipoort. Dit document is als volgt opgebouwd:

- Het eerste hoofdstuk bevat algemene informatie over de werking van Digipoort.
- Het tweede hoofdstuk bevat een globale beschrijving van de werking van het WUS 2.0 koppelvlak en de betrokken webservices.
- Het derde en vierde hoofdstuk beschrijven de definities van de verschillende protocollen.
- Het vijfde hoofdstuk geeft een overzicht van alle algemeen van toepassing zijnde standaarden en afspraken.

Deze koppelvlakbeschrijving is onderdeel van een grotere set documenten die de dienstverlening van Digipoort beschrijft.

Status

Dit document beschrijft de afspraken met betrekking tot 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 het koppelvlak. 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 PKI-overheid-certificaten.

Ondersteuning

Informatie met betrekking tot ondersteuning bij het gebruik van de services van Digipoort is beschikbaar op de website:

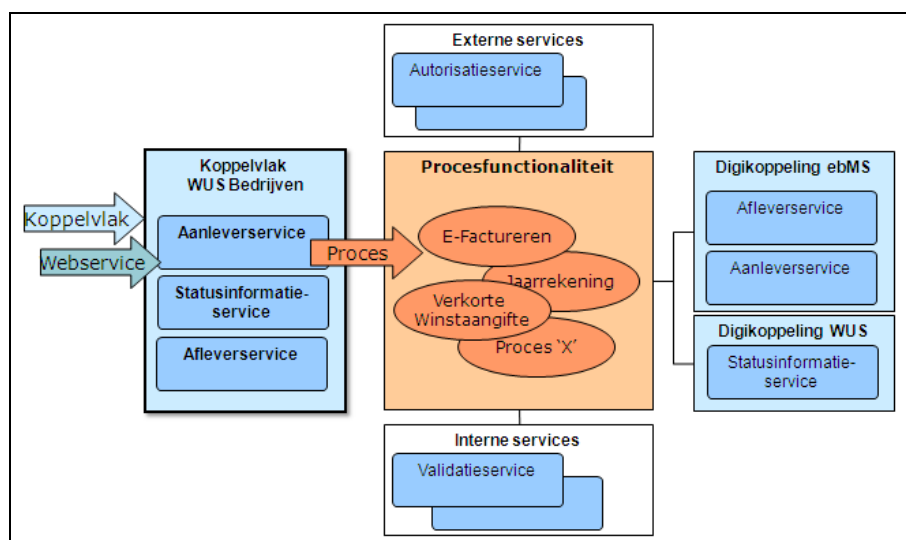
www.logius.nl/producten/gegevensuitwisseling/digipoort.

1 Berichtenverkeer

1.1 Inleiding

Digipoort kent services gericht op bedrijven en services gericht op de overheid. Daarnaast zijn er services die ondersteunend zijn bij de uitvoering van de verwerkingsprocessen, zoals de autorisatieservice en de validatieservice.

In onderstaande afbeelding zijn de services schematisch weergegeven.



Figuur 1 Services binnen Digipoort

Deze koppelvlakbeschrijving vormt de basis voor de services die Digipoort biedt aan bedrijven. Deze services zijn de Aanleverservice, Statusinformatieservice en de Afleverservice. Alle services worden ook daadwerkelijk als webservice aangeboden op Digipoort, behalve de Afleverservice. Aangezien het in dat laatste geval berichten betreft die *door* Digipoort worden gestuurd *naar* het bedrijf, moet deze webservice door het bedrijf zelf worden geïmplementeerd.

De details van elke service zijn beschreven in een afzonderlijk document: de Servicebeschrijving.

Het koppelvlak kan worden uitgebreid met nieuwe services. Deze voldoen dan altijd aan deze koppelvlakbeschrijving.

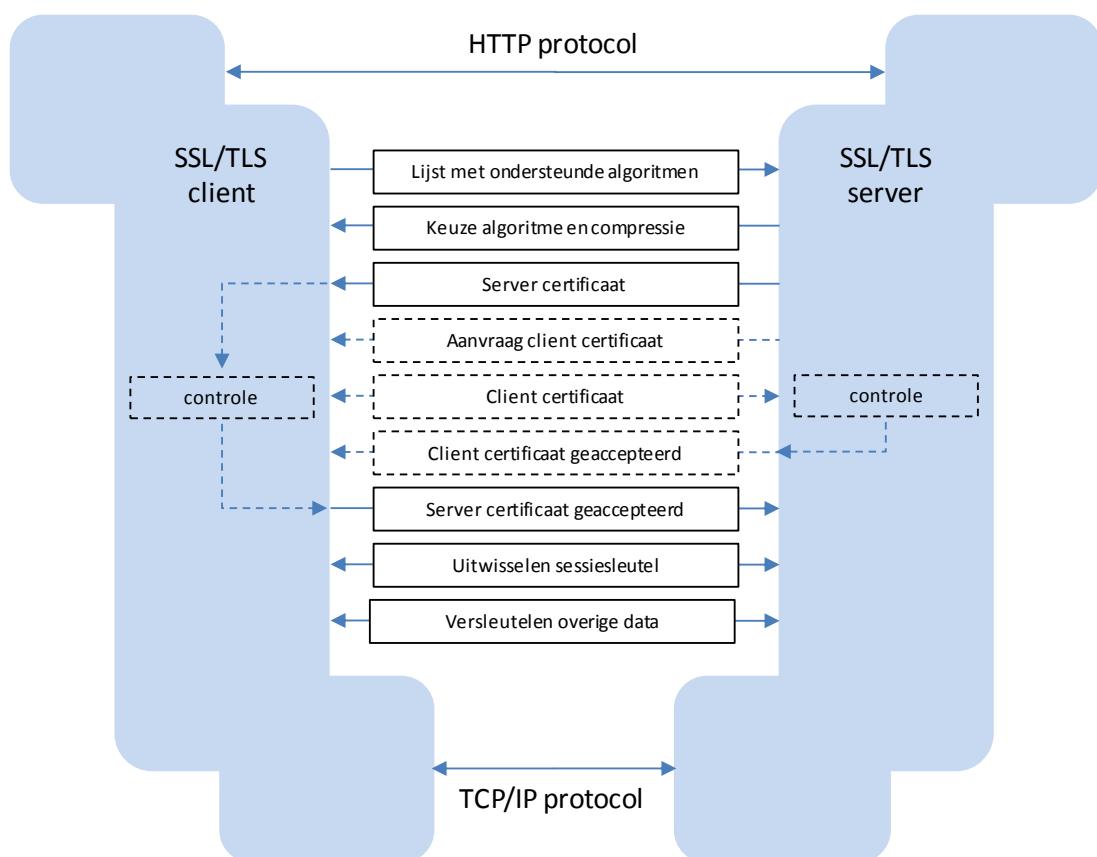
1.2 Beveiliging

1.2.1 Transportniveau

De authenticiteit van systemen in Digipoort en van de gebruikers van een service moet door alle deelnemende partijen vastgesteld kunnen worden

voordat een datacommunicatiesessie wordt gestart. De authenticiteit van systemen wordt met behulp van PKI-overheid-certificaten gecontroleerd¹. Feitelijk wordt de authenticiteit van bedrijven bepaald aan de hand van het PKI-overheid-clientcertificaat dat zich op het cliëntsysteem bevindt. Met behulp van dit certificaat opent de client een verbinding volgens het TLS/SSL-protocol (zie het overzicht in figuur 2). Dit protocol biedt naast authenticatie ook encryptie op transportniveau.

De geldigheid van het clientcertificaat wordt aan de hand van de gegevens in het certificaat gecontroleerd. Tevens wordt er tegen een Certificate Revocation List (CRL) gecontroleerd of het certificaat niet is ingetrokken.



Figuur 2: TLS/SSL-communicatie

1.2.2

Berichtniveau

Op berichtniveau wordt beveiliging toegepast door middel van WS-Security. Het bericht dient beveiligd te zijn met een handtekening over de SOAP body- en de SOAP header-elementen. Het certificaat dat hiervoor gebruikt wordt, moet aan dezelfde eisen voldoen als het certificaat dat gebruikt wordt op transportniveau. Het hoeft echter niet hetzelfde certificaat te zijn.

Deze beveiliging verzekert de integriteit van het bericht zelf. Ook als het bericht wordt gearchiveerd, blijft de WS-Security informatie met het bericht bewaard.

¹ In niet-productieomgevingen worden testcertificaten gebruikt.

Controle van de WS-Security handtekening houdt in dat de handtekening is gezet met een geldig certificaat en dat er een relatie bestaat tussen het certificaat en het bedrijf waarop het bericht betrekking heeft. Deze relatie kan er uit bestaan dat het certificaat van het bedrijf zelf is, of dat het certificaat hoort bij een partij die door het bedrijf is gemachtigd om namens het bedrijf informatie uit te wisselen met overheidspartijen.

De controle van de identiteit van het certificaat en de autorisatie van de betreffende partij, vindt plaats in het latere verwerkingsproces. Tijdens het verzoek wordt alleen de geldigheid van het certificaat gecontroleerd. Wel moet het bedrijfsnummer en berichtsoort in het aanleververzoek aanwezig zijn voor deze latere autorisatie.

1.2.3

Autorisatie

Een aantal verwerkingsprocessen vereist dat het bedrijf geautoriseerd wordt. Als dit het geval is zal degene die een verzoek doet aangeven bij welke AuSP-service hij geregistreerd staat middels het "auspEndpoint" element in het verzoek bericht.

De controle of er een relatie bestaat tussen het certificaat en het bedrijf waarop het bericht betrekking heeft vindt plaats door autorisatie. Een verwerkingsproces kan hierbij gebruik maken van de AuSP (Autorisatie Service Provider). De AuSP houdt een register bij waarin staat vermeld welke vertegenwoordigingsrelaties er bestaan tussen bedrijven en intermediairs. Dit register vermeldt voor welke bedrijven de inzender, dus degene die de handtekening heeft gezet, gestructureerde berichten mag inzenden en de status/retour informatie mag inzien. Dit is niet alleen nodig voor intermediairs, maar ook voor bedrijven die meerdere KvK- of Fi-nummers hebben.

Het bedrijf dient zich te kunnen autoriseren middels een PKIoverheid-certificaat, een berichtsoort en een bedrijfsnummer. De combinatie van deze drie gegevens dient bekend te zijn in het autorisatieregister van een AuSP-service. Digipoort controleert deze autorisatiegegevens bij de AuSP-service.

2 Sessieverloop

Een WUS webserviceclient van een bedrijf maakt een TLS-verbinding met een webservice van Digipoort of andersom. Over deze verbinding worden er SOAP requestberichten verzonden.

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 wordt het verwerkt. Als de verwerking niet mogelijk is wordt er een SOAP fault terug gezonden. Als het goed verlopen is wordt er een SOAP response terug verzonden.

Elke service bestaat tenminste uit de volgende onderdelen:

- Controleer verzoek
- Ontvang verzoek
- Verzend antwoord

Naast bovengenoemde onderdelen kunnen per service andere onderdelen zijn opgenomen. Deze zijn uitgewerkt in de servicebeschrijving.

2.1 Controleren structuur verzoek

Om SOAP berichten aan Digipoort aan te kunnen bieden of wanneer Digipoort SOAP berichten naar de overheidsdeelnemer verstuurt, wordt gebruik gemaakt van een verzoek met een voorgedefinieerde structuur. Deze structuur is vastgelegd met de Web Service Definition Language (WSDL). Bij de beschrijving van elke service is een WSDL bijgevoegd.

Nadat een verzoek (in de vorm van een SOAP-bericht) door Digipoort of door het bedrijf is ontvangen, dan dienen de volgende zaken gecontroleerd te worden:

Controle	Toelichting
Is een element aanwezig?	Hierbij wordt gecontroleerd of alle verplichte elementen zoals beschreven in de WSDL voorkomen in het aanleververzoek.
Is er geen onbekend element aanwezig?	Hierbij wordt gecontroleerd of in het verzoek geen elementen voorkomen, die niet in de WSDL zijn beschreven.
Bevat het element een waarde?	Hierbij wordt gecontroleerd of alle verplichte elementen ook daadwerkelijk een waarde bevatten.
Betreft het een toegestane waarde?	Hierbij wordt gecontroleerd of alle elementen toegestane waarden bevatten.
Is de lengte van de waarde juist?	Hierbij wordt gecontroleerd of de waarde van de elementen niet langer is dan de lengte zoals

	beschreven in de WSDL.
--	------------------------

2.2 Ontvangen verzoek

Elk verzoek aan een service van Digipoort wordt vastgelegd in de berichtenadministratie. De berichtenadministratie fungeert binnen Digipoort als audittrail. Op dezelfde wijze kan het bedrijf verzoeken van Digipoort vastleggen in een eigen berichtenadministratie.

2.3 Versturen antwoord

Wanneer het verzoek voldoet aan alle gestelde eisen, wordt het antwoord verstuurd.

Elk antwoord naar Digipoort wordt vastgelegd in de berichtenadministratie. Het bedrijf kan ook antwoorden van Digipoort in een eigen berichtenadministratie vastleggen.

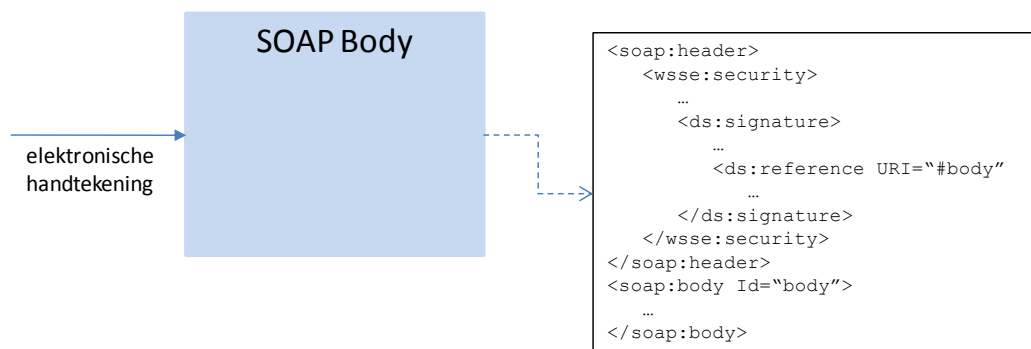
De elementen van het antwoord worden beschreven in de servicebeschrijving van de desbetreffende service.

Het antwoord bevat tevens een handtekening van Digipoort volgens WS-Security standaard. Dit is beschreven in het volgende hoofdstuk.

3 WS-Security

Een bedrijf of intermediair dient elementen van een SOAP-bericht te tekenen. Dit tekenen dient te geschieden met behulp van een elektronische handtekening en aan de hand van een door een CSP uitgegeven PKI-overheid-certificaat. Het certificaat, de handtekening en de gebruikte algoritmes dienen als WS-Security element in de header opgenomen te worden.

Voorbeeld:



Figuur 2 Handtekening volgens WS-Security

WS-Security levert het volgende:

- De mogelijkheid op het controleren van de integriteit van het bericht.
- De garantie van de identiteit van de verzender van het bericht.
- Het tijdstempel kan zorgen dat er geen aanval kan worden uitgevoerd op Digipoort. Daarnaast wordt het tijdstempel ook gebruikt om aan te geven wanneer een bericht is ontvangen bij Digipoort.

De public key van het certificaat waarmee de handtekening gezet wordt, moet meegeleverd worden in de header van de SOAP envelop als binary security token.

3.1 Teken van het bericht

De volgende onderdelen worden ondertekend:

- soap-env:Body
- het header-onderdeel timestamp
- het header-onderdeel ws-adressing (alle elementen)

De volgende eisen gelden voor de WS-Security elementen:

<http://www.w3.org/2000/09/xmlsig#>

Stap 1: Canonicalization

<http://www.w3.org/2001/10/xml-exc-c14n#>

Stap 2: Digest

<http://www.w3.org/2000/09/xmldsig#sha1>

Stap 3: Signature

<http://www.w3.org/2000/09/xmldsig#rsa-sha1>

3.2

Tijdstempel Aangemaakt

Het element "TimeStamp" en "Created" beschrijft de datum en het tijdstip waarop het verzoek door een gebruiker is verzonden vanuit of naar Digipoort. Het tijdstempel wordt verwacht in de UTC vorm. Daarnaast biedt het optionele "Expires" de mogelijkheid aan te geven tot wanneer het bericht afgehandeld dient te worden.

Deze WS-Security header elementen horen in de web service utility namespace: <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>

Element	TimeStamp
Verplicht	Ja
Type	DateTime in UTC

Element	Created
Verplicht	Ja
Type	DateTime in UTC

Element	Expires
Verplicht	Nee
Type	DateTime in UTC

4 WS-Addressing

Digipoort maakt gebruik van WS-Addressing 1.0 met namespace <http://www.w3.org/2005/08/addressing>.

De WS-Addressing elementen van de SOAP requests en responses dienen als volgt gevuld te zijn:

Element	Toelichting	Verplicht
wsa:To	De WSDL waarde of http://www.w3.org/2005/08/addressing/none of http://www.w3.org/2005/08/addressing/anonymous	Ja
wsa:Action	Deze waarde wordt gebruikt om een specifieke operatie aan te roepen.	Ja
wsa:MessageID	Het unieke id voor dit bericht als UUID.	Ja
wsa:RelatesTo	Het bevat de waarde van de wsa:MessageID van het originele verzoek	Alleen in response bericht
wsa:ReplyTo	http://www.w3.org/2005/08/addressing/anonymous	Nee

5 Algemene afspraken

5.1 Communicatiestandaarden

De communicatie tussen webservice client en de webservice verloopt over een aantal lagen. Per laag gelden standaarden. Samengevat gaat het om de volgende standaarden:

Laag	Standaard
Applicatielaag	XML
	SOAP
Sessielag	http
Transportlaag	TCP
Netwerklag	IP

5.2 Prefixen

Voor namespaces in de wsdl en SOAP berichten van de services worden de onderstaande prefixen gehanteerd:

Prefix	Specificatie	Namespace URI
tns	WUS 2.0 <Digipoort_Service> 1.0	<a href="http://logius.nl/digipoort/wus/2.0/<Digipoort_Service>/1.1/">http://logius.nl/digipoort/wus/2.0/<Digipoort_Service>/1.1/ voor elke WUS service van Digipoort
soapenv	SOAP 1.1	http://schemas.xmlsoap.org/soap/envelope/
wsdl	WSDL 1.1	http://schemas.xmlsoap.org/wsdl
ds	XML Signature 1.0	http://www.w3.org/2000/09/xmldsig#
xsd	XML Schema 1.0	http://www.w3.org/2001/XMLSchema
wsse	WS-Security 1.0	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsu	WS-Security 1.0	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
wsa	WS-Addressing 1.0	http://www.w3.org/2005/08/addressing
wsam	WS-Addressing 1.0 - Metadata	http://www.w3.org/2007/05/addressing/metadata
wsp	Webservices Policy 1.2	http://schemas.xmlsoap.org/ws/2004/09/policy
sp	Security Policy 1.1	http://schemas.xmlsoap.org/ws/2005/07/securitypolicy

5.3 Karaktercodering en karakterset

De ondersteunde karakterset is UTF-8.

5.4 Datum en tijd

Voor alle datum/tijd velden wordt gebruik gemaakt van het type `xsd:date` en `xsd:dateTime`, ingevuld naar de UTC (Z) variant op de ISO 8601 (NEN28601) standaard. Het gebruik van fracties van seconden is optioneel.

5.5 Gebruikte standaarden

Voor deze standaarden worden dezelfde keuzes gemaakt als voor de Digikoppeling-standaard WUS 2.0 die van toepassing is op de Nederlandse overhead. Zie www.logius.nl/digikoppeling.

Overheidsstandaarden:

- PKI overheid 1.1

WS-I standaarden:

- WS-I Basic Profile 1.2
- WS-I Basic Security Profile 1.0

W3C standaard:

- MTOM 1.0