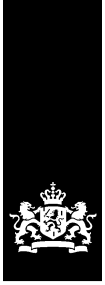


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakbeschrijving Digipoort
Digikoppeling WUS 2.0 (overheden)

Koppelvlakversie 1.1

Versie	1.0
Datum	10 juli 2012
Status	Definitief

Colofon

Projectnaam	Digipoort
Versienummer	1.0
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	NVT

Inhoud

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 Digipoort (via koppelvlak Digikoppeling WUS) 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 koppelvlak 'Digikoppeling WUS 2.0' en de betrokken webservices;
- Het derde hoofdstuk geeft een globale beschrijving van het SOAP-bericht;
- Het vierde en vijfde hoofdstuk beschrijven de definities van de verschillende protocollen;
- Het zesde 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 koppelvlak 'Digikoppeling WUS 2.0' 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 PKIoverheid-certificaten.

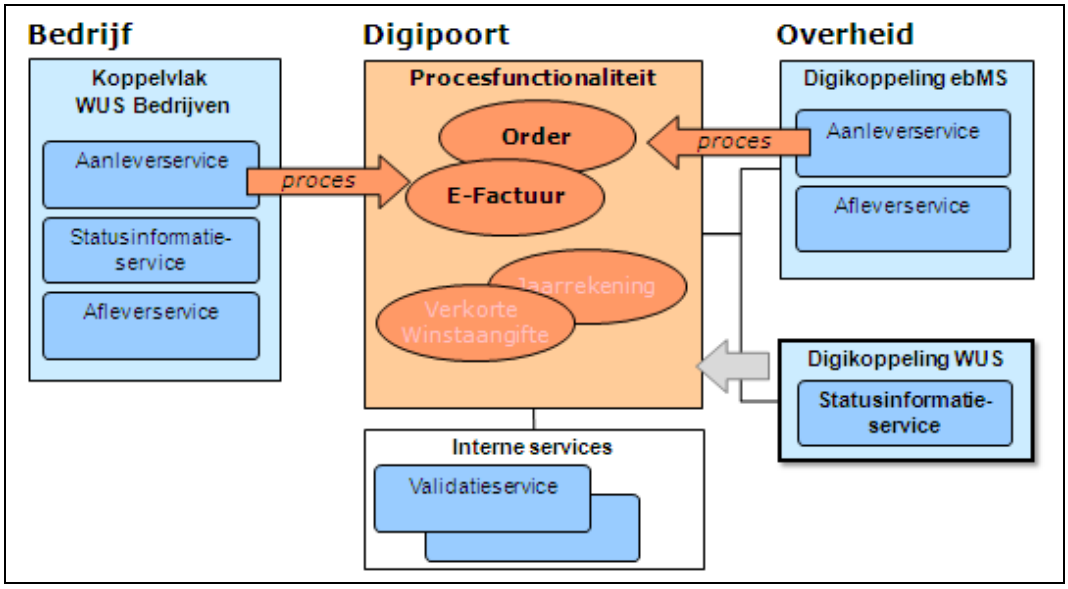
Ondersteuning
Informatie met betrekking tot ondersteuning bij het gebruik van de services van Digipoort is beschikbaar op de website: www.logius.nl/producten/gegevensuitwisseling/digipoort.

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 (koppelvlakversie 1.1)

Deze koppelvlakbeschrijving vormt de basis voor de services die Digipoort biedt aan overheden via het Digikoppeling WUS-koppelvlak. Het betreft momenteel alleen de Statusinformatieservice. De andere services zijn ingericht conform het ebMS-koppelvlak.

De details van elke service onder een koppelvlak zijn beschreven in afzonderlijk documenten: de Servicebeschrijvingen.

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 PKIoverheid-certificaten gecontroleerd[1].

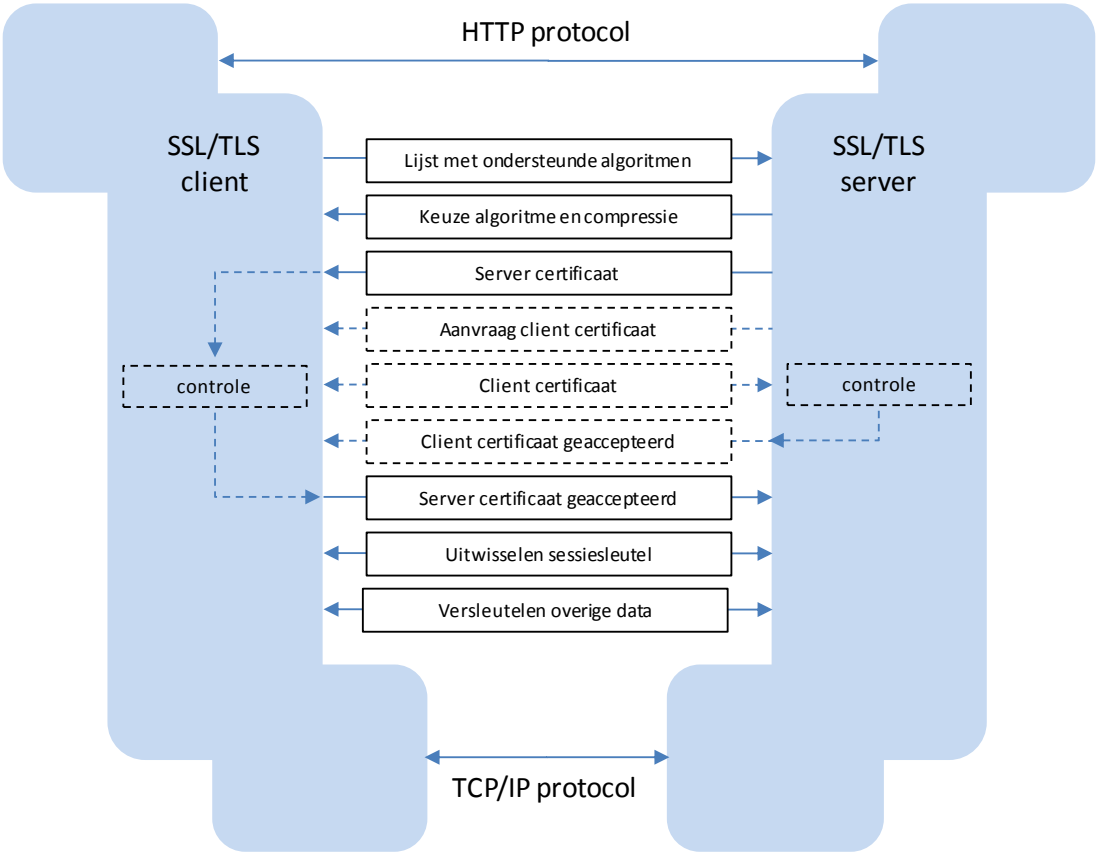
1 In niet-productieomgevingen worden testcertificaten gebruikt.

Voor een productieaansluiting op Digipoort bent u verplicht gebruik te maken van een PKIoverheid-certificaat (X.509). Dit certificaat waarborgt de veiligheid en betrouwbaarheid van de verbinding tussen uw systeem en Digipoort. Let wel, het PKIoverheid-certificaat is alleen verplicht op de productieomgeving. In de preproductieomgeving is het ook mogelijk om gebruik te maken van self-signed testcertificaten, geleverd door Logius.

U kunt een PKIoverheid-certificaat aanvragen via een Certificate Service Provider (CSP). Een overzicht van de huidige CSP's is te vinden op de website van Logius (http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/toetreden-tot-pkioverheid/, onder Toegetreden CSP's). Wegens de doorlooptijd van de aanvraag, adviseren wij u een PKIoverheid-certificaat vroegtijdig aan te vragen. Voor een testcertificaat kunt u zich richten tot het Service Centrum van Logius

Feitelijk wordt de authenticiteit van een overheidsorganisatie bepaald aan de hand van het PKIOverheid-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

Op transportniveau is de partij die wordt geauthenticeerd de partij waarmee de TLS-verbinding tot stand komt. Dit kan ook een *shared service centre* zijn dat voor een of meerdere overheidsorganisaties de verbinding met Digipoort verzorgt. Op transportniveau is het dus niet noodzakelijkerwijs de 'eigenaar' van de berichten (de organisatie namens wie een bericht wordt verstuurd) wiens identiteit wordt gecontroleerd.

1.2.2 Berichtniveau

Op berichtniveau kan aanvullende beveiliging worden toegepast door toepassing van WS-Security. Het bericht wordt dan zelf beveiligd middels een handtekening over de SOAP body- en gespecificeerde 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.

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 de overheidsorganisatie waarop het bericht betrekking heeft. Deze relatie kan er uit bestaan dat het certificaat van de overheidsorganisatie zelf is, of dat het certificaat hoort bij een partij die door deze organisatie is gemachtigd om namens de organisatie informatie uit te wisselen met bedrijven en andere overheidspartijen.

De controle van de identiteit, die door het certificaat wordt gerepresenteerd, en de autorisatie van de betreffende partij vindt plaats in het latere verwerkingsproces. Tijdens het verzoek worden alleen de geldigheid van het certificaat en van de handtekening gecontroleerd. Overheidsnummer (OIN) en berichtsoort moeten in het aanleververzoek aanwezig zijn om de latere autorisatie mogelijk te maken, ook daarop wordt derhalve gecontroleerd.

2 Sessieverloop

Een webservice client van een overheidsorganisatie maakt een TLS-verbinding met een webservice van Digipoort of andersom. Over deze verbinding worden er SOAP requestberichten verzonden (voor meer informatie over de structuur van de SOAP-berichten, zie hoofdstuk 3).

Als het bericht niet voldoet aan de eisen die worden gesteld in de WSDL, wordt er een SOAP fault teruggestuurd. Als het bericht wel voldoet aan de eisen, dan wordt het verder verwerkt. Ook in het geval dat de verwerking niet correct kan worden uitgevoerd, wordt er een SOAP fault teruggestuurd. Indien de verwerking succesvol verlopen is, wordt er een SOAP response verzonden.

Elke service bestaat tenminste uit de volgende onderdelen:

- Controleren verzoek
- Ontvangen (van het gecontroleerde) verzoek
- Verzenden antwoord

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

2.1 Controleren verzoek

SOAP-berichten die aan Digipoort worden aangeboden en SOAP-berichten die door Digipoort naar een overheidsorganisatie worden verstuurd, zijn opgemaakt conform een voorgedefinieerde structuur (SOAP request). Deze structuur is vastgelegd in een XML Schema (XSD), dat onderdeel uitmaakt van de WSDL die de webservice formeel beschrijft. Bij de beschrijving van elke service is de WSDL als apart bestand bijgevoegd.

Nadat een verzoek (in de vorm van een SOAP-bericht) door Digipoort of door de overheidsorganisatie is ontvangen, 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 audit trail. Op dezelfde wijze kan het de overheidsorganisatie 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. De overheidsorganisatie kan ook antwoorden van Digipoort in een eigen berichtenadministratie vastleggen.

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

3 SOAP-bericht

Het koppelvlak 'Digikoppeling WUS 2.0' maakt gebruik van de SOAP 1.1-standaard voor de samenstelling van elektronische berichten. SOAP is een gebruikelijke standaard bij elektronisch berichtenverkeer op basis van services.

Een bericht dat naar een service wordt gestuurd, wordt 'SOAP request' genoemd. Als reactie op een request kan een 'SOAP response' worden teruggestuurd. Indien er bij ontvangst of verwerking van het request-bericht fouten worden geconstateerd, wordt een 'SOAP fault' teruggestuurd waarin nadere informatie over de geconstateerde fout is opgenomen. Een beschrijving van de foutmeldingen is opgenomen in de documentatieset.

3.1 Structuur

De structuur van request- en responseberichten is afhankelijk van de service waarbinnen deze berichten worden gebruikt. Een gedetailleerde beschrijving is dan ook terug te vinden in de afzonderlijke servicebeschrijvingen.

3.2 Adressering

Digipoort-services onder het 'Digikoppeling WUS 2.0'-koppelvlak maken gebruik van WS-Addressing, waarmee het mogelijk is om berichten te routeren onafhankelijk van het gebruikte transportprotocol.

Meer details over WS-Addressing zijn te vinden in hoofdstuk 4.

3.3 Ondertekening bericht (WS-Security)

Berichten kunnen digitaal worden ondertekend. Hiervoor wordt gebruik gemaakt van de 'WS-Security'-standaard. Ondertekenen, indien toegepast, geldt voor zowel request- als responsberichten.

Meer informatie over de toepassing hiervan is te vinden in hoofdstuk 5.

3.4 MTOM

De inhoudelijke gegevens worden in het element 'berichtInhoud' opgenomen. Tevens is het mogelijk om extra bijlagen op te nemen. Bijlagen kunnen op twee manieren in het bericht worden opgenomen:

- Als Base64-gecodeerd binaire data;
- Op basis van MTOM.

Bij het toepassen van MTOM wordt ook wel gesproken van een geoptimaliseerd bericht. MTOM is beschreven in WS-I Basic Profile 1.2 (zie http://www.w3.org/TR/soap12-mtom/)

De meeste gangbare toolkits kunnen MTOM-berichten ontvangen en versturen. Het wel of niet toepassen van MTOM kan in de regel worden aangegeven middels een configuratiebestand of vanuit de code. Op deze manier wordt aan de webservice meegegeven of deze MTOM gebruikt dan wel kan gebruiken bij het ontvangen en versturen van berichten. Het daadwerkelijke gebruik van MTOM wordt feitelijk door de service requester bepaald; de service requester neemt hierin het initiatief. Indien een op MTOM ingerichte webservice een geoptimaliseerd bericht ontvangt, zal de respons ook geoptimaliseerd worden teruggestuurd. Indien het request niet was geoptimaliseerd (geen gebruik van MTOM) wordt ook de respons niet geoptimaliseerd.

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:

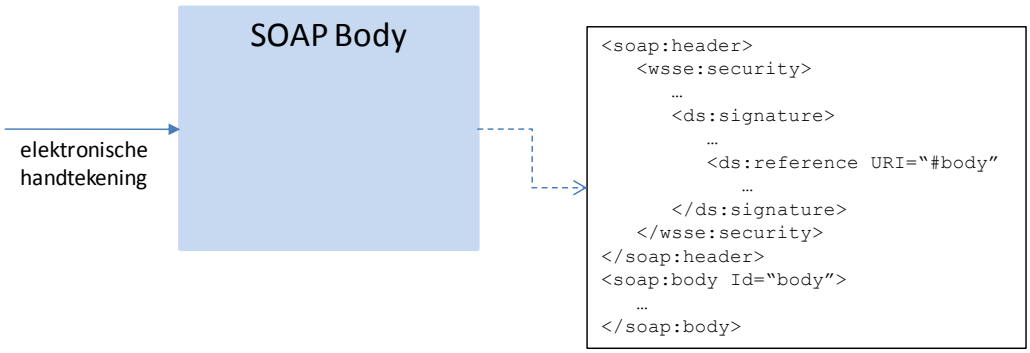
Element	**Toelichting**	**Verplicht**
wsa:To	De WSDL-waarde (request) of http://www.w3.org/2005/08/addressing/none of http://www.w3.org/2005/08/addressing/anonymous (response)	Ja
wsa:Action	Deze waarde wordt gebruikt om een specifieke operatie aan te roepen.	Ja
wsa:MessageID	Het unieke id voor dit bericht 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 WS-Security

Berichtondertekening kan worden toegepast als aanvullende veiligheidsmaatregel (naast transportbeveiliging via TLS/SSL die standaard wordt toegepast). Voor berichtondertekening wordt gebruik gemaakt van de 'WS-Security'-standaard. Toepassing hiervan betekent dat onderdelen van een bericht worden ondertekend met een elektronische handtekening[2]. Ondertekening vindt plaats met behulp van een PKIoverheid-certificaat.

Het certificaat, de handtekening en de bij ondertekening gebruikte algoritmes dienen als WS-Security element in de bericht-header opgenomen te worden.

Voorbeeld (ondertekenen Body):



Figuur 3 Digitaal ondertekenen volgens WS-Security

Het toepassen van WS-Security levert het volgende op:

- De mogelijkheid op het controleren van de integriteit van het bericht;
- De garantie van de identiteit van de verzender van het bericht;
- Opname van een tijdstempel in het bericht, waarmee wordt aangegeven wanneer het bericht is gecreëerd en (optioneel) tot wanneer het verwerkt kan worden. Hiermee wordt onder meer voorkomen dat een aanval kan worden uitgevoerd op 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*.

5.1 Tekenen van het bericht

De volgende onderdelen worden ondertekend:

- soap-env:Body

2 Ondertekening is van toepassing op SOAP request en –response-berichten, niet op SOAP faults.

- het header-onderdeel Timestamp
- het header-onderdeel WS-Addressing (alle elementen)

De volgende eisen gelden voor toepassing van WS-Security:
http://www.w3.org/2000/09/xmldsig#

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

5.2 Tijdstempel Aangemaakt

Binnen het element "TimeStamp" geeft het element "Created" de datum en het tijdstip aan waarop het verzoek is verzonden vanuit of naar Digipoort. Het tijdstempel wordt verwacht in de UTC-vorm (Zulu Time) volgens onderstaande notatie. Daarnaast biedt het optionele "Expires" de mogelijkheid aan te geven binnen welke periode het bericht afgehandeld dient te worden.

Voorbeeld:

```
<wsu:Timestamp ... >
      <wsu:Created>2011-11-30T11:12:12.459Z</wsu:Created>
      <wsu:Expires>2011-12-01T11:12:12.459Z</wsu:Expires>
</wsu:Timestamp>
```

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

Element	Created
Verplicht	Ja
Type	DateTime in UTC

Element	Expires
Verplicht	Nee
Type	DateTime in UTC

6 Algemene afspraken

6.1 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
Sessielaag	HTTP
Transportlaag	TCP
Netwerklaag	IP

6.2 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> 1.1	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

6.3 Karaktercodering en karakterset

De ondersteunde karakterset is UTF-8.

6.4 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.

6.5 Gebruikte standaarden

Overheidsstandaarden:

- Digikoppeling WUS 2.0
- 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

Voor meer informatie over de Digikoppeling Koppelvlakstandaarden, zie http://www.logius.nl/producten/gegevensuitwisseling/digikoppeling/.