



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Koppelvlakstandaard WUS

Digikoppeling 3.0

Document versie 3.2

Datum	6 november 2014
Status	Definitief

Colofon

Projectnaam	Digikoppeling 3.0
Versienummer	3.2 Definitief
Organisatie	Servicecentrum Logius Postbus 96810 2509 JE Den Haag T 0900 555 4555 servicecentrum@logius.nl
Bijlage(n)	0

Inhoud

Colofon	2
Inhoud	3
Inleiding	5
1.1 Doel en Doelgroep	5
1.2 Opbouw Digikoppeling documentatie	5
1.3 Digikoppeling	7
1.4 Koppelvlak & koppelvlakstandaard	8
1.5 Opbouw van dit document	8
2 Koppelvlakstandaard WUS	10
2.1 Inleiding	10
2.1.1 Wijzigingen in Digikoppeling 2.0 ten opzichte van Digikoppeling 1.0	10
2.1.2 Wijzigingen in Digikoppeling 3.0 ten opzichte van Digikoppeling 2.0	11
2.2 Ondersteunde varianten	11
2.3 Gehanteerde standaarden	13
2.4 Voorschriften	14
2.4.1 Service definitie WSDL	15
2.4.2 WS-Addressing	16
2.4.3 Binaire Data	18
2.4.4 Beveiliging	19
2.4.5 WS-Reliable Messaging	23
2.4.6 Naamgeving, namespaces	25
2.5 Foutafhandeling	25
3 Digikoppeling profielen WUS	26
3.1 WUS Profiel Digikoppeling 2W-be	27
3.2 WUS Profiel Digikoppeling 2W-be-S	28
3.3 WUS Profiel Digikoppeling 2W-be-SE	28
3.4 WUS Profiel Digikoppeling 2W-R	28
3.5 WUS Profiel Digikoppeling 2W-R-S	28
3.6 WUS Profiel Digikoppeling 2W-R-SE	29
Bijlage 1 – Voorbeeld WSDL	30
Digikoppeling 2 - Digikoppeling compliancevoorziening.xsd	30
Digikoppeling 2 - compliancevoorziening- Digikoppeling 2.xsd	31
Digikoppeling 2 - compliancevoorziening-abstract-definition-Digikoppeling 2.wsdl	31

<i>Digikoppeling 2 - voorbeeld-servicebinding.wsdl</i>	32
Bijlage 2 - Voorbeeld SOAP berichten Digikoppeling 2W-be profiel	34
Bijlage 3 - Voorbeeld SOAP berichten Digikoppeling 2W-be profiel met MTOM	36
Bijlage 4 - Voorbeeld SOAP berichten Digikoppeling 2W-be- S profiel	38
Bijlage 5 - Voorbeeld SOAP berichten Digikoppeling 2W-be- S profiel met MTOM	42
Bijlage 6 - Voorbeeld SOAP berichten Digikoppeling 2W-be- SE profiel	46
Bijlage 7 - Voorbeeld SOAP berichten Digikoppeling 2W-be- SE profiel met MTOM	52
Bijlage 8 – Voorbeeld SOAP berichten voor reliable berichten	57

Inleiding

1.1 Doel en Doelgroep

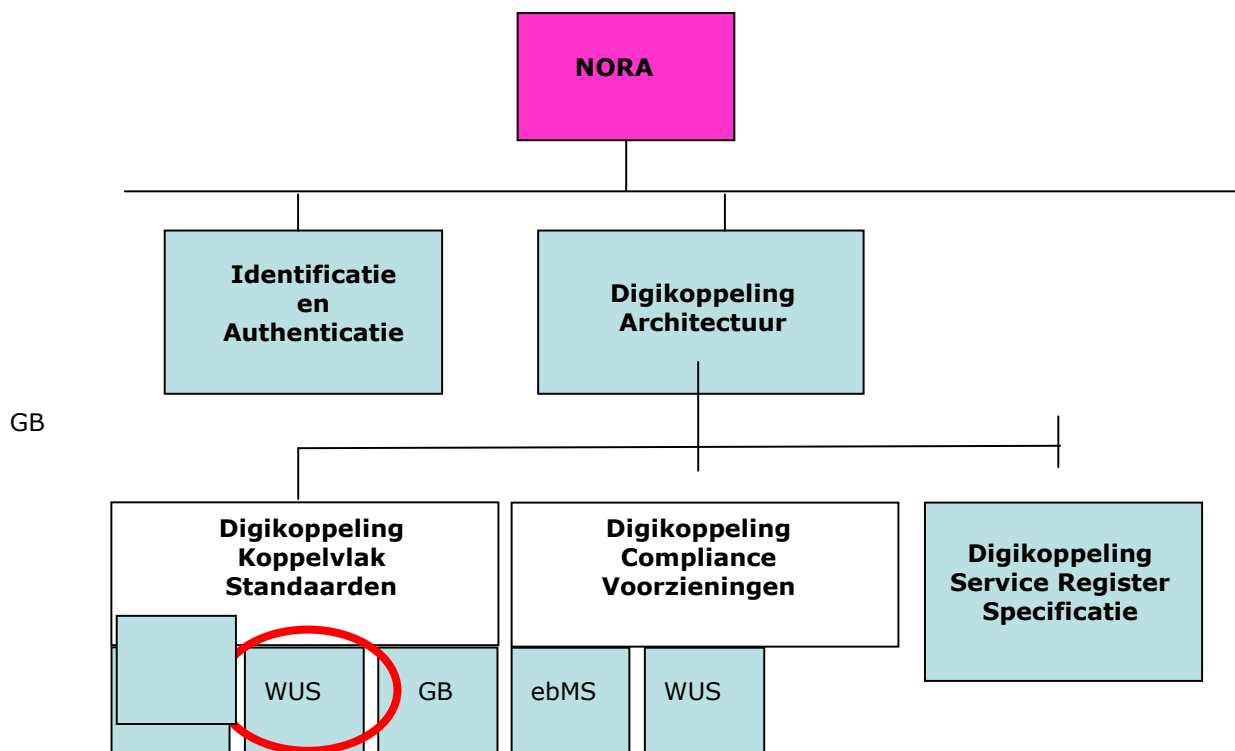
Dit document beschrijft de functionele specificaties voor Digikoppeling WUS Profile, onderdeel van Digikoppeling 3.0.

Het document is bestemd voor architecten en ontwikkelaars die op basis van WUS gegevens willen uitwisselen via Digikoppeling.

Alle Digikoppeling webservices die op WUS gebaseerd zijn, moeten conformeren aan de koppelvlakstandaard WUS. Deze wordt tot in detail in dit document gespecificeerd. Doel van dit document is ontwikkelaars te informeren wat deze koppelvlakstandaard nu precies inhoudt en waar zij zich aan moeten conformeren. Het document is bestemd voor architecten en ontwikkelaars die op basis van WUS gegevens willen uitwisselen via Digikoppeling. Het gaat hierbij om zowel service providers als service requesters (clients).

1.2 Opbouw Digikoppeling documentatie

Digikoppeling is beschreven in een set van documenten. Deze set is als volgt opgebouwd:



Figuur 1 – Opbouw documentatie Digikoppeling

Dit document beschrijft de WUS variant van de koppelvlakstandaarden. Naast de Koppelvlakstandaard WUS is er ook de ebMS-standaard. Die wordt in een apart document beschreven.

1.3

Digikoppeling

Deze paragraaf bevat zeer beknopt een aantal hoofdpunten uit de overige documentatie.

Digikoppeling biedt de mogelijkheid om op een sterk gestandaardiseerde wijze berichten uit te wisselen tussen serviceaanbieders (service providers) en serviceafnemers (service requesters of consumers).

De uitwisseling tussen service providers en requesters wordt in drie lagen opgedeeld:

- Inhoud: op deze laag worden de afspraken gemaakt over de inhoud van het uit te wisselen bericht, dus de structuur, semantiek, waardebereiken etc.
Digikoppeling houdt zich niet met de inhoud bezig, 'heeft geen boodschap aan de boodschap'.
- Logistiek: op deze laag bevinden zich de afspraken betreffende transportprotocollen (HTTP), messaging (SOAP), beveiliging (authenticatie en encryptie) en betrouwbaarheid. Dit is de laag van Digikoppeling.
- Transport: deze laag verzorgt het daadwerkelijke transport van het bericht.

Digikoppeling richt zich dus uitsluitend op de logistieke laag. Deze afspraken komen in de koppelvlakstandaarden en andere voorzieningen.

Leidend principe (requirement)

De koppelvlakstandaarden dienen te leiden tot een maximum aan interoperabiliteit met een minimum aan benodigde ontwikkelinspanning. Daarom wordt gekozen voor bewezen interoperabele internationale standaarden.

Digikoppeling maakt berichtenuitwisseling mogelijk op basis van de ebXML/ebMS en WUS families van standaarden inclusief de daarbij behorende verwante standaarden.

Aan te sluiten overheidsorganisaties hebben aangegeven op een uniforme manier (één stekker) te willen aansluiten aan Digikoppeling. Organisaties die beschikken over eigen middleware (ESB, broker) kunnen de aansluiting aan Digikoppeling, de adapters, in het algemeen realiseren via voorzieningen in die middleware.

1.4 Koppelvlak & koppelvlakstandaard

Een koppelvlak is een interface die volgens vergaande standaarden de gegevensuitwisseling vastlegt. Het werken met vaste standaarden is essentieel voor een koppelvlak. Hierdoor wordt implementatie vergemakkelijkt. Ook wordt het mogelijk diverse soorten berichten door te sturen met een grote mate van interoperabiliteit, omdat via de standaard afspraken over hun inhoud gemaakt is.

Eén van de belangrijkste eisen die door de overheid gesteld worden bij de inrichting van generieke voorzieningen, is dat er niet veel maatwerk ontwikkeld hoeft te worden, maar dat er van "off the shelf" commercieel of OPEN geleverde software gebruik gemaakt kan worden. Voor Digikoppeling, dus voor de logistieke laag, betreft dat het niet willen ontwikkelen van software voor de adapters.

Dit doel kan bereikt (benaderd) worden doordat gekozen wordt voor internationale (de jure of de facto) vastgelegde standaarden, die door "alle" leveranciers interoperabel zijn geïmplementeerd.

Een andere eis is dat met name afnemers gebruik kunnen maken van één "stekker" (één logistiek koppelpunt). Aanbieders dienen hiervoor de nodige voorzieningen te treffen.

Specificatie van de koppelvlakstandaard

De koppelvlakspecificatie beschrijft de eisen die gesteld worden aan de adapters om interoperabel met elkaar te kunnen communiceren. Digikoppeling gaat over logistiek, dus over de envelop en niet over de inhoud. De hele set informatie die tezamen nodig is voor een complete generieke Digikoppeling koppelvlakdefinitie bestaat uit:

- Interfacedefinitie "on the wire", (voorbeeld)listing van SOAP headers en informatie over velden en hun specifieke inhoud.

De voor Digikoppeling vereiste interoperabiliteit van de WUS standaarden van OASIS en W3C wordt gebaseerd op de profielen (en tests) van OASIS WS-BRSP (voorheen WS-I).

1.5 Opbouw van dit document

Hoofdstuk 1 bevat een aantal algemene inleidende onderwerpen. Hoofdstuk 2 bevat de kern van de standaard. Deze is onderverdeeld naar onderwerpen/gebieden: WSDL, WS-Addressing, naamgeving, beveiliging, betrouwbaarheid en binaire data. Het identificeert de gekozen internationale (WS-I) profielen die dienen als fundament voor de Digikoppeling Koppelvlakstandaard WUS. Die keuzes, de nadere invullingen voor Digikoppeling binnen de ruimte van die standaarden/profielen en specifieke aandachtspunten bij de keuzes, vormen tezamen de "voorschriften" per onderwerp. Hoofdstuk 3 definieert de resulterende Digikoppeling WUS profielen.

Bijlage 1 bevat een voorbeeld XSD en WSDL.

Bijlage 2 bevat berichtvoorbeelden voor profiel Digikoppeling 2W-be (TLS).

Bijlage 3 bevat berichtvoorbeelden voor profiel Digikoppeling 2W-be (TLS) op basis van MTOM.

Bijlage 4 bevat berichtvoorbeelden voor profiel Digikoppeling 2W-be-S (TLS en ondertekening).

Bijlage 5 bevat berichtvoorbeelden voor profiel Digikoppeling 2W-be-S (TLS en ondertekening) op basis van MTOM.
Bijlage 6 bevat berichtvoorbeelden voor profiel Digikoppeling 2W-be-SE (TLS, ondertekening en versleuteling).
Bijlage 7 bevat berichtvoorbeelden voor profiel Digikoppeling 2W-be-SE (TLS, ondertekening en versleuteling) op basis van MTOM.
Bijlage 8 bevat de belangrijkste berichtvoorbeelden voor de Reliable profielen

Status

Dit document is een Definitief versie van de Digikoppeling Koppelvlakstandaard WUS 3.0.

Gehanteerde terminologie: Glossary

Voor de definities die binnen het Digikoppeling project gehanteerd worden, zie de 'Digikoppeling Glossary' via de onderstaande website.

Website

Dit document en andere documentatie is beschikbaar op www.logius.nl/digikoppeling.

2 Koppelvlakstandaard WUS

2.1 Inleiding

WUS is een acroniem voor WSDL, UDDI en SOAP: WUS dus. Daarmee wordt een familie van internationale standaarden van OASIS en W3C bedoeld; deze worden ook vaak met WS-* aangeduid. Deze standaarden gaan over application-to-application webservices, die informatie over heterogene middleware platforms en applicaties kunnen dragen.

Alle Digikoppeling webservices die op WUS gebaseerd zijn, moeten aan deze koppelvlakstandaard conformeren. Doel van de Koppelvlakstandaard WUS is het eenduidig en bruikbaar definiëren van het koppelvlak voor WUS. Er zijn daarvoor de volgende onderwerpen relevant: WSDL met adressering en naamgeving, beveiliging, betrouwbaarheid, binaire data, resulterende berichtheaders, profielen van Digikoppeling en compliancevoorzieningen. Deze standaard wordt verder aangevuld met "Best Practices" en adviezen, beschreven in een apart document. Alle documentatie over Digikoppeling is te vinden op de website www.logius.nl/digikoppeling.

WSDL

Een webservice wordt deels formeel en automatisch verwerkbaar gedefinieerd (beschrijving – description) door een WSDL. Deze WSDL geeft een beschrijving van de eisen die ten aanzien van de communicatie gesteld worden. Een WSDL kan onder andere bestaan uit meerdere schema definities in aparte XSD's en policy definities. Gezamenlijk vormt dit een abstracte definitie van de webservice. De webservice communiceert feitelijk door middel van SOAP berichten, die gegenereerd worden op basis van de WSDL. Adressering en naamgeving zijn specifieke aandachtsgebieden.

Resulterende berichtheaders

Deze standaard beschrijft per definitie aan welke eisen een Digikoppeling WUS implementatie moet voldoen. De praktijk leert dat dergelijke eisen vaak erg abstract zijn en dus gebaat zijn bij voorbeelden. Voorbeelden zijn gewenst zowel voor een mogelijk resulterende WSDL als voor de resulterende berichten, met name de headers – zie hoofdstuk 3.

2.1.1 *Wijzigingen in Digikoppeling 2.0 ten opzichte van Digikoppeling 1.0* Beveiliging

Deze versie van de koppelvlakstandaard schrijft beveiliging op transport niveau voor, volgens tweezijdige TLS. Aspecten die hierbij een rol spelen zijn in de "Point-to-Point beveiliging" paragraaf van hoofdstuk 2 opgenomen. Er wordt tevens de optie geboden om beveiliging op berichtniveau toe te passen, dit is in paragraaf "End-to-End beveiliging" van hoofdstuk 2 opgenomen.

Attachments (Binaire data)

Het is vaak gewenst om aan een XML-bericht een aantal binaire bestanden toe te voegen (zogenoemde attachments), zoals bijvoorbeeld documenten of afbeeldingen. Deze versie van de koppelvlakstandaard ondersteunt het versturen van binaire bestanden volgens de MTOM standaard, of opgenomen als base64binary in de payload van het bericht. Voor het

versturen van grote attachments is het mogelijk om gebruik te maken van Koppelvlakstandaard Grote Berichten.

2.1.2 *Wijzigingen in Digikoppeling 3.0 ten opzichte van Digikoppeling 2.0*

Reliable messaging

Reliable messaging is een belangrijke uitbreiding op digikoppling 2.0. Zoals beschreven ondersteunt Digikoppeling zowel ebMS als WUS voor berichtuitwisseling. WUS werd voorheen enkel gebruikt om bevraging te doen en was niet geschikt om meldingen te doen omdat binnen de standaard nog geen reliability was toegevoegd. Met Digikoppeling 3.0 is WS-RM toegevoegd binnen de WUS standaard inclusief de bijbehorende Digikoppeling profielen. Hiermee is het mogelijk om betrouwbare meldingen met de WUS standaard te doen.

Non-repudiation

WS-Security is sinds Digikoppeling 2.0 toegevoegd. Hierbij werd enkel gebruik gemaakt van WS-Security versie 1.0. Sinds versie 1.1 van WS-Security is een extra element 'signatureConfirmation' toegevoegd dat antwoord geeft op een tweezijdig 'non-repudiation' vraag. Digikoppeling 3.0 heeft dit element toegevoegd in de standaard en hiermee dus ook WS-Security 1.1.

2.2 **Ondersteunde varianten**

Om redenen van interoperabiliteit, eenvoud en overzichtelijkheid onderscheidt deze Digikoppeling Koppelvlakstandaard een drietal varianten van uitwisselingen. Elke variant veronderstelt bepaalde voorgedefinieerde keuzes voor parameters als synchroniciteit, beveiliging en betrouwbaarheid en is daarmee een "profiel" voor WUS.

Elke uitwisseling op basis van de WUS-protocollen over Digikoppeling 3.0 zal moeten voldoen aan één of een combinatie van de volgende Digikoppeling WUS-varianten:

- **Best Effort:** dit zijn synchrone uitwisselingen die geen faciliteiten voor betrouwbaarheid (ontvangstbevestigingen, duplicaateliminatie etc.) vereisen. Voorbeelden zijn toepassingen waar het eventueel verloren raken van sommige berichten niet problematisch is en waar snelle verwerking gewenst is.
- **End-to-End Security:** zowel op Best Effort als Reliable basis wordt een bericht beveiligd tussen de uiteindelijke consumer en de uiteindelijke provider, ook wanneer er zich intermediairs bevinden in het pad tussen die twee. Het betreft hier authenticatie van de consumerorganisatie, conform het Digikoppeling authenticatiemodel, waarbij alleen de identiteit van de consumerorganisatie relevant is, en encryptie van het bericht (payload inclusief attachments) onderweg. Voor de authenticatie en encryptie wordt gebruikgemaakt van WS-Security.
- **Reliable Messaging:** dit zijn asynchrone uitwisselingen die ondersteuning bieden voor betrouwbaarheid. Hiermee is het mogelijk om binnen WUS een melding met End-to-End security met een hoge betrouwbaarheidsgraad te bieden. Bij End-to-End security wordt het bericht gesigneerd door de verzender waarbij de ontvanger een bevestiging terug stuurt ter invulling van een non-repudiation eis.

NB. De versies WUS Digikoppeling 1.0 en WUS Digikoppeling 1.1 ondersteunen alleen Best Effort. WUS Digikoppeling 2.0 bevat zowel Best Effort als End-to-End Security. WUS Digikoppeling 3.0 biedt bovendien Reliable Messaging.

Voor alle profielen gelden de volgende eigenschappen:

- Attachments: één of meerdere bijlagen, naast natuurlijk het reeds bestaande (xml) bericht zelf. Dit kan, maar hoeft niet, toegepast te worden in combinatie de bovengenoemde profielen: het is dus optioneel.
NB. De versies Digikoppeling 1.0 en Digikoppeling 1.1 ondersteunden géén attachments! (Gebruik van Base64 encoded xml elementen is natuurlijk wel mogelijk.)
- Vertrouwelijkheid en authenticatie van zender en ontvanger wordt als volgt gerealiseerd:
 - voor Point-to-Point Security, door middel van twee-zijdig TLS op transport-niveau (in het HTTP kanaal). (De toepassing ervan is verplicht op alle Digikoppeling versies.)
 - voor End-to-End Security, door middel van signing (ondertekening) en (optioneel) encryptie (versleuteling) op berichtniveau (payload inclusief de attachments, ook wel 'bijlagen' genoemd) in combinatie met (point-to-point) twee-zijdig TLS in het HTTP kanaal. NB. De versies Digikoppeling 1.0 en Digikoppeling 1.1 ondersteunen géén End-to-End security.

De onderstaande tabel geeft in essentie de eigenschappen van de verschillende Digikoppeling 3.0 profielen weer. Voor alle profielen wordt tweezijdig TLS gebruikt op transportniveau (HTTPS).

Profile Names			Transport characteristics				
Digikoppeling 3.0 WUS			2-zijdig TLS	Signed	Encrypted	Reliable	Attachments
Best Effort		Digikoppeling 2W-be	✓	—	—	—	Optional
End-to-End Security	Best Effort – Signed	Digikoppeling 2W-be-S	✓	✓	—	—	Optional
	Best Effort – Encrypted	Digikoppeling 2W-be-SE	✓	✓	✓	—	Optional
Reliable		Digikoppeling 2W-R	✓	—	—	✓	Optional
End-to-End Security	Reliable – Signed	Digikoppeling 2W-R-S	✓	✓	—	✓	Optional
	Reliable – Encrypted	Digikoppeling 2W-R-SE	✓	✓	✓	✓	Optional

Compliancevoorzieningen

Voor de Digikoppeling Koppelvlakstandaard WUS zijn ook compliancevoorzieningen beschikbaar gesteld, waarmee een ontwikkelaar kan testen "of het werkt". Deze compliancevoorzieningen zijn gedefinieerd aan de hand van de WSDL's die via Digikoppeling website beschikbaar zijn.

De volgende compliancevoorzieningen zijn beschikbaar:

- Digikoppeling service requester compliancevoorziening: wordt gebruikt om een ontwikkelde servicere requester (client) te testen.
- Digikoppeling service provider compliancevoorziening: wordt gebruikt om een ontwikkelde service provider (service) te testen.

De documenten over de compliancevoorzieningen zijn te vinden op de Digikoppeling website.

2.3 Gehanteerde standaarden

In dit hoofdstuk worden de verschillende versies van de onderliggende internationale standaarden vermeld.

Overwegingen

Primair wordt gekozen voor de interoperabele profielen van OASIS WS-BRSP (voorheen WS-I). Het gaat dan om WS-I Basic Profile (BP) 1.2, een set specificaties van webservices die interoperabiliteit bevorderen. Digikoppeling kiest voor standaarden die algemeen interoperabel beschikbaar zijn, dat wil zeggen interoperabel geïmplementeerd zijn in het grootste deel van de (ontwikkel) tools. De kans daarop is groter bij "final" standaarden dan bij drafts. Digikoppeling kiest daarom voor WS-I Standaarden met status final. Alleen indien er een zeer dringende reden is, wordt voor (delen uit) een standaard met status Draft gekozen.

De status (maart 2013) van de diverse "deliverables" van deze WS-I organisatie is als volgt:

- WS-I BP 1.1 heeft de status "final"; in deze standaard is nog een beperkt aantal onderwerpen opgenomen. Deze zijn gebaseerd op onderliggende standaarden als WSDL 1.1, SOAP 1.1 en UDDI.
- WS-I BP 1.2 is in November 2010 final. In deze versie zijn zaken als WS-addressing en MTOM (attachments) opgenomen.
- WS-I heeft sinds november 2010 een final versie uitgebracht van BP 2.0. Ook in deze versie zal expliciet niet met WSDL 2.0 gewerkt worden.
- WS-I Basic Security Profile (BSP) 1.0 is beschikbaar met status final sinds 30 maart 2007; BSP 1.0 verwijst naar BP 1.0 en 1.1.
- BSP 1.1 is final sinds januari 2010.
- WS-I als losse organisatie is sinds november 2010 opgeheven en alle specificaties zijn onder gebracht in OASIS. OASIS heeft hiervoor een committee opgericht, namelijk WebService Basic Reliable Secure Profiles (WS-BRSP). De profielen heten vooralsnog WS-I profielen.

Resulterende beslissingen ten aanzien van standaarden

Gekozen wordt in Digikoppeling versie 3.0:

- WS-I BP 1.2; deze is gebaseerd op onderliggende standaarden: SOAP 1.1, WSDL 1.1 en de te kiezen onderdelen van WS-Addressing en MTOM.
- WS-I BSP 1.1 voor berichtbeveiliging op basis van WS-Security.
- TLS 1.0, conform de aanbevelingen in WS-I BSP 1.0 voor beveiliging op transport/kanaal niveau en aanbevelingen van NIST.
- WS-I Simple SOAP Binding Profile Version 1.0.
- WS-I Reliable Secure Profile Version 1.0

Bovenstaande standaarden zijn gebaseerd op diverse onderliggende standaarden. Gevolg is dat de Digikoppeling WUS standaard versie 3.0 gebruikmaakt van de volgende set van standaarden:

Standaarden	Gevolg van onder andere
HyperText Transfer Protocol 1.1 (RFC2616)	WS-I Basic Profile 1.2
SOAP 1.1	WS-I Basic Profile 1.2
WSDL 1.1	WS-I Basic Profile 1.2
XML 1.0 (Second Edition)	WS-I Basic Profile 1.2
XML Schema Part 1: Structures	WS-I Basic Profile 1.2
XML Schema Part 2: Data types	WS-I Basic Profile 1.2
TLS 1.0 (RFC2246)	WS-I Basic Profile 1.2
HTTP over TLS Transport Layer Security (RFC2818)	WS-I Basic Profile 1.2
Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 3280)	PKI overheid 1.1
WS-Security 1.0	WS-I Basic Security Profile 1.1
WS-Addressing 1.0	WS-I Basic Profile 1.2
Web Services Addressing 1.0 – Metadata	WS-I Basic Profile 1.2
SOAP 1.1 Binding for MTOM 1.0	WS-I Basic Profile 1.2
WS-Security 1.1	WS-I Basic Security Profile 1.1
WS-ReliableMessaging 1.1	WS-I Reliable Secure Profile 1.0

2.4 Voorschriften

De inhoud van de Digikoppeling standaard vloeit voort uit bovengenoemde standaarden, of vormt een nadere invulling daarvan (een keuze uit toegestane mogelijkheden in die standaarden).

In de paragrafen hierna worden die onderdelen achtereenvolgens behandeld:

- WSDL,

- WS-Addressing,
- Binaire data,
- Beveiliging,
- Betrouwbaarheid,
- Namespace.

2.4.1

Service definitie WSDL

Voorschriften ten gevolge van de keuze voor BP 1.2

Nr	Omschrijving
WW001	Voor de SOAP berichten wordt SOAP 1.1 en "document-literal binding" gehanteerd. Hierbij wordt als transport binding HTTP voorgeschreven.
WW002	Door het opleggen van het SOAP style type "document/literal" zal de inhoud van de berichten beschreven worden door XML en geen afgeleide daarvan. Dit houdt in dat er niet een eigen mapping mag worden geïntroduceerd voor encoding types zoals bijvoorbeeld bij SOAP encoding het geval is. Kortom, de datatypen moeten voldoen aan de XML Schema Part 2: Datatypes
WW003	Bij document -literal mag het SOAP "body" element slechts 1 XML element bevatten. Hierbinnen kunnen eventueel wel meerdere elementen opgenomen worden.
WW004	<p>Basic Profile stelt eisen aan het "PortType" van een WSDL. Hierbij mogen de "parts" van de "messages" alleen een "element" bevatten (geen "parts" die een "type" attribuut gebruiken). "R2204 A document-literal binding in a DESCRIPTION MUST refer, in each of its soapbind:body element(s), only to wsdl:part element(s) that have been defined using the element attribute." Er is geen voorbeeld bij WS-I, maar een voorbeeld kan zijn:</p> <pre> <element name="TradePriceRequest"> <complexType> <all> <element name="tickerSymbol" type="string"/> </all> </complexType> </element> ... <message name="GetLastTradePriceInput"> <part name="body" element="xsd1:TradePriceRequest"/> </message> </pre>

Aanvullende voorschriften (dus specifieke Digikoppeling-invulling binnen de ruimte van een bovengenoemde standaard)

Nr	Omschrijving
WS001	Er kunnen meerdere operaties per webservice gedefinieerd worden.
WS002	De SOAPAction aanduiding in de WSDL wordt gevuld met een lege string (""), wordt weggelaten, of heeft dezelfde vulling als de {http://www.w3.org/2007/05/addressing/metadata}Action in de WSDL. In de HTTP Header van het bericht moet de SOAPAction een lege string met quotes zijn (""), of een waarde hebben gelijk aan de WS-Addressing Action (wsa:Action).
WS003	De Digikoppeling WUS ondersteunt alleen de zogenaamde "request/response" berichtenuitwisseling (zie WSDL 1.1 specificatie paragraaf "2.4 Port Types").
WS005	De WSDL bevat slechts één "portType" per WSDL bestand.
WS006	Digikoppeling ondersteunt alleen UTF-8.
WS007	In de header zijn geen eigen velden (header blocks) toegestaan. De header bevat alleen de in het betreffende profiel vastgestelde velden, die dus uitsluitend gedefinieerd zijn in het betreffende WS-I profiel (respectievelijk de onderliggende OASIS/W3C standaarden).
WS008	Het is verplicht een WS-Addressing Action referentie op te nemen in de WSDL. Het definiëren van een WS-Addressing action in WSDL kan met behulp van de Web Services Addressing 1.0 – Metadata standaard. Informatie hierover is te vinden via http://www.w3.org/TR/2007/REC-ws-addr-metadata-20070904/#explicitaction . Zie voor mogelijke vulling van wsam:action in WSDL "4.4.4 Default Action Pattern for WSDL 1.1" van de Web Services Addressing 1.0 – Metadata standaard (http://www.w3.org/TR/2007/REC-ws-addr-metadata-20070904/).

2.4.2

WS-Addressing

Voorschriften als gevolg van het toepassen van WS-Addressing

Nr	Omschrijving
WA001	<p>Digikoppeling WUS gebruikt de volgende velden uit WS-Addressing :</p> <p>wsa:To wsa:Action wsa:MessageID wsa:RelatesTo wsa:ReplyTo wsa:From</p> <p>De communicatie binnen het Digikoppeling domein is voor een deel afhankelijk van de toepassing van WS-Addressing velden. Aangezien er meerdere WS-Addressing specificaties zijn, die onder meer verschillende namespaces kunnen hebben, is er voor gekozen om alleen de specificatie van 2005/08 (http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/) of van 2006/05 (http://www.w3.org/TR/ws-addr-core/) verplicht te stellen in de berichten binnen het Digikoppeling domein. Hieronder wordt de toepassing van de verschillende velden toegelicht.</p> <p>Er is gekozen voor een zo klein mogelijke subset uit de WS-Addressing standaard om de kans op interoperabiliteitsissues te minimaliseren. Met het toepassen van deze standaard wordt het "achter de voordeur" routeren mogelijk.</p>

wsa:To

Dit wordt gebruikt om de endpoint vast te leggen waar het bericht naar toe dient te gaan.

De wsa:To is van het type wsa:EndPointReferenceType en dient gevuld te worden met een 'Adres' element. De waarde van het adres element kan hetzij een absolute URI zijn of

"http://www.w3.org/2005/08/addressing/anonymous". Voor asynchrone berichten (meldingen) via WUS dient het To-adres aangevuld te worden met een OIN door het gebruik van querystring parameters (e.g. <http://service-end-point?oin=xxxxxx>). De waarde van de oin in het adres is het oin nummer van de ontvangende partij.

wsa:Action

Deze waarde wordt gebruikt om een specifieke operatie aan te roepen. Deze waarde is terug te vinden in de WSDL van de betreffende aan te roepen webservice van de Service Provider. Dit veld is verplicht en moet in het bericht worden opgenomen.

wsa:MessageID

De waarde hiervan kan door de service requester of provider zelf ingevuld worden zolang dit een waarde is die aan de onderliggende specificatie voldoet (<http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/>).

wsa:RelatesTo

Dit element komt alleen voor in de SOAP header van het response bericht. Het bevat de waarde van de wsa:MessageID van het request bericht.

wsa:ReplyTo

De verplichte specificatie van wsa:ReplyTo geldt alleen voor het request bericht. De specificatie mag zowel plaatsvinden door gebruik te maken van de default-waarde als door expliciete opname van deze SOAP-header.

Voor zowel synchrone communicatie t.b.v. bevestigingen als asynchrone communicatie t.b.v. meldingen zal het replyTo veld gevuld zijn met de waarde <http://www.w3.org/2005/08/addressing/anonymous> of het element volledig weglaten. Bij weglaten van dit veld moet de ontvanger conform WS-Addressing specificatie alsnog de waarde "http://www.w3.org/2005/08/addressing/anonymous" gebruiken.

wsa:From

Het gebruik van wsa:From is optioneel voor synchrone berichten voor bevestigingen. De waarde van dit veld wordt gebruikt om aan te geven waar het bericht vandaan komt. De wsa:From is van het type wsa:EndPointReferenceType en dient gevuld te worden met een 'Adres' element. De waarde van het adres element kan hetzij een absolute URI zijn of "http://www.w3.org/2005/08/addressing/anonymous".

Voor asynchrone berichten via WUS dient het From-adres aangevuld te worden met een OIN door het gebruik van querystring parameters (e.g. <http://service-end-point?oin=xxxxxx>). De waarde van de oin in het bericht is het oin nummer van de verzendende partij.

De elementen wsa:To, wsa:ReplyTo en wsa:From zijn allen van de type 'wsa:EndPointReferenceType'. Dit type stelt enkel het element 'Address' verplicht. De overige velden zijn optioneel en zijn om compatibiteitsredenen niet toegestaan binnen Digikoppeling.

Het is toegestaan om overige WS-Addressing velden op te nemen in de berichten omdat bij sommige toolkits het genereren van deze velden niet onderdrukt kan worden. Hierbij geldt wel de beperking dat de waarde voor deze velden het routeringsmechanisme niet verstoort. Derhalve moet, indien het bericht andere velden dan hierboven bevat, de waarde "http://www.w3.org/2005/08/addressing/anonymous" of "http://www.w3.org/2005/08/addressing/none" aan deze velden toegekend worden.

Overzicht verplichte WS-Addressing properties in request en response berichten (volgens <http://www.w3.org/TR/2007/REC-ws-addr-metadata-20070904/>):

WS-Addressing request headers

Field	Property	Mandatory	Description
-------	----------	-----------	-------------

wsa:To	[destination]	Y	Provides the address of the intended receiver of this message.
wsa:Action	[action]	Y	Identifies the semantics implied by this message.
wsa:From	[source endpoint]	Y ¹	Provides the address of the original sender of this Message
wsa:ReplyTo	[reply endpoint]	Y ²	Intended receiver for the reply to this message.
wsa:FaultTo	[fault endpoint]	N	Intended receiver for faults related to this message. May be included to direct fault messages to a different endpoint than [reply endpoint].
wsa:MessageID	[message id]	Y	Unique identifier for this message. Used in the [relationship] property of the reply message.
wsa:RelatesTo	[relationship]	N	Indicates relationship to a prior message. Unused in this MEP, but could be included to facilitate longer running message exchanges.

WS-Addressing response headers

Field	Property	Mandatory	Description.
wsa:To	[destination]	Y	Provides the address of the intended receiver of this message.
wsa:Action	[action]	Y	Identifies the semantics implied by this message.
wsa:From	[source endpoint]	N	Message origin. Unused in this MEP, but could be included to facilitate longer running message exchanges.
wsa:ReplyTo	[reply endpoint]	N	Intended receiver for replies to this message. Unused in this MEP, but could be included to facilitate longer running message exchanges.
wsa:FaultTo	[fault endpoint]	N	Intended receiver for faults related to this message. Unused in this MEP, but could be included to facilitate longer running message exchanges.
wsa:MessageID	[message id]	Y*	Unique identifier for this message. Unused in this MEP, but may be included to facilitate longer running message exchanges.
wsa:RelatesTo	[relationship]	Y	Indicates that this message is a reply to the request message, using the request message [message id] value and the predefined http://www.w3.org/2005/08/addressing/reply IRI.

* Hiermee wordt afgeweken van wat de Web Services Addressing 1.0 – Metadata standaard voorschrijft. Volgens deze standaard is de MessageID in response optioneel.
Bovenstaande properties kunnen in een aantal gevallen ook gespecificeerd worden door betreffende velden in de header weg te laten³.

2.4.3

Binaire Data

Met het toestaan van MTOM/XOP worden er in de nieuwe versie van Digikoppeling Koppelvlakstandaard WUS twee mogelijkheden ondersteund

¹ Source endpoint is verplicht voor asynchrone meldingen. Voor bevestigingen is het optioneel.

² Impliciet specificeren van het reply endpoint door weglaten van ReplyTo is ook toegestaan.

³ Zie WS-addressing 1.0- Core, paragraaf 2.1 en paragraaf 3.2; zie ook BP 1.2 paragraaf 3.7.14.

om binaire data te versturen. Dat zijn Base64Binary (Base64Binary in payload element van het bericht) of MTOM (MIME wrappers waarbij binaire data in een aparte Multipart/Related pakket is opgenomen). Bij het toepassen van MTOM wordt er ook wel gesproken van een geoptimaliseerd bericht.

De meest gangbare toolkits kunnen MTOM berichten ontvangen en versturen. Het wel of niet toepassen van MTOM kan vaak vanuit de code of middels een configuratiebestand geregeld worden. Aan de web service kan aangegeven worden of deze MTOM berichten kan ontvangen en versturen. Gezien het gebruik van MTOM door de web service requester bepaald wordt, moeten alle Digikoppeling 2 web service implementaties dit ondersteunen. Concreet betekent dit dat in de toolkit wordt aangegeven dat een web service een response volgens MTOM verstuurt indien deze een MTOM request heeft ontvangen en een niet geoptimaliseerd bericht verstuurt indien het request ook niet geoptimaliseerd was. De web service requester neemt dus het initiatief hierin.

Nr	Omschrijving
WM001	Toepassen MTOM wordt door web service requester bepaald.

2.4.4

Beveiliging

In deze versie wordt Point-to-Point en End-to-End beveiliging ondersteund. Point-to-Point beveiliging wordt uitgevoerd op basis van TLS, End-to-End beveiliging op basis van WS-Security 1.0 of WS-Security 1.1.

Point-to-Point beveiliging

Deze beveiliging zorgt ervoor dat het volledige bericht en het http-protocol is beveiligd tijdens het transport van verzender naar ontvanger. Alle Digikoppeling profielen verplichten point-to-point beveiliging. Hierbij gelden de volgende voorschriften:

Nr	Omschrijving
WT001	Authenticatie op transport niveau gebeurt op basis van TLS V1.0 met tweezijdige authenticatie. Client and Server authenticatie is vereist gebruikmakend van HTTPS and TLS 1.0 [RFC 2246]. De TLS implementatie mag niet op SSL v3 terug kunnen vallen.
WT002	De te gebruiken certificaten in de productie omgeving voldoen aan de eisen van PKIoverheid (PvE 3b) en de inhoud van de identificerende velden in het certificaat dienen te voldoen aan de afspraken als gesteld in de functionele eisen Authenticatie Digikoppeling. Met het toepassen van PKIoverheid-certificaten die Digikoppeling compliant zijn, wordt hieraan voldaan.
WT003	De onderstaande TLS encryptie algoritmen en sleutellengtes MOETEN minimaal worden ondersteund: 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
WT004	De geldigheid van het certificaat wordt getoetst met betrekking tot de geldigheidsdatum en de

	Certificate Revocation List(CRL) die voldoet aan de eisen van PKI-overheid.
WT005	De betreffende CRL dient zowel voor de versturende als ontvangende partij te benaderen zijn.
WT006	Voor communicatie over HTTPS wordt port 443 gebruikt.
WT007	Binnen een TLS-sessie kunnen meerdere berichten verstuurd worden.
WT008	Voor de TLS-sessie moet een maximale duur gelden, na het verloop hiervan wordt de verbinding verbroken. Partijen zijn vrij om de maximale duur zelf te bepalen.

End-to-End beveiliging.

Deze beveiliging is optioneel en wordt bovenop point-to-point beveiliging ingezet op SOAP niveau met behulp van ondertekening en versleuteling. End-to-End beveiliging is primair van toepassing in de scenario's waar intermediairs betrokken zijn gedurende de gegevensuitwisseling en in scenario's waarbij onweerlegbaarheid van belang is.

Nr	Omschrijving
WB001	Toepassen WS-Security 1.0 en WS-Security 1.1
	<p>Overwegingen:</p> <p>Basic Security Profile 1.1 is sinds 2010 november final geworden. Hierin worden zowel de WS-Security 1.0 als de WS-Security 1.1 namespaces beide gebruikt. WS-Security 1.1 heeft een extra signatureConfirmation element toegevoegd die verplicht is voor meldingen. Bij gebruik van dit element zal de webservice een signatureConfirmation terug sturen naar de verzender ter bevestiging van correct ontvangst (non-repudiation).</p>
WB002	<p>Toepassen van Timestamp in security header met Timestamp Created is verplicht. Timestamp Expires is optioneel.</p> <p>Timestamp Created Verplicht onderdeel van een Timestamp.</p> <p>Timestamp Expires Optioneel onderdeel van een Timestamp.</p> <p>Timestamp tijd De tijdstamp moet een Universal Time Coordinated (UTC) tijdzone aanduiding hebben. Bij het toepassen van een timestamp gaat tijdsynchronisatie van de verschillende communicerende systemen een rol spelen. Indien dit niet mogelijk is moet hiermee met de vulling van de Created en Expires rekening worden gehouden door middel van een "timestampSkew".</p>
	<p>Overwegingen:</p> <p>Bij toepassen van Timestamp Expires is tijdsynchronisatie van belang. Om mogelijke problemen hiermee te voorkomen, zou er overwogen kunnen worden om een eis op te nemen dat de Expires niet in Timestamp opgenomen mag worden. Omdat het expliciet weglaten van de Expires niet in alle tooling mogelijk is, wordt hiervoor niet gekozen. Tevens kan het zijn dat door het ontbreken van tijdsynchronisatie er problemen zijn met de Timestamp Created, in de situatie waarbij de ontvanger heeft vastgesteld dat de Timestamp Created in de toekomst ligt. Hiervoor biedt tooling vaak een "timestampSkew". Deze geeft de toegestane afwijking ten opzichte van UTC aan.</p>

WB003	Indien WS-Security wordt toegepast, is ondertekenen verplicht en versleutelen optioneel (keuze profiel Digikoppeling 2W-be-S, Digikoppeling 2W-be-SE, Digikoppeling 2W-R-S of Digikoppeling 2W-R-SE).	
	<p>Overwegingen:</p> <p>De berichten kunnen zowel ondertekend als versleuteld worden. Gezien het doel van WS-Security, te weten het "door een intermediair heen" kunnen doorgeven van authenticatie-informatie, is ondertekenen primair van belang; daarmee is ook onweerlegbaarheid geregeld. Uiteraard kan het in een bepaalde situatie ook een eis zijn dat het bericht niet leesbaar is voor de intermediair.</p>	
WB004	Ondertekenen van bericht onderdelen SOAP:body, SOAP:headers (WS-Addressing headers en Timestamp) is verplicht bij toepassing van End-to-End beveiliging.	
	<p>Overwegingen:</p> <p>Met het ondertekenen wordt authenticatie, integriteit en onweerlegbaarheid ondersteund. Het is van belang dat de integriteit en onweerlegbaarheid van de inhoud en header van het bericht kan worden vastgesteld, de SOAP:body, SOAP:header (WS-Addressing en het Timestamp element) zullen dus ondertekend moeten worden.</p>	
WB005	Bij toepassen van versleutelen geldt dit voor de volgende bericht onderdelen: SOAP:body	
	<p>Overwegingen:</p> <p>De WS-Addressing headers worden niet versleuteld, dit omdat deze anders niet leesbaar zijn voor intermediairs. De wsa:Action en de ondertekening worden dus niet versleuteld. Ook de SOAPAction kan niet afgeschermd worden. Door beveiliging op transport niveau is het risico van een niet afgeschermd wsa:Action en SOAPAction tot een minimum beperkt.</p>	
WB006	Berichten worden eerst ondertekend en vervolgens versleuteld.	
	<p>Overwegingen:</p> <p>Omdat er zowel wordt ondertekend als versleuteld, moet de volgorde hiervan gespecificeerd worden. Het voorstel is om eerst te ondertekenen en dan te versleutelen.</p>	
WB007	Technische gegevens ten behoeve van ondertekenen:	
	Parameter	Waarde
	Onderteken optie Algoritme	Exclusive XML Canonicalization (http://www.w3.org/2001/10/xml-exc-c14n#)
	DigestMethodAlgo rithm	SHA-1 (http://www.w3.org/2000/09/xmldsig#sha1)
	SignatureMethodA lgorithm	SHA-1 (http://www.w3.org/2000/09/xmldsig#hmac-sha1 of http://www.w3.org/2000/09/xmldsig#rsa-sha1)
WB008	Technische gegevens ten behoeve van versleutelen:	
	Parameter	Waarde

	<table><tr><td>Data Encryption Algorithms</td><td>3DES (http://www.w3.org/2001/04/xmlenc#tripledes-cbc) of AES128 (http://www.w3.org/2001/04/xmlenc#aes128-cb) of AES256 (http://www.w3.org/2001/04/xmlenc#aes256-cbc)</td></tr><tr><td>Key Transport Algorithms</td><td>RSA-1_5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5) of RSA-OAEP (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p)</td></tr></table>	Data Encryption Algorithms	3DES (http://www.w3.org/2001/04/xmlenc#tripledes-cbc) of AES128 (http://www.w3.org/2001/04/xmlenc#aes128-cb) of AES256 (http://www.w3.org/2001/04/xmlenc#aes256-cbc)	Key Transport Algorithms	RSA-1_5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5) of RSA-OAEP (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p)	
Data Encryption Algorithms	3DES (http://www.w3.org/2001/04/xmlenc#tripledes-cbc) of AES128 (http://www.w3.org/2001/04/xmlenc#aes128-cb) of AES256 (http://www.w3.org/2001/04/xmlenc#aes256-cbc)					
Key Transport Algorithms	RSA-1_5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5) of RSA-OAEP (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p)					
WB009	Security token X.509 Certificate Token (PKI Overheid Digikoppeling certificaat).					
WB010	Publieke sleutel dat gebruikt is voor het signing proces dient meegeleverd te worden met het bericht via een 'Direct security token' reference.					
	Overwegingen: Het certificaat wordt in het bericht meegestuurd. Hiermee kan de ontvanger door middel van het meegeleverd certificaat de handtekening controleren. Het certificaat dient uiteraard wel vertrouwd te zijn via een truststore configuratie.					
WB011	Het toepassen van End-to-End beveiliging wordt op serviceniveau aangeduid. Alle operaties en dus berichten (request en response) worden ontsloten volgens één bepaald Digikoppeling profiel.					
	Overwegingen: Beveiligingseisen kunnen op het niveau van het bericht gedefinieerd worden, maar niet alle toolkits kunnen hiermee overweg. Totdat alle belangrijke toolkits dit wel kunnen, is het beter om bericht beveiliging op serviceniveau te definiëren. Beveiligingseisen op webserviceniveau vereenvoudigt tevens de registratie in het Digikoppeling Service Register.					
WB012	Voor het versleutelen van het responsebericht wordt het certificaat in het requestbericht gebruikt.					
	Toelichting: In eis WB010 wordt aangegeven dat het certificaat voor ondertekening in het bericht wordt opgenomen. Indien een web service wordt ontsloten volgens het Digikoppeling 2W-be-SE of 2W-R-SE profiel moet deze op basis van het requestbericht kunnen bepalen welk certificaat gebruikt moet worden om de payload van de response te versleutelen. Dit kan door het certificaat in het requestbericht te gebruiken voor versleuteling van de response. Ook de requester dient hier dus rekening mee te houden bij ontsleutelen van het responsebericht. Om het request bericht initieel te versleutelen dient de publieke sleutel van de ontvangende partij al in de truststore geregistreerd te zijn.					

Een contract wordt voor een Digikoppeling WUS Koppelvlak gedefinieerd door een WSDL. De WSDL 1.1 specificatie op zich biedt geen mogelijkheden om het gebruik van WS-Security aan te geven. De WSDL-specificatie is wel extensible en er zijn standaarden waarin het gebruik van WS-Security kan worden aangegeven. Dit zijn:

- WS-Policy (versie 1.2 / 1.5),
- WS-PolicyAttachment (1.2/1.5),
- WS-SecurityPolicy 1.1,
- WS-SecurityPolicy 1.2,

- WS-SecurityPolicy 1.3

Van deze standaarden bestaan dus ook weer verschillende versies. Het voordeel om deze specificaties toch toe te passen, is dat toolkits deze specificaties kunnen consumeren en daardoor berichten conformeren aan de betreffende policies. Deze worden nog onvoldoende breed ondersteund om interoperabiliteit te garanderen. Daarom zullen er best practices komen die de verschillende combinaties ten aanzien van WS-Security beschrijven in WS-SecurityPolicy 1.1 en/of 1.2 policies. Deze kunnen mogelijk een eenvoudige basis vormen voor een Digikoppeling 2W-be-S of Digikoppeling 2W-be-SE implementatie. Mocht de toolkit deze policies niet ondersteunen, dan kunnen ze wellicht gebruikt worden bij de handmatige configuratie hiervan.

2.4.5

WS-Reliable Messaging

WS-Reliable Messaging is een standaard om een succesvolle bericht aflevering te garanderen tussen twee endpoints. Het omschrijft een protocol waar d.m.v. van een message identifier in combinatie met een sequence nummer bepaald kan worden of een bericht is ontvangen. Indien een bericht niet ontvangen is, zal het automatisch opnieuw verstuurd worden naar de bestemming. Voor het gebruik van deze standaard, gelden de volgende voorschriften:

Nr	Omschrijving
WR001	Toepassen WS-ReliableMessaging 1.1
	<p>Overwegingen:</p> <p>WS-ReliableMessaging kende voorheen twee verschillende stromingen, namelijk WS-ReliableMessaging en WS-Reliability. WS-Reliability was buiten de OASIS groep opgezet en was in 2005 ondergebracht bij OASIS. Deze versie is door OASIS omgedoopt tot WS-Reliable Messaging 1.0. OASIS heeft vervolgens in 2007 versie 1.1 uitgebracht waarin beide stromingen zijn verwerkt tot 1 standaard. In 2009 is versie 1.2 uitgebracht met kleine aanpassingen waaronder de verwijzing naar de final WS-policy 1.5 standaard.</p> <p>In RSP 1.0 is opgenomen dat WS-RM 1.2 gebruikt dient te worden. Hoewel het verschil tussen 1.1 en 1.2 enkel een indirecte policy verwijzing is met geen functionele impact, hebben vele implementaties nog geen officiële statement met ondersteuning van WS-RM 1.2. Om deze reden is de voorgeschreven versie 1.1 voor Digikoppeling 3.0. Omdat er geen functionele verschillen zijn, wordt RSP 1.0 t.o.v. WS-ReliableMessaging eisen wel als maatstaf gehouden met uitzondering van het gebruik van WS-RMP. Het gebruik van policies binnen Digikoppeling is namelijk optioneel.</p>
WR002	Implementatie van WS-ReliableMessaging dient te voldoen aan de voorwaarden die beschreven zijn in de Reliable Secure Profile 1.0.
	<p>Overwegingen:</p> <p>Zoals beschreven in WR001 is de gekozen WSRM 1.1 versie afwijkend ten opzicht van RSP 1.0. Ondanks deze afwijking, worden de gestelde interoperabele voorwaarden in RSP m.b.t. WS-RM als standaard gehandhaafd.</p> <p>RSP 1.0 bevat naast WS-RM ook voorschriften voor Secure Conversation en Make Connection. Om praktische redenen maakt Digikoppeling enkel gebruik van de</p>

	WS-RM onderdeel. Voor beveiliging volgt Digikoppeling de richtlijnen zoals deze beschreven staan in de vorige hoofdstuk.
WR003	Ondertekenen van wsrn:Sequence header onderdelen is verplicht bij toepassing van het reliable profiel inclusief signing
	Overwegingen: Om de mogelijkheid tot DoS attacks en sequence attacks te voorkomen is bij Reliable secure beveiliging de ondertekening van de sequence headers verplicht.
WR004	Delivery Assurance 'InOrder' dient altijd in combinatie zijn met een 'ExactlyOnce' strategie
	Overwegingen: WS-ReliableMessaging bevat de mogelijkheid om de delivery assurance te bepalen door middel van policies of framework specifieke configuratie. Behalve garantie van aflevering kan hiermee ook worden afgedwongen dat berichten op volgorde van versturing worden verwerkt. Hiervoor dient de delivery assurance type 'InOrder' gebruikt te worden. Deze moet ten alle tijde gecombineerd zijn met de 'exactlyOnce' delivery type om bericht verlies te voorkomen. Indien er geen policies gebruikt worden, zal via WSDL documentatie elementen in de WSDL duidelijk gemaakt worden welke assurance type door de server gehonoreerd wordt.
WR005	WS-ReliableMessaging dient altijd in combinatie te worden gebruikt met WS-addressing
	Overweging: WS-ReliableMessaging maakt gebruik van de WS-addressing elementen als input voor de WS-RM lifecycle berichten. Het gebruik van WS-addressing dient te voldoen aan de voorschriften zoals deze beschreven staan in '2.4.2. WS-addressing'.
WR006	Het gebruik van signatureConfirmation element bij End-To-End security profiel
	Indien End-to-End security nodig is voor reliable verkeer dient het bericht gesigned te worden. Tevens dient voor het retour gebruik gemaakt te worden van het signatureConfirmation element in het response bericht. Dit element valt onder WS-Security 1.1. In het response bericht dient een signatureConfirmation element toegevoegd te worden waar de signature waarde van de request is opgenomen.
WR007	Beveiligen WS-RM lifecycle berichten
	Lifecycle berichten zijn losse WS-RM berichten die de WS-RM sequence lifecycle beheert. Services die WS-RM ondersteunen en secure dienen te zijn, moeten ook de WS-RM lifecycle berichten voorzien van WS-Security headers. Het gebruik van WS-Security dient te conformeren aan de End-To-End beveiligingseisen zoals beschreven in paragraaf 2.4.4
WR008	Delivery Assurance 'exactlyOnce' dient altijd gebruikt te worden
	Om de risico van interoperabiliteitsissues te beperken is gekozen om 'exactlyOnce' te verplichten als Delivery Assurance waarde.

WR009	Reliable berichten zijn altijd asynchrone berichten (meldingen)
	Reliable berichten worden gebruikt voor het doen van meldingen waarbij geen directe terugkoppeling vereist is. Dit in tegenstelling tot het doen van bevestigingen. Meldingen dienen dus altijd asynchroon te zijn (non-blocking webservice call)
WR010	AcksTo publiek endpoint sterk afgeraden
	<p>WS-RM ondersteunt onder andere twee technieken om acknowledgements te ontvangen, namelijk:</p> <ul style="list-style-type: none"> - een actieve terugkoppeling van acknowledgement berichten via een publieke AcksTo adres - een passieve terugkoppeling van acknowledgement berichten door mee te liften op response berichten (piggybacking) door voor AcksTo "http://www.w3.org/2005/08/addressing/anonymous" op te nemen. <p>Het gebruik van een publieke AcksTo adres binnen Digikoppeling zorgt voor extra complexiteit en wordt daarom sterk afgeraden! Meer achtergrond is in de best practice opgenomen.</p>

Het gebruik van WS-RM kan feitelijk ook worden vastgelegd in het WSDL contract door gebruik te maken van het Policy framework. WS-ReliableMessaging Policies is hiervoor gedefinieerd. Het gebruik van policies heeft als voordeel dat het gebruik van WSRM technisch is vastgelegd waardoor frameworks hierop automatisch kunnen reageren. Hoewel WSRM policies reeds bepaald zijn in final specificaties, kunnen de implementaties van frameworks hier in de praktijk niet altijd mee omgaan. Om interoperabiliteit te waarborgen en consistentie binnen de profielen te houden, is voor Digikoppeling besloten om vanuit de standaard niet het gebruik van policies te verplichten maar optioneel te houden. In de best practices zal aandacht besteedt worden aan het gebruik van policies.

2.4.6

Naamgeving, namespaces

Er worden geen aanvullende eisen gesteld aan de namespaces. In de header mogen alleen velden voorkomen conform OASIS/W3C standaarden (gebaseerd op de daar gedefinieerde namespaces) , of service-specifieke namen, gedefinieerd door de provider met een namespace gedefinieerd door de provider. Ook aan de naamgeving van services, operations etc. worden vanuit Digikoppeling geen eisen gesteld. De prefix "Digikoppeling" is gereserveerd voor mogelijk toekomstig gebruik.

2.5

Foutafhandeling

Er worden momenteel nog geen eisen gesteld aan de foutafhandeling, anders dan in de onderliggende specificaties vermeld wordt, zoals WS-I Basic Profile 1.2. In het document " Digikoppeling Best Practises WUS" is een aantal adviezen opgenomen.

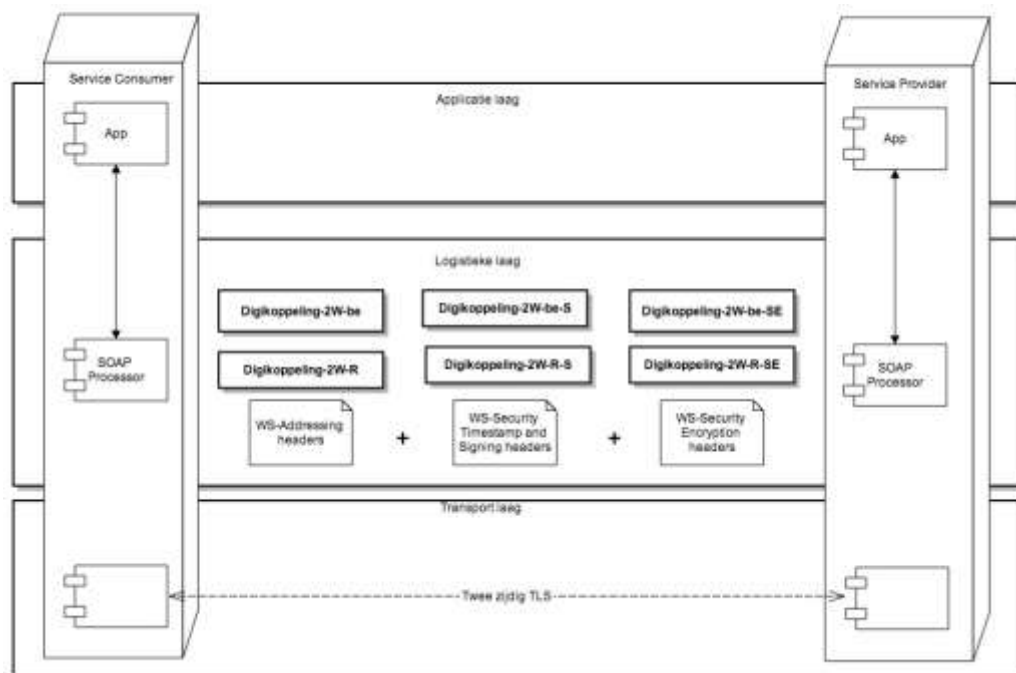
Aanvullende standaarden die gebruikt worden in combinatie met Digikoppeling kunnen overigens wel eisen stellen aan de fouthandeling.

3 Digikoppeling profielen WUS

Op Digikoppeling wordt gewerkt met zogenaamde “profielen”. Een profiel is een gedefinieerde bundeling van functionaliteit en daarmee van voorschriften. In de huidige Digikoppeling versie zijn zes WUS-profielen aanwezig, Digikoppeling 2W-be, Digikoppeling 2W-be-S en Digikoppeling 2W-be-SE, Digikoppeling 2W-R, Digikoppeling 2W-R-S, Digikoppeling 2W-R-SE genaamd.

Voor alle zes de profielen gelden dat deze zowel geoptimaliseerd (volgens de MTOM standaard) als niet geoptimaliseerd verstuurd kunnen worden. Hierom zijn voor elk profiel voorbeeldberichten opgenomen in zowel de geoptimaliseerde (MTOM) als niet geoptimaliseerde vorm. Alle voorbeeldberichten in de bijlagen zijn gebaseerd op de WSDL in bijlage 1.

Ten aanzien van beveiliging maken alle profielen gebruik van tweezijdig TLS, zie hoofdstuk 2 paragraaf “Point-to-Point beveiliging”.



In het bovenstaande figuur wordt schematisch weergegeven welke WUS profielen Digikoppeling biedt en wat de algemene verschillen zijn. Alle profielen worden in de volgende paragrafen in meer detail beschreven. In de bijlage zijn voorbeeld berichten opgenomen voor de profielen. Deze bieden een duidelijk inzicht hoe de berichten uiteindelijk eruit komen te zien.

Het Reliable concept is in die zin anders dan de andere profielen omdat er zowel losse lifecycle management berichten gestuurd worden als SOAP headers die met bestaande berichten meekomen (piggybacking concept). Lifecycle berichten zijn losse WS-RM specifieke berichten die gericht zijn om de WS-RM sequence te starten en af te sluiten.

In het volgende diagram worden de lifecycle berichten schematisch weergegeven:



In het bovenstaande sequentie diagram worden de lifecycle berichten versimpeld weergegeven. Om reliable messaging tot stand te brengen is het essentieel dat elk bericht uniek geïdentificeerd kan worden door middel van een sequentie die bekend is bij beide endpoints. Deze sequentie wordt afgestemd in de eerste createSequence call. Alle opvolgende berichten worden voorzien van een oplopende sequence. De sequence acknowledgements geven vervolgens aan welke berichten ontvangen zijn. Sequences die niet acknowledged zijn zullen opnieuw verstuurd worden. Tenslotte wordt een sequence beëindigd met een terminateSequence.

Bij het gebruik van het reliable profiel is het van belang om te weten dat buiten de WSDL gedefinieerde berichten ook losse WSRM lifecycle berichten gestuurd worden. Frameworks en toolkits die WSRM 1.1 ondersteunen, zullen vaak transparant voor de applicatie de berichten verkeer afhandelen.

3.1 WUS Profiel Digikoppeling 2W-be

Beveiliging

Dit profiel maakt voor de beveiliging alleen gebruik van tweezijdig TLS.

Headerblocks

Alleen de verplichte WS-Addressing headers zijn hier van toepassing (zie soapenv:Header in bijlage 2, figuur 5a en 5b).

MTOM

De geoptimaliseerde (MTOM) voorbeeldberichten worden weergegeven in bijlage 3, figuur 6a en 6b.

3.2 WUS Profiel Digikoppeling 2W-be-S

Beveiliging

Dit profiel maakt voor de beveiliging gebruik van tweezijdig TLS en tevens worden de berichtonderdelen ondertekend zoals vermeld in hoofdstuk 2, paragraaf End-to-End beveiliging.

Headerblocks

In dit profiel zijn de WS-Addressing en WS-Security 1.0 ondertekening (wsse:Security) headers van toepassing (zie bijlage 4, figuur 7a en 7b).

MTOM

De geoptimaliseerde (MTOM) voorbeeldberichten voor profiel Digikoppeling 2W-be-S worden weergegeven in bijlage 5, figuur 8a en 8b.

3.3 WUS Profiel Digikoppeling 2W-be-SE

Beveiliging

Dit profiel maakt voor de beveiliging gebruik van tweezijdig TLS en tevens worden de berichtonderdelen ondertekend en versleuteld zoals vermeld in hoofdstuk 2, paragraaf End-to-End beveiliging.

Headerblocks

In dit profiel zijn de WS-Addressing en WS-Security 1.0 ondertekening (wsse:Security) headers van toepassing. Ook wordt hierbij de payload van het bericht versleuteld (xenc:EncryptedData) (zie bijlage 6, figuur 9a en 9b).

MTOM

De geoptimaliseerde (MTOM) voorbeeldberichten voor profiel Digikoppeling 2W-be-SE worden weergegeven in bijlage 7, figuur 10a en 10b.

3.4 WUS Profiel Digikoppeling 2W-R

Beveiliging

Dit profiel maakt voor de beveiliging alleen gebruik van tweezijdig TLS met reliable messaging ondersteuning

Headerblocks

De verplichte WS-Addressing headers zijn hier van toepassing en de WS-ReliableMessaging headers.

3.5 WUS Profiel Digikoppeling 2W-R-S

Beveiliging

Dit profiel maakt voor de beveiliging gebruik van tweezijdig TLS en tevens worden de berichtonderdelen ondertekend en versleuteld zoals vermeld in hoofdstuk 2, paragraaf End-to-End beveiliging.

Headerblocks

In dit profiel zijn de WS-Addressing, WS-ReliableMessaging en WS-Security 1.0, WS-Security 1.1 ondertekening (wsse:Security) headers van toepassing (zie bijlage 8)

MTOM

De geoptimaliseerde (MTOM) voorbeeldberichten voor profiel
Digikoppeling 2W-R-S.

3.6 WUS Profiel Digikoppeling 2W-R-SE

Beveiliging

Dit profiel maakt voor de beveiliging gebruik van tweezijdig TLS en tevens worden de berichtonderdelen ondertekend en versleuteld zoals vermeld in hoofdstuk 2, paragraaf End-to-End beveiliging.

Headerblocks

In dit profiel zijn de WS-Addressing, WS-ReliableMessaging en WS-Security 1.0, WS-Security 1.1 ondertekening (wsse:Security) headers van toepassing. Ook wordt hierbij de payload van het bericht versleuteld (xenc:EncryptedData) (zie bijlage 8)

MTOM

De geoptimaliseerde (MTOM) voorbeeldberichten voor profiel
Digikoppeling 2W-R-SE

Bijlage 1 – Voorbeeld WSDL

Digikoppeling 2 - Digikoppeling compliancevoorziening.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://service.voorbeeld.osb.gbo.overheid.nl/200706/osb-voorbeeld.xsd"
targetNamespace="http://service.voorbeeld.osb.gbo.overheid.nl/200706/osb-voorbeeld.xsd"
elementFormDefault="qualified">
  <xsd:element name="ping">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="berichtIn" type="xsd:string" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="pingResponse">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="berichtUit" type="xsd:string" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="toUpperCase">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="data" type="xsd:string" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="toUpperCaseResponse">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="dataUit" type="xsd:string" minOccurs="0"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>

  <xsd:element name="fout">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="foutMelding" type="xsd:string" nillable="true"/>
        <xsd:element name="foutMeldingCode" type="xsd:string" nillable="true"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

Digikoppeling 2 - compliancevoorziening- Digikoppeling 2.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://service.compliance.osb.gbo.overheid.nl/xsd/012009/compliancevoorziening-v2"
targetNamespace=
"http://service.compliance.osb.gbo.overheid.nl/xsd/012009 /compliancevoorziening-v2"
elementFormDefault="qualified">

  <xsd:complexType name="AttachmentType">
    <xsd:sequence>
      <xsd:element name="fileName" nillable="false" type="xsd:string" minOccurs="1"/>
      <xsd:element name="binaryData" nillable="false" type="xsd:base64Binary"
minOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:element name="binData" type="tns:AttachmentType"/>
  <xsd:element name="binDataResponse" type="tns:AttachmentType"/>

</xsd:schema>
```

Digikoppeling 2 - compliancevoorziening-abstract-definition- Digikoppeling 2.wsdl

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-v2"
xmlns:cv2="http://service.compliance.osb.gbo.overheid.nl/xsd/012009/compliancevoorziening-v2"
xmlns:cv1=
"http://service.compliance.osb.gbo.overheid.nl/200706/osb-compliancevoorziening.xsd"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
targetNamespace=
"http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-v2">
  <wsdl:types>
    <xsd:schema elementFormDefault="qualified"
xmlns:xmime="http://www.w3.org/2005/05/xmlmime">
      <xsd:import namespace=
"http://service.compliance.osb.gbo.overheid.nl/xsd/012009/compliancevoorziening-v2"
schemaLocation="./compliancevoorziening-osb2.xsd"/>
      <xsd:import namespace="http://service.compliance.osb.gbo.overheid.nl/200706/osb-
compliancevoorziening.xsd" schemaLocation="./osb-compliancevoorziening.xsd"/>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="pingRequest">
    <wsdl:part name="parameters" element="cv1:ping"/>
  </wsdl:message>
  <wsdl:message name="pingResponse">
    <wsdl:part name="parameters" element="cv1:pingResponse"/>
  </wsdl:message>
  <wsdl:message name="toUpperCaseRequest">
    <wsdl:part name="parameters" element="cv1:toUpperCase"/>
  </wsdl:message>
  <wsdl:message name="toUpperCaseResponse">
    <wsdl:part name="parameters" element="cv1:toUpperCaseResponse"/>
  </wsdl:message>
  <wsdl:message name="binData">
    <wsdl:part name="parameters" element="cv2:binData"/>
  </wsdl:message>
```

```

</wsdl:message>
<wsdl:message name="binDataResponse">
  <wsdl:part name="parameters" element="cv2:binDataResponse"/>
</wsdl:message>

<wsdl:message name="TestFout">
  <wsdl:part name="parameters" element="cv1:fout"/>
</wsdl:message>
<wsdl:portType name="IOSB2ComplianceService">
  <wsdl:operation name="ping">
    <wsdl:input message="tns:pingRequest"
      wsam:Action="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzi
ening-v2/IOSB2ComplianceService/pingRequest"/>
    <wsdl:output message="tns:pingResponse"
      wsam:Action="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzi
ening-v2/IOSB2ComplianceService/pingResponse"/>
    <wsdl:fault name="TestFoutMelding" message="tns:TestFout"/>
  </wsdl:operation>
  <wsdl:operation name="toUpperCase">
    <wsdl:input message="tns:toUpperCaseRequest"
      wsam:Action="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzi
ening-v2/IOSB2ComplianceService/toUpperCaseRequest"/>
    <wsdl:output message="tns:toUpperCaseResponse"
      wsam:Action="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzi
ening-v2/IOSB2ComplianceService/toUpperCaseResponse"/>
    <wsdl:fault name="TestFoutMelding" message="tns:TestFout"/>
  </wsdl:operation>
  <wsdl:operation name="binData">
    <wsdl:input message="tns:binData"
      wsam:Action="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzi
ening-v2/IOSB2ComplianceService/binDataRequest"/>
    <wsdl:output message="tns:binDataResponse"
      wsam:Action="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzi
ening-v2/IOSB2ComplianceService/binDataResponse"/>
    <wsdl:fault name="TestFoutMelding" message="tns:TestFout"/>
  </wsdl:operation>

</wsdl:portType>
</wsdl:definitions>

```

Digikoppeling 2 - voorbeeld-servicebinding.wsdl

```

<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:wsa="http://ws-i.org/schemas/conformanceClaim/"
  xmlns:tns="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-v2"
  targetNamespace=
"http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-v2">
  <wsdl:import namespace=
"http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-v2"
    location="./compliancevoorziening-abstract-definition-osb2.wsdl"/>
  <wsdl:binding name="OSB2ComplianceServiceBinding" type="tns:IOSB2ComplianceService">

    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>

    <wsdl:operation name="ping">

```



```

    <soap:operation soapAction=
      "http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-
      v2/IOSB2ComplianceService/pingRequest"/>
    <wsdl:input>
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="TestFoutMelding">
      <soap:fault name="TestFoutMelding" use="literal"/>
    </wsdl:fault>
  </wsdl:operation>
  <wsdl:operation name="toUpperCase">
    <soap:operation
      soapAction="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzie-
      ning-v2/IOSB2ComplianceService/toUpperCaseRequest"/>
    <wsdl:input>
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="TestFoutMelding">
      <soap:fault name="TestFoutMelding" use="literal"/>
    </wsdl:fault>
  </wsdl:operation>
  <wsdl:operation name="binData">
    <soap:operation
      soapAction="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzie-
      ning-v2/IOSB2ComplianceService/binDataRequest"/>
    <wsdl:input>
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="TestFoutMelding">
      <soap:fault name="TestFoutMelding" use="literal"/>
    </wsdl:fault>
  </wsdl:operation>

</wsdl:binding>
<wsdl:service name="OSB2ComplianceService">
  <wsdl:port name="OSB" binding="tns:OSB2ComplianceServiceBinding">
    <soap:address location="https://www.wus.cv.prod.osb.overheid.nl/wsdl/ictu-ocvwus-
    ws/OSB2ComplianceService"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

Bijlage 2 - Voorbeeld SOAP berichten Digikoppeling 2W-be profiel

In figuur 2 wordt een voorbeeld van een bericht ("on the wire") weergegeven dat voldoet aan profiel Digikoppeling 2W-be en de beschreven WSDL (zie bijlage 1, binDataRequest). Het bericht is op te delen in verschillende lagen, een "SOAP Header", een "SOAP Envelope" en een "SOAP Body". De figuur toont tevens de HTTP-gegevens.

```
POST /osb-20/services/OSB2ComplianceService HTTP/1.1
Content-Type: text/xml; charset=UTF-8
SOAPAction:
"http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-
v2/IOSB2ComplianceService/binDataRequest"
User-Agent: Axis2
Host: 127.0.0.1:8888
Transfer-Encoding: chunked
<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsa:To>https://www.wus.cv.prod.osb.overheid.nl/wsdl/ictu-ocvwus-
ws/OSB2ComplianceService</wsa:To>

    <wsa:MessageID>urn:uuid:A9E4C7EA594A920DD91227194939525@osbclient.overheidsservi
cebus.nl</wsa:MessageID>

    <wsa:Action>http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzieni
ng-v2/IOSB2ComplianceService/binDataRequest</wsa:Action>
  </soapenv:Header>
  <soapenv:Body>
    <ns1:binData
xmlns:ns1=
"http://service.compliance.osb.gbo.overheid.nl/xsd/012009/compliancevoorziening-v2">
      <ns1:Attachment><ns1:fileName>Plaatje.gif</ns1:fileName>

      <ns1:binaryData>MIIEQDCCAyigAwIBAgIEAJiafTANBgqhkiG9w0BAQUFADBAMQswCQYDVQQ
GEWJOTDEWM

      BQGA1UEChMNT1NCIFRFRU1QgUk9PVDEZMBcGA1UEAxMQT1NCIFRFRU1QgUm9vdCBDQTAeFw0
wNzAzM

      ...
    </ns1:binaryData>
  </ns1:Attachment>
</ns1:binData>

  </soapenv:Body>
</soapenv:Envelope>
```

Figuur 5a: SOAP request volgens profiel Digikoppeling 2W-be

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 20 Nov 2008 15:29:04 GMT

<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">

    <wsa:Action>http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-v2/IOsb2ComplianceService/binDataResponse</wsa:Action>

    <wsa:RelatesTo>urn:uuid:A9E4C7EA594A920DD91227194939525@osbclient.overheidsservicebus.nl</wsa:RelatesTo>
    <wsa:To> http://www.w3.org/2005/08/addressing/anonymous </wsa:To>
    <wsa:MessageID>urn:uuid:E32CE28BB6C5C6053D11773522754354@services.orgx.nl
    </wsa:MessageID>
  </soapenv:Header>
  <soapenv:Body>
    <ns1:binDataResponse xmlns:ns1="http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-v2">
      <ns1:Attachment>
        <ns1:fileName>Plaatje.gif</ns1:fileName>

        <ns1:binaryData>MIIEQDCCAyigAwIBAgIEAJiafTANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEWJOTDEWMB
          QGA1UEChMNT1
        ...
      </ns1:binaryData>
    </ns1:Attachment>
  </ns1:binDataResponse>

</soapenv:Body></soapenv:Envelope>

```

Figuur 5b: SOAP response volgens profiel Digikoppeling 2W-be

Bijlage 3 - Voorbeeld SOAP berichten Digikoppeling 2W-be profiel met MTOM

In figuur 3 worden dezelfde gegevens getoond (binDataRequest) als in bijlage 2, maar dan in berichten op basis van de MTOM standaard.

```
Host: 127.0.0.1:8888
Transfer-Encoding: chunked

938
--MIMEBoundaryurn_uuid_01EE09F11C88F70DDE1227195215464
Content-Type: application/xop+xml; charset=UTF-8; type="text/xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:01EE09F11C88F70DDE1227195215465@apache.org>
  <?xml version='1.0' encoding='UTF-8'?>
    <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
      <soapenv:Header
xmlns:wsa="http://www.w3.org/2005/08/addressing"> <wsa:To>https://www.wus.cv.prod.os
b.overheid.nl/wsdl/ictu-ocvwus-ws/OSB2ComplianceService</wsa:To>

      <wsa:MessageID>
urn:uuid:01EE09F11C88F70DDE1227195215212@osbclient.overheidsservicebus.nl
      </wsa:MessageID>

      <wsa:Action>http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzieni
ng-v2/IOSB2ComplianceService/binDataRequest</wsa:Action>
      </soapenv:Header> <soapenv:Body> <ns1:binData
xmlns:ns1="http://service.compliance.osb.gbo.overheid.nl/xsd/012009/compliancevoorzienin
g-v2">
        <ns1:Attachment>
          <ns1:fileName> Plaatje.gif </ns1:fileName>
          <ns1:binaryData>
            <xop:Include
href="cid:1.urn:uuid:01EE09F11C88F70DDE1227195215575@apache.org"
xmlns:xop="http://www.w3.org/2004/08/xop/include" /> </ns1:binaryData>
          </ns1:Attachment>
        </ns1:binData>
      </soapenv:Body>
    </soapenv:Envelope>
  --MIMEBoundaryurn_uuid_01EE09F11C88F70DDE1227195215464
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:01EE09F11C88F70DDE1227195215575@apache.org>

  0âĈš#@0âĈš#(Â #####
  --MIMEBoundaryurn_uuid_01EE09F11C88F70DDE1227195215464--
0
```

Figuur 6a: SOAP request volgens profiel Digikoppeling 2W-be met MTOM

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related;
boundary=MIMEBoundaryurn_uuid_D30A43B194E39E511C1227195220199;
type="application/xop+xml";
start="<0.urn:uuid:D30A43B194E39E511C1227195220200@apache.org>"; start-
info="text/xml"
  Transfer-Encoding: chunked
  Date: Thu, 20 Nov 2008 15:33:40 GMT

427
--MIMEBoundaryurn_uuid_D30A43B194E39E511C1227195220199
Content-Type: application/xop+xml; charset=UTF-8; type="text/xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:D30A43B194E39E511C1227195220200@apache.org>

  <?xml version='1.0' encoding='UTF-8'?>
    <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
      <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
        <wsa:To> http://www.w3.org/2005/08/addressing/anonymous </wsa:To>
        <wsa:MessageID>urn:uuid:R32CE28BB6C5C6053D11773522754323@services.orgx.nl
        </wsa:MessageID>
        <wsa:Action>http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorzienin
        g-v2/IOSB2ComplianceService/binDataResponse</wsa:Action>

        <wsa:RelatesTo>urn:uuid:01EE09F11C88F70DDE1227195215212@osbclient.overheidsservice
        bus.nl</wsa:RelatesTo>
      </soapenv:Header>
      <soapenv:Body>
        <ns1:binDataResponse
        xmlns:ns1="http://service.compliance.osb.gbo.overheid.nl/xsd/012009/compliancevoorzienin
        g-v2"><ns1:Attachment>
          <ns1:fileName>Plaatje.gif </ns1:fileName>
          <ns1:binaryData>
            <xop:Include
            href="cid:1.urn:uuid:D30A43B194E39E511C1227195220201@apache.org"
            xmlns:xop="http://www.w3.org/2004/08/xop/include" />
          </ns1:binaryData>
        </ns1:Attachment>
        </ns1:binDataResponse>
      </soapenv:Body>
    </soapenv:Envelope>
  38
--MIMEBoundaryurn_uuid_D30A43B194E39E511C1227195220199
4d8
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:D30A43B194E39E511C1227195220201@apache.org>

  0â€š#@0â€š#(Â# ####
  ...

--MIMEBoundaryurn_uuid_D30A43B194E39E511C1227195220199
2
--
0

```

Figuur 6b: SOAP response volgens profiel Digikoppeling 2W-be met MTOM

Bijlage 4 - Voorbeeld SOAP berichten Digikoppeling 2W-be-S profiel

In figuur 4 wordt een voorbeeld van een bericht ("on the wire") weergegeven dat voldoet aan profiel Digikoppeling 2W-be-S en de beschreven WSDL (zie bijlage 1, ping). Het bericht is op te delen in verschillende lagen, een "SOAP Header", een "SOAP Envelope" en een "SOAP Body". De figuur toont tevens de HTTP-gegevens.

```
POST /osb-20/services/OSB2ComplianceService HTTP/1.1
Content-Type: text/xml; charset=UTF-8
SOAPAction: "http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest"
User-Agent: Axis2
Host: 127.0.0.1:8888
Transfer-Encoding: chunked
<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
      soapenv:mustUnderstand="1">
<wsu:Timestamp xmlns:wsu=
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  wsu:Id="Timestamp-17153368">
    <wsu:Created>2008-12-15T11:29:07Z</wsu:Created>
    <wsu:Expires>2008-12-16T15:15:47Z</wsu:Expires>
  </wsu:Timestamp>
  <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
    EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary"
    ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"
    wsu:Id="CertId-
15308409">MIIESDCCAzCgAwIBAgIGEgABICM5MA0GCSqGSIb3DQEBBQUAMDUXCzAJBgNVBAYTAk5M
MQwwCgYDVQQKEwNPU0I
  </wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-10175206">
<ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
  <ds:Reference URI="#Id-30533424">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>eyy5Pt/4Jn/nRSMx3dzsLSMLeUM=</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#id-13080585">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>PG9uYxXQvJrSJrhoaeyw5xWfUuc=</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#id-3916915">
    <ds:Transforms>
      ...
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
```

```

    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>KlaS154/IDR05pNsAb/UYNiWam0=</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#id-31365828">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>NdaLSa3zws3NI71yw/8sRN9VOOw=</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#Timestamp-17153368">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.
      687
      w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>pbkGYUKb42h/eM2iuZ3G+RQd9VM=</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
  jYS/BqIRmtr/zVVibrRW680NLrpq/GURf7vJpiOy42g2hapCDQfdpuGHVUOo8zdM+dQ+1XI/zU+X
  /BAKIE2Fn2cfs0pD4JYfYRINKgFoFO+noLGR9v3pZg5dfVlpKXbzZAoXxC6HsmP5yQwHJ9rMhBSq
  r85LpNaGMrrpd5/nFY4=
</ds:SignatureValue>
<ds:KeyInfo Id="KeyId-24389376">
  <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
    wsu:Id="STRId-28259286">
    <wsse:Reference URI="#CertId-15308409"
      ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
    </wsse:SecurityTokenReference>
  </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
<wsa:To xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
  wsu:Id="id-
13080585">http://www.ocv.wus.compliance.osb.overheid.nl/OSB2ComplianceService</wsa:To>
  <wsa:MessageID xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
    wsu:Id="id-
3916915">urn:uuid:02875597AE9A49ABAB1229340545618@osbclient.overheidsservicebus.nl</wsa:
MessageID>
  <wsa:Action xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
    wsu:Id="id-
31365828">http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/wsdl/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest</wsa:Action>
  </soapenv:Header>
  <soapenv:Body
    xmlns:wsu=
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
    wsu:Id="Id-30533424">
    <ns2:ping xmlns:ns2="http://service.compliance.osb.gbo.overheid.nl/200706/osb-
compliancevoorziening.xsd">
      <ns2:berichtIn>test</ns2:berichtIn></ns2:ping>
    </soapenv:Body>
  </soapenv:Envelope>

```

Figuur 7a: SOAP request volgens profiel Digikoppeling 2W-be-S

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

Content-Type: text/xml; charset=UTF-8

Transfer-Encoding: chunked

Date: Mon, 15 Dec 2008 11:29:11 GMT

```
<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security
xmlns:wsse=
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    soapenv:mustUnderstand="1">
      <wsu:Timestamp
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
        wsu:Id="Timestamp-318747">
          <wsu:Created>2008-12-15T11:29:11Z</wsu:Created>
          <wsu:Expires>2008-12-16T15:15:51Z</wsu:Expires>
        </wsu:Timestamp>
        <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
          EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary"
          ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"
          wsu:Id="CertId-
16994998">MIIeYzCCA0ugAwIBAgIGEgABICMyMA0GCSqGSIb3DQEBBQUAMDUxCzAJBgNVBAY
...
        </wsse:BinarySecurityToken>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-15858385">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#Id-22033496">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
              <ds:DigestValue>Vn1AXdaoPz7lGsOtSomjja/umNw=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#id-29873515">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
              <ds:DigestValue>z18cqye4y4DzzScr4UijYGT3RU=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#id-9209226">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
              <ds:DigestValue>Gs7mCvTYqRwokenpbh+IYy1ZD8A=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#Timestamp-318747">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
              <ds:DigestValue>/pfyRzjBJYkKKVslK7mWteSdDJg=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>
```



```

mm6q6K7T14iinMV1SmM2VsuBQQgUJlyDmWxzO+R/aZ0OG64ABhst6BhRS7X/tB5OKN1KoOYr1Kul
7tPcXy+J05u1NnYtM9PliJDrMBRqp+PscxGX4p3vCkMJspFbbFxrCs9R44cjrUkDCbYMZaAtqSnY
Om42j1xmdZVDFFagu4Y=
</ds:SignatureValue>
<ds:KeyInfo Id="KeyId-16501616">
  <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
    wsu:Id="STRId-15282649">
    <wsse:Reference URI="#CertId-16994998" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature></wsse:Security><wsa:Action xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  wsu:Id="id-
29873515">http://service.compliance.osb.gbo.overheid.nl/wSDL/012009/compliancevoorziening-
v2/IOSB2ComplianceService/pingResponse</wsa:Action>
  <wsa:RelatesTo xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
    wsu:Id="id-
9209226">urn:uuid:02875597AE9A49ABAB1229340545618@osbclient.overheidsservicebus.nl</wsa:
RelatesTo>
<wsa:To> http://www.w3.org/2005/08/addressing/anonymous </wsa:To>
<wsa:MessageID>urn:uuid:R32CE28BB6C5C6053D11773522754323@services.orgx.nl
</wsa:MessageID>

  </soapenv:Header><soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Id-22033496">
    <ns2:pingResponse xmlns:ns2="http://service.compliance.osb.gbo.overheid.nl/200706/osb-
compliancevoorziening.xsd">
      <ns2:berichtUit>test</ns2:berichtUit></ns2:pingResponse>
    </soapenv:Body>
</soapenv:Envelope>

```

Figuur 7b: SOAP response volgens profiel Digikoppeling 2W-be-S

Bijlage 5 - Voorbeeld SOAP berichten Digikoppeling 2W-be-S profiel met MTOM

In figuur 5 worden dezelfde gegevens getoond (ping) als in bijlage 4, maar dan in berichten op basis van de MTOM standaard.

```
POST /osb-20/services/OSB2ComplianceService HTTP/1.1
Content-Type: multipart/related;
boundary=MIMEBoundaryurn_uuid_A74BAEB4ECA18AC2D21229430743620;
type="application/xop+xml";
start="<0.urn:uuid:A74BAEB4ECA18AC2D21229430743621@apache.org>"; start-info="text/xml"
SOAPAction: "http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest"
User-Agent: Axis2
Host: 127.0.0.1:8888
Transfer-Encoding: chunked

--MIMEBoundaryurn_uuid_A74BAEB4ECA18AC2D21229430743620
Content-Type: application/xop+xml; charset=UTF-8; type="text/xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:A74BAEB4ECA18AC2D21229430743621@apache.org>

<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">
      <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-1977511">
        <wsu:Created>2008-12-16T12:32:23Z</wsu:Created>
        <wsu:Expires>2008-12-17T16:19:03Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"
        wsu:Id="CertId-
15308409">MIIESDCCAzCgAwIBAgIGEgABICM5MA0GCSqGSIb3DQEBBQUAMDUxCzAJBgNVBAYTAk5
...
      </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-
33040770">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#Id-17153368">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <ds:DigestValue>MwSgC7w41uQBKOKWTYzqp13WWRg=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#id-23886295">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
```

```

        <ds:DigestValue>j2CzxnMRBnrYjEpJM99eQBui31w=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#id-11746570">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>ykXMc3qdWnVCJNZY2B5gQk26sdI=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#id-23894119">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>tG+8Gi3kN1V/mLsLpFxVPPvmUxw=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#Timestamp-1977511">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>XOTMKiFPUQJR8X5P0kjPOWmR27Y=</ds:DigestValue>
    </ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>

yfUSZr7s2GY7eYZHYX7m6GTtaIvpBsrrghG4uIOcn1fPuY0QnNyDDa3G3c/51d2ybllDxpJDchtq

MHzcPP97Lfsz/YopW3d2LPnfWge74E0GyCfNzJxAD+9yvncvUpSnTq8ji3+IpMSRil//ZBqB6f8A
li/IRr0SIBBtiFx/pS0=
</ds:SignatureValue>
<ds:KeyInfo Id="KeyId-15142448">
    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
    wsu:Id="STRId-3969559">
        <wsse:Reference URI="#CertId-15308409" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
    </wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature></wsse:Security><wsa:To xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="id-23886295">myservice</wsa:To>
<wsa:MessageID xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
wsu:Id="id-
11746570">urn:uuid:A74BAEB4ECA18AC2D21229430742540@osbclient.overheidsservicebus.nl</wsa:
MessageID>
    <wsa:Action xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
wsu:Id="id-23894119">
http://service.compliance.osb.gbo.overheid.nl/wSDL/012009/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest</wsa:Action>
</soapenv:Header><soapenv:Body xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Id-17153368">
    <ns2:ping xmlns:ns2="http://service.compliance.osb.gbo.overheid.nl/200706/osb-
compliancevoorziening.xsd">
        <ns2:berichtIn>test</ns2:berichtIn></ns2:ping>
    </soapenv:Body>
</soapenv:Envelope>

```

--MIMEBoundaryurn_uuid_A74BAEB4ECA18AC2D21229430743620--

Figuur 8a: SOAP request volgens profiel Digikoppeling 2W-be-S met MTOM

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

Content-Type: multipart/related;

boundary=MIMEBoundaryurn_uuid_E85428962F63918A691229430745289;

type="application/xop+xml";

start="<0.urn:uuid:E85428962F63918A691229430745290@apache.org>"; start-info="text/xml"

Transfer-Encoding: chunked

Date: Tue, 16 Dec 2008 12:32:25 GMT

158d

--MIMEBoundaryurn_uuid_E85428962F63918A691229430745289

Content-Type: application/xop+xml; charset=UTF-8; type="text/xml"

Content-Transfer-Encoding: binary

Content-ID: <0.urn:uuid:E85428962F63918A691229430745290@apache.org>

```
<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
      soapenv:mustUnderstand="1">
        <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd"
          wsu:Id="Timestamp-22926122">
            <wsu:Created>2008-12-16T12:32:25Z</wsu:Created>
            <wsu:Expires>2008-12-17T16:19:05Z</wsu:Expires>
          </wsu:Timestamp>
          <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
            EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary"
            ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"
            wsu:Id="CertId-
16994998">MIIeYzCCA0ugAwIBAgIGeGABICMyMA0GCSqGSIb3DQEBAQUAMDUxCzAJBgNVBAYTAK
...
          </wsse:BinarySecurityToken><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-30227927">
            <ds:SignedInfo>
              <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
              <ds:Reference URI="#Id-13798906">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>6TdUhJy6dIDuUI22HImCk0zB5gY=</ds:DigestValue>
              </ds:Reference>
              <ds:Reference URI="#id-19736274">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>Cld/pido7c0QgSp4Q1iBFuMpDCY=</ds:DigestValue>
              </ds:Reference>
              <ds:Reference URI="#id-305514">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>EtrXxr6dgQ4hBRZrYQ/YwtUsuXY=</ds:DigestValue>
              </ds:Reference>
              <ds:Reference URI="#Timestamp-22926122">
```

```

    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>yxDD+Y7BOgc4NjcTQGba+pB4J68=</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>

U9b5eGA+Hzlf85lrDU5FLgmRyw/1G5pMysfn109a0a2X2CTe7ZQDuB0nb/Bnb9+4xo65h2bciEqH

C2sV+GsobFuqn81CDWF9As4/2SueE5FbCxdFEn54rKpVJHqL+4/ctToj7XqaG9WEaoojDKFML1RX
V87p0u1Uy19AJz+D2A8=
</ds:SignatureValue>
<ds:KeyInfo Id="KeyId-21690871">
  <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="STRId-23126121">
    <wsse:Reference URI="#CertId-16994998" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature></wsse:Security><wsa:Action xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="id-
19736274">http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening-
v2/IOSB2ComplianceService/pingResponse</wsa:Action>
  <wsa:RelatesTo xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="id-305514">

urn:uuid:A74BAEB4ECA18AC2D21229430742540@osbclient.overheidsservicebus.nl</wsa:RelatesTo>
<wsa:To> http://www.w3.org/2005/08/addressing/anonymous </wsa:To>
<wsa:MessageID>urn:uuid:R32CE28BB6C5C6053D11773522754323@services.orgx.nl
</wsa:MessageID>
  </soapenv:Header>
  <soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="Id-13798906">
    <ns2:pingResponse
xmlns:ns2="http://service.compliance.osb.gbo.overheid.nl/200706/osb-compliancevoorziening.xsd">
      <ns2:berichtUit>test</ns2:berichtUit></ns2:pingResponse>
    </soapenv:Body>
  </soapenv:Envelope>
38

--MIMEBoundaryurn_uuid_E85428962F63918A691229430745289
2
--
0

```

Figuur 8b: SOAP response volgens profiel Digikoppeling 2W-be-S met MTOM

Bijlage 6 - Voorbeeld SOAP berichten Digikoppeling 2W-be-SE profiel

In figuur 6 wordt een voorbeeld van een bericht ("on the wire") weergegeven dat voldoet aan profiel Digikoppeling 2W-be-SE en de beschreven WSDL (zie bijlage 1, ping). Het bericht is op te delen in verschillende lagen, een "SOAP Header", een "SOAP Envelope" en een "SOAP Body". De figuur toont tevens de HTTP-gegevens.

```
POST /osb-20/services/OSB2ComplianceService HTTP/1.1
Content-Type: text/xml; charset=UTF-8
SOAPAction: "http://www.wus.cv.osb.overheid.nl/wsdl/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest"
User-Agent: Axis2
Host: 127.0.0.1:8888
Transfer-Encoding: chunked                f9c
<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xenc="http://www.w3.org/2001/04/xmldsig#">
<soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">
    <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-27058272">
      <wsu:Created>2009-01-05T13:54:12Z</wsu:Created>
      <wsu:Expires>2009-01-06T17:40:52Z</wsu:Expires>
    </wsu:Timestamp>
    <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
    ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"
    wsu:Id="urn:uuid:0625A3A4A48379AC7712311636530001">MIIEYzCCA0ugAwIBAgIG
    ...
  </wsse:BinarySecurityToken>
  <xenc:EncryptedKey Id="EncKeyId-urn:uuid:0625A3A4A48379AC7712311636530312">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmldsig#rsa-1_5" />
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <wsse:SecurityTokenReference><wsse:Reference
URI="#urn:uuid:0625A3A4A48379AC7712311636530001" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
</wsse:SecurityTokenReference>
</ds:KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>Uuln0SurImVOI2VjtS6Z
    ...
  </xenc:CipherValue>
</xenc:CipherData>
<xenc:ReferenceList>
<xenc:DataReference URI="#EncDataId-5165021"/>
</xenc:ReferenceList></xenc:EncryptedKey>
<wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
    ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" wsu:Id="CertId-15308409">MIIESDCCAzCgA
    ...
  </wsse:BinarySecurityToken>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-26882784">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
```

```

sha1"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
    <ds:Reference URI="#Id-5165021">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    />
    <ds:DigestValue>Mx59BLTUq1Vq4/4df7VA6ja5HyI= </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#id-25840096">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    />
    <ds:DigestValue>JIQsk3ApXZCMBzsAjBCNRrzVvhU= </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#id-33040770">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    />
    <ds:DigestValue>rTiWFRbKIO58TfU+kbQCAv0Ls7E= </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#id-15142448">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    />
    <ds:DigestValue>OrsPPIIWaXFYIQRc2VyP08a0YYg= </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#Timestamp-27058272">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    />
    <ds:DigestValue>50vFrtodtu5u7nDM3/IXQUIQWBY= </ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
XmmyUCangWyU8YqWSOxL8FSqR82hu/k7CKWXHV3Z+jqgpgDIQ0xltELh9pLu/
...
    </ds:SignatureValue>
    <ds:KeyInfo Id="KeyId-23668144">
        <wsse:SecurityTokenReference
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="STRId-9523050"> <wsse:Reference
URI="#CertId-15308409" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-x509-token-profile-1.0#X509v3" />
        </wsse:SecurityTokenReference>
    </ds:KeyInfo>
</ds:Signature>
</wsse:Security>

```

```

<wsa:To xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-25840096">http://localhost:8888/osb-20/services/OSB2ComplianceService</wsa:To><wsa:MessageID xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-33040770">urn:uuid:D115F21849DE6F3C9E1231163651509@osbclient.overheidsservicebus.nl</wsa:MessageID><wsa:Action xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-15142448">http://www.wus.cv.osb.overheid.nl/wsdl/compliancevoorziening-v2/IOSB2ComplianceService/pingRequest</wsa:Action>
</soapenv:Header>
<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Id-5165021"><xenc:EncryptedData Id="EncDataId-5165021" Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
    <wsse:Reference URI="#EncKeyId-urn:uuid:0625A3A4A48379AC7712311636530312" />
  </wsse:SecurityTokenReference>
  </ds:KeyInfo><xenc:CipherData><xenc:CipherValue>
...
</xenc:CipherValue>
</xenc:CipherData></xenc:EncryptedData>
</soapenv:Body>
</soapenv:Envelope>

```

Figuur 9a: SOAP request volgens profiel Digikoppeling 2W-be-SE

HTTP/1.1 200 OK
 Server: Apache-Coyote/1.1
 Content-Type: text/xml; charset=UTF-8
 Transfer-Encoding: chunked
 Date: Tue, 16 Dec 2008 08:26:51 GMT

```
<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
      wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">
      <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
        wss-wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-22665343">
        <wsu:Created>2008-12-16T08:26:51Z</wsu:Created>
        <wsu:Expires>2008-12-17T12:13:31Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
        200401-wss-wssecurity-utility-1.0.xsd"
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
        message-security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
        profile-1.0#X509v3"

wsu:Id="urn:uuid:DB86307BA43623702512294160114061">MIIESDCCAzCgAwIBAgIGeGABIC
M5MA0GCSqGSIB3DQE
...
      </wsse:BinarySecurityToken>
      <xenc:EncryptedKey Id="EncKeyId-urn:uuid:DB86307BA43623702512294160114062">
      <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <wsse:SecurityTokenReference><wsse:Reference
URI="#urn:uuid:DB86307BA43623702512294160114061"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
        profile-1.0#X509v3" />
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>

<xenc:CipherData><xenc:CipherValue>D69CUOQ5tcFeTK08MkDlcaZo2dH1o7ua7f/FTpHh9rxE
Dv6LMI54xkiB0ID+1D9ndD3aM/
...
      </xenc:CipherValue></xenc:CipherData><xenc:ReferenceList><xenc:DataReference
URI="#EncDataId-26517368" />
      </xenc:ReferenceList>
    </xenc:EncryptedKey>
    <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
      200401-wss-wssecurity-utility-1.0.xsd"
      EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
      message-security-1.0#Base64Binary"
      ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
      profile-1.0#X509v3"
      wsu:Id="CertId-
      16994998">MIIEYzCCA0ugAwIBAgIGeGABICMyMA0GCSqGSIB3DQEBBQUAMDUxCzAJBg
...
    </wsse:BinarySecurityToken><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-13859719">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
        c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
        />
        <ds:Reference URI="#Id-26517368">
          <ds:Transforms>
```

```

        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>Wbe8V88WlQPa8ORo8jrLVDYx+wg=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#id-5480205">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>OaJGWc0zp0Ay3bDpVI0Y0QekMuk=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#id-32459563">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>535+CNcgq7nnK619jL6j0MmA1W4=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#Timestamp-22665343">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>xARBpZGWlKcJlk3YiRUqZFD0i00=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>

jBf8FptfqyaMi3AvNi9PX+rh45b2gNuiQKgM7CTAiB4aAgICjHzazueGHnbWjiXf0FjScX9++mzw

WQNEmyhEo7/8mohKc7F3pzNX8LJNM8I4p/upeHdLHBSvRmB0tK5JGr0N6vt+utg8zg7lnCT9T4u
C
    Pbv+fueO5RWXgNHOH2M=
  </ds:SignatureValue>
  <ds:KeyInfo Id="KeyId-12972559">
    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
      wsu:Id="STRId-26664489">
      <wsse:Reference URI="#CertId-16994998" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
    </wsse:SecurityTokenReference>
  </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
  <wsa:Action xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
    wsu:Id="id-
5480205">http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening
-v2/IOSB2ComplianceService/pingResponse</wsa:Action>
  <wsa:RelatesTo xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
    wsu:Id="id-
32459563">urn:uuid:73CAFA2DD4F970A3CE1229416003618@osbclient.overheidsservicebus.
nl</wsa:RelatesTo>
  <wsa:To> http://www.w3.org/2005/08/addressing/anonymous </wsa:To>
  <wsa:MessageID>urn:uuid:R32CE28BB6C5C6053D11773522754323@services.orgx.nl
  </wsa:MessageID>
</soapenv:Header>
  <soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="Id-26517368">
    <xenc:EncryptedData Id="EncDataId-26517368"
      Type="http://www.w3.org/2001/04/xmllenc#Content">

```

```

        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-
cbc" />
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
            <wsse:Reference URI="#EncKeyId-
urn:uuid:DB86307BA43623702512294160114062" /></wsse:SecurityTokenReference>
          </ds:KeyInfo> <xenc:CipherData> <xenc:CipherValue>ZOSkShiOTMjliOu6Q6nJ
          ...
          </xenc:CipherValue>
          </xenc:CipherData>
        </xenc:EncryptedData>
      </soapenv:Body>
    </soapenv:Envelope>

```

Figuur 9b: SOAP response volgens profiel Digikoppeling 2W-be-SE

Bijlage 7 - Voorbeeld SOAP berichten Digikoppeling 2W-be-SE profiel met MTOM

In figuur 7 worden dezelfde gegevens getoond (ping, deze bevat geen attachment) als in bijlage 6, maar dan in berichten op basis van de MTOM standaard.

```
POST /osb-20/services/OSB2ComplianceService HTTP/1.1
Content-Type: multipart/related;
boundary=MIMEBoundaryurn_uuid_5F19D72879326F6D391231164403089;
type="application/xop+xml";
start="<0.urn:uuid:5F19D72879326F6D391231164403090@apache.org>"; start-
info="text/xml"
    SOAPAction: "http://www.wus.cv.osb.overheid.nl/wsdl/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest"
    User-Agent: Axis2
    Host: 127.0.0.1:8888
    Transfer-Encoding: chunked

20e5
--MIMEBoundaryurn_uuid_5F19D72879326F6D391231164403089

Content-Type: application/xop+xml; charset=UTF-8; type="text/xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5F19D72879326F6D391231164403090@apache.org>

<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><soapenv:Header
xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">
        <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-5165021">
            <wsu:Created>2009-01-05T14:06:42Z</wsu:Created>
            <wsu:Expires>2009-01-06T17:53:22Z</wsu:Expires>
        </wsu:Timestamp>
        <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" wsu:Id="urn:uuid:DB81B78708A15F815B12311644029061">MIIEYzCC
        ...
    </wsse:BinarySecurityToken>
    <xenc:EncryptedKey Id="EncKeyId-urn:uuid:DB81B78708A15F815B12311644029372">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <wsse:SecurityTokenReference>
        <wsse:Reference URI="#urn:uuid:DB81B78708A15F815B12311644029061"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token- profile-
1.0#X509v3" />
    </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData><xenc:CipherValue>YM0YD2vrqP6Wqa
    ...
    </xenc:CipherValue>
    </xenc:CipherData>
    <xenc:ReferenceList><xenc:DataReference URI="#EncDataId-3201069"
/></xenc:ReferenceList>
</xenc:EncryptedKey>
```

```

<wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" wsu:Id="CertId-15308409">MIIESDCCAz
...
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-26882784">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
  />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
    <ds:Reference URI="#Id-3201069">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
        </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>v0hP6ueISgD4ZFHXXlcMvqADpMI=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#id-25840096">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <ds:DigestValue>JlQsk3ApXZCMBzsAjBCNRrzVvhU=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#id-33040770">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
            </ds:Transforms>
            <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <ds:DigestValue>e+Z6/cgQ5IL8rCx5FRyhEDsZNak=</ds:DigestValue>
          </ds:Reference>
          <ds:Reference URI="#id-15142448">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
              </ds:Transforms>
              <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
              <ds:DigestValue>OrsPPIIWaXFYIQRc2VyP08a0YYg=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#Timestamp-5165021">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                </ds:Transforms>
                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>kcGzI+vvtUdOovdthiHHfw+W5To=</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>
M9UCgUciQWM84Z8RkVPu+T
...
</ds:SignatureValue>

```

```

        <ds:KeyInfo Id="KeyId-23668144">
            <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="STRId-
9523050">
                <wsse:Reference URI="#CertId-15308409"
Value="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" />
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
</wsse:Security>
<wsa:To xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="id-25840096">http://localhost:8888/osb-
20/services/OSB2ComplianceService</wsa:To>
<wsa:MessageID xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
wsu:Id="id-33040770">
urn:uuid:5F19D72879326F6D391231164401400@osbclient.overheidsservicebus.nl
</wsa:MessageID>
<wsa:Action xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="id-
15142448">http://www.wus.cv.osb.overheid.nl/wsd/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest</wsa:Action>
</soapenv:Header>
<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="Id-3201069"><xenc:EncryptedData Id="EncDataId-
3201069" Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
<wsse:Reference URI="#EncKeyId-urn:uuid:DB81B78708A15F815B12311644029372" />
</wsse:SecurityTokenReference>
        </ds:KeyInfo><xenc:CipherData><xenc:CipherValue>qWzSjj6arR4mV4fr
...
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</soapenv:Body>
</soapenv:Envelope>
--MIMEBoundaryurn_uuid_5F19D72879326F6D391231164403089--
0

```

Figuur 10a: SOAP request volgens profiel Digikoppeling 2W-be-SE met MTOM

HTTP/1.1 200 OK
 Server: Apache-Coyote/1.1
 Content-Type: multipart/related;
 boundary=MIMEBoundaryurn_uuid_D237042BF33A4E62EF1229429324229;
 type="application/xop+xml";
 start="<0.urn:uuid:D237042BF33A4E62EF1229429324230@apache.org>"; start-
 info="text/xml"
 Transfer-Encoding: chunked
 Date: Tue, 16 Dec 2008 12:08:44 GMT

2000
 --MIMEBoundaryurn_uuid_D237042BF33A4E62EF1229429324229
 Content-Type: application/xop+xml; charset=UTF-8; type="text/xml"
 Content-Transfer-Encoding: binary
 Content-ID: <0.urn:uuid:D237042BF33A4E62EF1229429324230@apache.org>

```
<?xml version='1.0' encoding='UTF-8'?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">
      <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-4629854">
        \<wsu:Created>2008-12-16T12:08:44Z</wsu:Created>
        <wsu:Expires>2008-12-17T15:55:24Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-
token-profile-1.0#X509v3"

wsu:Id="urn:uuid:DB86307BA43623702512294293242033">MIIESDCCAzCgAwIBAgIGEgABIC
M5MA0GCS
      ...
    </wsse:BinarySecurityToken>
    <xenc:EncryptedKey Id="EncKeyId-
urn:uuid:DB86307BA43623702512294293242034">
      <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
1_5" />
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <wsse:SecurityTokenReference>
          <wsse:Reference URI="#urn:uuid:DB86307BA43623702512294293242033"
            ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" />
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>

      <xenc:CipherData><xenc:CipherValue>WYEUZEeAuTD/mqcPfBeP6iftUHI/7T4Fwd9XQo7VWPH
UYwWknjVGZAAf0/uQiRVSYz75lyGyZwZ5mvcqcm7nWk+
      ...
    </xenc:CipherValue>
  </xenc:CipherData>
  <xenc:ReferenceList>
    <xenc:DataReference URI="#EncDataId-1244162" />
  </xenc:ReferenceList>
  </xenc:EncryptedKey>
  <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
    EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary"
```

```

        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-
token-profile-1.0#X509v3"
        wsu:Id="CertId-
16994998">MIEYzCCA0ugAwIBAgIGEgABICMyMA0GCSqGSIb3DQEBBQUAMDUxCzAJBgNVBAY
TA
        ...
        </wsse:BinarySecurityToken>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-
1108000">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
                    <ds:Reference URI="#Id-1244162">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                                </ds:Transforms>
                                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                                    <ds:DigestValue>8hLTTUD78/yVBCu4pR2V8WRrW5U=</ds:DigestValue>
                                </ds:Reference>
                                <ds:Reference URI="#id-9249408">
                                    <ds:Transforms>
                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                                            </ds:Transforms>
                                            <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                                                <ds:DigestValue>v4FybpKIXWFOfhRyVNHjoUIoW40=</ds:DigestValue>
                                            </ds:Reference>
                                            <ds:Reference URI="#id-30684172">
                                                <ds:Transforms>
                                                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                                                        </ds:Transforms>
                                                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                                                            <ds:DigestValue>BuMJ3iHapgFXGTjGPdxao6zB8gk=</ds:DigestValue>
                                                        </ds:Reference>
                                                        <ds:Reference URI="#Timestamp-4629854">
                                                            <ds:Transforms>
                                                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                                                                    </ds:Transforms>
                                                                    <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                                                                        <ds:DigestValue>8jNpQyRf2ZzgGEV+Te7dP+p5HKc=</ds:DigestValue>
                                                                    </ds:Reference>
                                                                </ds:SignedInfo>
                                                                <ds:SignatureValue>
C8s8A9Yi7nvzZOG+t18FX1fCcyYCSesfMnKq9duEuq9KSGyaDONuLJWJghpNB9WATTGsk5RAFn/
x
K+ifjppnnrrNa7wTh7uoGMwobD/2kq4kPxV3xLV/apLsBWmW8HBG+so2nJ13iyxPuRNC775N89V
r
                2zWEMYJK47DEfzziMY0=
            </ds:SignatureValue>
            <ds:KeyInfo Id="KeyId-33008558">
                <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"

```



```

wsu:Id="STRId-19426064"><wsse:Reference URI="#CertId-16994998"
ValueTypes="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" />
</wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature></wsse:Security><wsa:Action xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="id-
9249408">http://service.compliance.osb.gbo.overheid.nl/wsdl/012009/compliancevoorziening
-v2/IOSB2ComplianceService/pingResponse</wsa:Action>
<wsa:RelatesTo xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="id-
30684172">urn:uuid:4FFB73E4329420D4E11229429322134@osbclient.overheidsservicebus.n
l</wsa:RelatesTo>
<wsa:To> http://www.w3.org/2005/08/addressing/anonymous </wsa:To>
<wsa:MessageID>urn:uuid:R32CE28BB6C5C6053D11773522754323@services.orgx.nl
</wsa:MessageID>
</soapenv:Header>
<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd" wsu:Id="Id-1244162">
<xenc:EncryptedData Id="EncDataId-1244162"
Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xml
3df
enc#aes128-cbc" /><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
<wsse:Reference URI="#EncKeyId-
urn:uuid:DB86307BA43623702512294293242034" /></wsse:SecurityTokenReference>
</ds:KeyInfo><xenc:CipherData><xenc:CipherValue>gh2bynOGnqc3lbOfdAR8bwZFs6cQ...
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</soapenv:Body>
</soapenv:Envelope>
38

--MIMEBoundaryurn_uuid_D237042BF33A4E62EF1229429324229
2
--
0

```

Figuur 10b: SOAP response volgens profiel Digikoppeling 2W-be-SE met MTOM

Bijlage 8 – Voorbeeld SOAP berichten voor reliable berichten

WS-RM maakt gebruik van zowel losse WS-RM lifecycle berichten als specifieke databerichten inclusief WS-RM SOAP headers. In de volgende voorbeeld berichten worden de volgende berichten getoond:

- reliable bericht zonder signing en encryption voor een createSequence
- reliable response bericht met acknowledgement header informatie zonder signing en encryption
- reliable databericht inclusief signing en encryption

Het volgende bericht toont een createSequence bericht net response zonder signing en encryption.

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>

```

```

        <Action xmlns="http://www.w3.org/2005/08/addressing">http://docs.oasis-
open.org/ws-rx/wsrn/200702/CreateSequence
        </Action>
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:4ed110f2-
caff-4422-b2f6-7232c6d6294c
        </MessageID>
        <To xmlns="http://www.w3.org/2005/08/addressing">http://localhost:9090/wsrn-
compliancey/services/ComplianceServicePort
        </To>
        <ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
            <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
        </ReplyTo>
    </soap:Header>
    <soap:Body>
        <CreateSequence xmlns="http://docs.oasis-open.org/ws-rx/wsrn/200702"
xmlns:ns2="http://www.w3.org/2005/08/addressing">
            <AcksTo>
                <ns2:Address>http://www.w3.org/2005/08/addressing/anonymous
                </ns2:Address>
            </AcksTo>
            <Expires>PT0S</Expires>
            <Offer>
                <Endpoint><Address
xmlns="http://www.w3.org/2005/08/addressing">http://localhost:9090/wsrn-
compliancey/services/ComplianceServicePort</Address></Endpoint>
                <Identifier>urn:uuid:f2a32487-d594-4371-b4a4-8a96f472581e
                </Identifier>
                <Expires>PT0S</Expires>
            </Offer>
        </CreateSequence>
    </soap:Body>
</soap:Envelope>

```

Response

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <Action xmlns="http://www.w3.org/2005/08/addressing">http://docs.oasis-
open.org/ws-rx/wsrn/200702/CreateSequenceResponse
        </Action>
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:26365b91-
aac5-4c71-9c1d-01276331da14
        </MessageID>
        <To
xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/anonymou
s</To>
        <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:4ed110f2-
caff-4422-b2f6-7232c6d6294c
        </RelatesTo>
    </soap:Header>
    <soap:Body>
        <CreateSequenceResponse xmlns="http://docs.oasis-open.org/ws-rx/wsrn/200702"
xmlns:ns2="http://www.w3.org/2005/08/addressing">
            <Identifier>urn:uuid:4a98dfe1-b3cf-4672-ae8f-b3eeffe98dd2
            </Identifier>
            <Expires>P0Y0M0DT0H0M0.0S</Expires>
            <Accept>

```

```

        <AcksTo>
          <ns2:Address>http://localhost:9090/wsrn-
compliancey/services/ComplianceServicePort
        </ns2:Address>
        </AcksTo>
      </Accept>
    </CreateSequenceResponse>
  </soap:Body>
</soap:Envelope>

```

Voorbeeld van een response bericht op een data bericht dat gesigned is.

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
      soap:mustUnderstand="1">
        <wsse:BinarySecurityToken
          EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary"
          ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509v3"
          wsu:Id="X509-
DFA75C6787DBD9A1EE13674161388124">MIIBqzCCARSgAwIBAgIEUS3+cDANBgkqhkiG9w0BAQUFA
DAaMRgwFgYDVQQDEw93c3JtLWNvbXBsaWZ3kwhhcnMTMwMjI3MTIzOTExWhcNMTUwMjI3MTIzOTEx
yWJAAaMRgwFgYDVQQDEw93c3JtLWNvbXBsaWZ3kwhhcnMTMwMjI3MTIzOTExWhcNMTUwMjI3MTIzOTEx
M810vLOZ/uHWMdgnJFjH3cAIAPhFdonjAph09tVjXjTOKBMfwIzvyE7nGBAJd6gcc5ELJHnuEu4Ol1hctJAuZ
RT+3E9JBLXXepZqjg59Ioc/taUtLhXG8nxSSou5LzIN3INvIE8M/FfWiQgN6dYnf+Scl76HeQXbgh9N5Uq6RZ
LAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAldIKNXnLNyU0qOWicq5JPg3+mV2OWBvRnYv3Ow7HrX5cxp
Q4n+sVqiVmnimirBjBsUPWtG1q9vcrMUcP4eM1M1r841HxwVrxZ9ENvpOBaCFQ1uxEGaav5GWTArBTUh
mK+RzPrhMug8DDK6BED0jtEBEjIVodgiJD5VkWmhsidsk=
        </wsse:BinarySecurityToken>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
          Id="SIG-8">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod
              Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
              <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                PrefixList="soap" />
            </ds:CanonicalizationMethod>
            <ds:SignatureMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#TS-6">
              <ds:Transforms>
                <ds:Transform
                  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsse soap" />
                  </ds:Transform>
                </ds:Transforms>
              </ds:Reference>
            </ds:SignatureMethod>
          </ds:SignedInfo>
        </ds:Signature>
      </wsse:Security>
    </soap:Header>
  </soap:Envelope>

```

```

        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

        <ds:DigestValue>SoZySMub9D8iAjPWvqVZ0HZQmqY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#id-7">
        <ds:Transforms>
        <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces

xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="" />
        </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

        <ds:DigestValue>kyYgfkPQx3dzI+kmZG3rAt3LDrE=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#SC-5">
        <ds:Transforms>
        <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces

xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsse soap" />
        </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

        <ds:DigestValue>JfNj8eZaty1vqkouEhWZ2FtQyCs=</ds:DigestValue>
        </ds:Reference>
        </ds:SignedInfo>

        <ds:SignatureValue>E6PE+u40NMurhIVyzqSUxNjS87g+7UtazINa6igQncMt/g+YRM4TU6Vf6f/O
c/VfX2cLy4E62HGiqfYjcyQdKIScHxOA23s4xk6SmwggQa//Y4pKWYHJeZJgLBGkWkmOMxVeUbNuj5LY65
Etg3gjBxAyVWZ0+fEKKfjt6nObg2E=
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-DFA75C6787DBD9A1EE13674161388125">
        <wsse:SecurityTokenReference wsu:Id="STR-
DFA75C6787DBD9A1EE13674161388126">
        <wsse:Reference URI="#X509-
DFA75C6787DBD9A1EE13674161388124"
        ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
        </wsse:SecurityTokenReference>
        </ds:KeyInfo>
        </ds:Signature>
        <wsu:Timestamp wsu:Id="TS-6">
        <wsu:Created>2013-05-01T13:48:58.812Z</wsu:Created>
        <wsu:Expires>2013-05-01T13:53:58.812Z</wsu:Expires>
        </wsu:Timestamp>
        <wsse11:SignatureConfirmation
xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
secect-1.1.xsd"

```

```

Value="NCWZtISJ13m7lLnVLS86gnLB2NkK+C1un7KpZPdEm3pN9ObOLkRGHFYM4anPjCFCZjD
qCta1EihsgZjDKVubw5eZv6MC5Dik8i3xgMIZRaE4qqwiTxoifwoe0FCMKC5VjGFK1AIyYcZ/XzbtMUxktzcg
9VUfcA/tigco7b1PzGA="
wsu:Id="SC-5" />
</wsse:Security>
<Action xmlns="http://www.w3.org/2005/08/addressing">http://docs.oasis-
open.org/ws-rx/wsrn/200702/SequenceAcknowledgement
</Action>
<MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:4749b94a-
76c1-478d-88af-b09f8be14818
</MessageID>
<To
xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/anonymou
s</To>
<ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
<Address>http://www.w3.org/2005/08/addressing/none</Address>
</ReplyTo>
<RelatesTo
xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/unspecific
d
</RelatesTo>
<ns2:SequenceAcknowledgement
xmlns:ns2="http://docs.oasis-open.org/ws-rx/wsrn/200702"
xmlns:ns3="http://www.w3.org/2005/08/addressing">
<ns2:Identifier>urn:uuid:d3ead09b-6ab4-4b2e-9a04-900e035bc600
</ns2:Identifier>
<ns2:AcknowledgementRange Lower="1" Upper="1" />
</ns2:SequenceAcknowledgement>
</soap:Header>
<soap:Body
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
wsu:Id="id-7" />
</soap:Envelope>

```

Bij deze nog een voorbeeld data bericht dat verstuurd wordt inclusief signing en encryption:

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
      soap:mustUnderstand="1">
        <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
          Id="EK-FB8988E877FC99911913674851726744">
          <xenc:EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p" />
          <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <wsse:SecurityTokenReference>
              <ds:X509Data>
                <ds:X509IssuerSerial>

```

```

<ds:X509IssuerName>CN=wsm-
compliance</ds:X509IssuerName>

<ds:X509SerialNumber>1361968752</ds:X509SerialNumber>
</ds:X509IssuerSerial>
</ds:X509Data>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
<xenc:CipherData>

  <xenc:CipherValue>u0cmcmb7qSziWuPg2QHTB+dj3XGBJkRXnt4UbvMt+GvysF9TheszHSfqMu
KIUDUiwA+U/p1wCom4rGR1iSMAeTah9X6gVTciwDuhkPLCi8edO7ETdp9u6zf6W3TezRWIhksU2579jnV7
uPNZIKGDRmosPMwl4ZIRK33F/U4c5Dg=
  </xenc:CipherValue>
</xenc:CipherData>
<xenc:ReferenceList>
  <xenc:DataReference URI="#ED-4" />
</xenc:ReferenceList>
</xenc:EncryptedKey>
<wsse:BinarySecurityToken
  EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary"
  ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509v3"
  wsu:Id="X509-
FB8988E877FC99911913674851724601">MIICVTCCAb6gAwIBAgIEUSsgNjANBgkqhkiG9w0BAQUFADB
vMQswCQYDVQQGEwJOTDEVMBMGA1UECBMMWnVpZCBib2xsYW5kMREwDwYDVQQHEwhEZW4gSGFh
ZzENMA8GA1UEChMEbUdCQTEOMAwGA1UECxFMRGVsdGEwFzAVBgNVBAMTDIBlcGlqbiBkZSBKb25nMB
4XDTEzMDIyNTA4MjYzMFoXDTEzMDUyNjA4MjYzMFoYbWZELMAkGA1UEBhMCTkwxFtATBgNVBAgTDGFp1a
WQgSG9sbGFuZDERMA8GA1UEBxMIRGVuIEhhYWcxDTALBgNVBAoTBG1HQkExDjAMBgNVBAwTBURlbH
RhMRcwFQYDVQQDEw5QZXBpam4gZGUgSm9uZzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAhHt
FdmHhidE/dobMGVrISyRXXcez7gskkNj/HAacmwKWuRXvq/yNtc3z/9kBD7SwU7NPX/302KWgKTLu3iwe
+9xwCkMMz6MjNH7dSgH37/IWzS5ESxkmkks2hJ5dL1E581Ti2uOQ6F2ZJ6DXbE2vgASxwyT46IEItXvQzf
92qDsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQACyCt9LhWtLR1pRsMliUq0gh4nbiWrjR3o7PII+clNrZ5A
dVtirGBNsbD8mqYIonDu/iGOEuiciePf1hQUXVvKjRjIRgHBGWiaNL6kbP0Sz/OT8wg56Ay4oPFvLhjrQMC1ea
LxK+xAjqc5Sy7STCjNLomSntegt3bgeRp/y9apNw==
  </wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  Id="SIG-3">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
      Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
      <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
      PrefixList="soap" />
    </ds:CanonicalizationMethod>
    <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <ds:Reference URI="#id-2">
      <ds:Transforms>
        <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="" />
        </ds:Transform>
      </ds:Transforms>
    </ds:Reference>
  </ds:SignedInfo>
</ds:Signature>

```

```

        </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

        <ds:DigestValue>/UIasHwFy/BavxVYvb6hYOvTwD8=</ds:DigestValue>
        </ds:Reference>
        </ds:SignedInfo>

        <ds:SignatureValue>CqQID3kxqtHMET/4RSYIU9xvEQVWJHI3pZ0I0BWI2iv4dR2En+BF3dBWFEI
P9pMTK/nD0kRagAXFq+mz/jjo8QG1q1eF1qOKPyZZ8oIdTq4Qn2LFiE58Z8MwqIsaoq2Bm89BrGkSXwnM
2xzPZA3d+JC0l1Jh2nKkT96OJAMv42A=
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-FB8988E877FC99911913674851724642">
        <wsse:SecurityTokenReference wsu:Id="STR-
FB8988E877FC99911913674851724663">
        <wsse:Reference URI="#X509-
FB8988E877FC99911913674851724601"
        ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
        </wsse:SecurityTokenReference>
        </ds:KeyInfo>
        </ds:Signature>
        <wsu:Timestamp wsu:Id="TS-1">
        <wsu:Created>2013-05-02T08:59:32.446Z</wsu:Created>
        <wsu:Expires>2013-05-02T09:59:32.446Z</wsu:Expires>
        </wsu:Timestamp>
        </wsse:Security>
        <Action xmlns="http://www.w3.org/2005/08/addressing">http://docs.oasis-
open.org/ws-rx/wsrn/200702/CreateSequence
        </Action>
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:880a35bb-
9874-41c4-8427-6b5ddd74338d
        </MessageID>
        <To xmlns="http://www.w3.org/2005/08/addressing">http://localhost:9090/wsrn-
compliance/services/ComplianceServicePort
        </To>
        <ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
        <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
        </ReplyTo>
        </soap:Header>
        <soap:Body
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
wsu:Id="id-2">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="ED-4" Type="http://www.w3.org/2001/04/xmlenc#Content">
        <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#tripleDES-cbc" />
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <wsse:SecurityTokenReference
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd"
wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-
wss-soap-message-security-1.1#EncryptedKey">

```

```

        <wsse:Reference URI="#EK-
FB8988E877FC99911913674851726744" />
        </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData>

        <xenc:CipherValue>YUaIIJYKUG1nA7KN901LG6I+joUOJOI4ToUOrAFhX0vW8Z1zoY8lQuzm/gt/3
Bib12YMRL1zP1M6iqVtWTXpIdX9pbbqHyxiuZVy5rZjvSF9dP9IHOGL5qFMkERvF2849jG2ABMYHTzH2P6d
9wNHuXyVzOp0foPHdoxxkoXTScu9S4DA+rjUVu15Mgow6BnWfWREggmkhRVNk4gv+V6gqFxnH00GL
MTXITQFpKjYxIPOw5gu3rNeFxo93xHlwY04hbu9xDe7DnQozHbHEPoZWE/METZh6Ro/J697KUO4c5dV7Dt
keV/elq/A3jV9CIAtwohErOoJSVZn8L6SDqc6lByLkmNu+Lp+YNv1zSS1AUyU/QH9Qj2g6QGItkYQevYBqX
Zgak42Wqb8yeMRhS4Cq6zCpFt1fUb6nJIcew+e9tcLOCNjKKquZmGLenCHabCorajvzdZ/VdXUqyekcaTpa
bt5djEIVl9cRZjG6fikv0=
        </xenc:CipherValue>
    </xenc:CipherData>
</xenc:EncryptedData>
</soap:Body>
</soap:Envelope>

```