



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Gebruikershandleiding Compliancevoorziening

WUS

Versie 1.32

Datum 16 september 2010

Colofon

Projectnaam	Digikoppeling
Versienummer	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 <i>Over Digikoppeling (voorheen Overheidservicebus)</i>	5
1.1.1 <i>Leidend principe: één stekker</i>	5
1.1.2 <i>Koppelvlak en koppelvlakstandaard</i>	5
1.2 <i>Interactiepatroon tussen organisaties</i>	6
1.3 <i>Terminologie</i>	6
1.4 <i>Gerelateerde documenten</i>	6
2 Over Digikoppeling 2 Compliancevoorziening WUS	7
2.1 <i>Service of cliënt slechts eenmaal valideren</i>	9
2.2 <i>Drie componenten</i>	9
2.3 <i>PKIoverheid-certificaten</i>	9
3 Service requester testvoorziening	10
3.1 <i>Vorbereiding</i>	10
3.1.1 <i>Transportlaag</i>	10
3.1.2 <i>Service requester implementeren</i>	10
3.1.3 <i>Service requester valideren</i>	11
3.2 <i>Mogelijke fouten</i>	12
4 Service provider testvoorziening	13
4.1 <i>Vorbereiding</i>	13
4.1.1 <i>Service provider implementeren</i>	13
4.2 <i>Service provider valideren</i>	13
4.3 <i>Mogelijke fouten</i>	15
Bijlage 1: Voorbeeldberichten	16
<i>Profiel OSB2W-be ping request</i>	16
<i>Profiel OSB2W-be ping request MTOM</i>	17
<i>Profiel OSB2W-be ping response</i>	18
<i>Profiel OSB2W-be response MTOM</i>	19
<i>Profiel OSB2W-be-S ping request</i>	20
<i>Profiel OSB2W-be-S ping request MTOM</i>	20
<i>Profiel OSB2W-be-S ping response</i>	20

<i>Profiel OSB2W-be-S ping response MTOM</i>	<i>20</i>
<i>Profiel OSB2W-be-SE ping request</i>	<i>20</i>
<i>Profiel OSB2W-be-SE ping request MTOM.....</i>	<i>20</i>
<i>Profiel OSB2W-be-SE ping response.....</i>	<i>20</i>
<i>Profiel OSB2W-be-SE ping response MTOM.....</i>	<i>20</i>

Inleiding

1.1 **Over Digikoppeling (voorheen Overheidsservicebus)**

Digikoppeling 2 Compliancevoorziening WUS is een onderdeel van Digikoppeling. Het project Digikoppeling definieert koppelvlakken om de uitwisseling van berichten tussen overheidsorganisaties — serviceaanbieders (service providers) en serviceafnemers (service requesters) — te standaardiseren. Deze uitwisseling valt uiteen in drie lagen:

1. **Inhoud**
Afspraken over de inhoud van het uit te wisselen bericht: structuur, semantiek, waardebereik enzovoort.
2. **Logistiek**
Afspraken over transportprotocol (HTTP), messaging (SOAP), beveiliging (authenticatie en encryptie) en betrouwbaarheid.
3. **Transport**
Het daadwerkelijke transport van het bericht.

Digikoppeling richt zich uitsluitend op de logistieke laag. De afspraken op deze laag zijn vastgelegd in 'koppelvlakstandaarden' en andere voorzieningen.

1.1.1 *Leidend principe: één stekker*

Overheidsorganisaties hebben aangegeven op een uniforme manier te willen aansluiten op Digikoppeling: één stekker. Digikoppeling biedt dit ene 'koppelvlak', waarmee alle interactie tussen organisatie onderling, via Digikoppeling, wordt afgehandeld. Koppelvlakstandaarden moeten zorgen voor maximale interoperabiliteit bij minimale ontwikkelinspanning. Daarom is gekozen voor bewezen, interoperabele internationale standaarden: de ebXML/ebMS- en WUS-families (WSDL, UDDI en SOAP) inclusief verwante standaarden. Organisaties die weinig expertise hebben op het gebied van ebXML en WUS kunnen berichten uitwisselen via WUS-lite en JMS (Java Message Service) via de Digikoppeling Gateway (lees hier meer over in de Digikoppeling Gateway-documentatie).

1.1.2 *Koppelvlak en koppelvlakstandaard*

Een koppelvlak is een interface die gegevensuitwisseling verzorgt. Werken met vérgaande, vaste standaarden is essentieel: het vergemakkelijkt implementatie. Ook wordt het mogelijk verschillende soorten berichten te versturen met een grote mate van interoperabiliteit. In de standaard zijn immers afspraken over inhoud gemaakt.

Kant-en-klare software

Eén van de belangrijkste eisen van de overheid voor inrichting van generieke voorzieningen, is dat er niet veel maatwerk ontwikkeld hoeft te worden. Er moet kant-en-klare commercieel of open geleverde software gebruikt worden. Voor Digikoppeling betekent dit dat geen software voor adapters wordt ontwikkeld, maar dat gekozen is voor internationaal (de jure of de facto) vastgelegde standaarden, die 'alle' leveranciers interoperabel hebben geïmplementeerd.

1.2 Interactiepatroon tussen organisaties

De afspraken die organisaties onderling maken over hun berichtenuitwisseling (het interactiepatroon), bepalen welke koppelvakstandaard nodig is: ebMS of WUS. Digikoppeling heeft Compliancevoorzieningen voor de ebMS- én voor de WUS-koppelvakstandaard. Dit document beschrijft alleen de laatste. Lees het document 'Digikoppeling Architectuur' voor meer over hoe interactiepatronen zich tot koppelvakstandaarden verhouden.

1.3 Terminologie

Lees voor uitleg van termen die binnen het Digikoppeling-project gebruikt worden in de 'Digikoppeling Glossary'.

1.4 Gerelateerde documenten

- Digikoppeling Koppelvakstandaard WUS 2.0 [KVS2]
- OCV WUS 2.0 Use Case Model
- Digikoppeling Compliancevoorziening WUS WSDL 2.0 [OCV2-WSDL]
- Digikoppeling Glossary

2 Over Digikoppeling 2 Compliancevoorziening WUS

Overheidsorganisaties die aansluiten op Digikoppeling willen bepalen of hun service(client)-implementaties aan de Digikoppeling WUS-standaard voldoen. De compliancevoorziening WUS is een web applicatie die de logistieke laag van deze implementaties valideert op basis van de Koppelvlakstandaard WUS. De URL van deze web applicatie is <https://www.wus.cv.osb.overheid.nl/ictu-ocvwus-war/>. Het valideren geschiedt door een voorgedefinieerd berichten uit te wisselen tussen de compliancevoorziening en een web service of web service cliënt implementatie. Welke berichten dit zijn, wordt bepaald door het WSDL-bestand (Web Services Description Language) dat ook het koppelvlak van de compliancevoorziening definieert [OCV2-WSDL].

Er zijn momenteel twee versies van Digikoppeling WUS. Voor Digikoppeling versie 1.x was een vorige versie van de compliancevoorziening WUS beschikbaar. Deze handleiding beschrijft het gebruik voor de nieuwe versie, de Digikoppeling 2 compliancevoorziening WUS. Deze compliancevoorziening ondersteunt hetzelfde profiel als versie 1.x (Digikoppeling2W-be) en tevens twee nieuwe profielen (Digikoppeling2W-be-S en Digikoppeling2W-be-SE). Voor ondersteuning van deze drie profielen is een nieuwe versie van de compliancevoorziening WUS ontwikkeld. De technische aspecten die samenhangen met deze profielen zijn te vinden in de Digikoppeling 2.0 Koppelvlakstandaard WUS. Bij toepassen van profielen Digikoppeling2W-be-S en Digikoppeling2W-be-SE worden timestamps toegepast. Tijdsynchronisatie van de systemen gaat hier dus een rol spelen. Tevens worden voor de profielen Digikoppeling2W-be-S en Digikoppeling2W-be-SE aparte rapporten gegenereerd die specifiek kijken naar aspecten die een rol spelen bij het ondertekenen en versleutelen van berichten (zie kolom "BSP Rapport").

Het contract (WSDL) dat voor communicatie met deze compliancevoorziening gebruikt moet worden is anders dan die van versie 1.x. Organisaties die dus al met versie 1 een test hebben uitgevoerd en nu een profiel van versie 2 willen testen dienen hier rekening mee te houden. De service(client)-implementatie moet dus op basis van een nieuwe WSDL ontwikkeld worden.

Het WSDL-bestand kunt u downloaden via:

- <http://wus.cv.prod.osb.overheid.nl/ictu-ocvwus-ws/OSB2W-be?wsdl=1>
- <http://wus.cv.prod.osb.overheid.nl/ictu-ocvwus-ws/OSB2W-be?xsd=1>
- <http://wus.cv.prod.osb.overheid.nl/ictu-ocvwus-ws/OSB2W-be?wsdl>

Deze WSDL is niet de WSDL voor het HTTPS endpoint. Voor de implementatie die over HTTPS moet communiceren moet de WSDL dus aangepast worden. Verander de soap:address location zoals hieronder in rood aangeven naar "https://www.wus.cv.prod.osb.overheid.nl/ictu-ocvwus-ws/secure/Digikoppeling2W-be".

Dus van:

```
<wsdl:service name="OSB2ComplianceService">
<wsdl:documentation>
```

```

    <wsi:Claim conformsTo="http://ws-i.org/profiles/basic/1.1" />
  </wsdl:documentation>
<wsdl:port name="OSB2"
binding="tns:OSB2ComplianceServiceBinding">
<soap:address
location="http://www.wus.cv.prod.osb.overheid.nl/wsdl/ictu-
ocvwus-ws/OSB2W-be"/>
</wsdl:port>
</wsdl:service>

```

Naar:

```

<wsdl:service name="OSB2ComplianceService">
<wsdl:documentation>
  <wsi:Claim conformsTo="http://ws-i.org/profiles/basic/1.1" />
  </wsdl:documentation>
<wsdl:port name="OSB2"
binding="tns:OSB2ComplianceServiceBinding">
<soap:address
location="https://www.wus.cv.prod.osb.overheid.nl/wsdl/ictu-
ocvwus-ws/secure/OSB2W-be"/>
</wsdl:port>
</wsdl:service>

```

Dit is slechts een voorbeeld voor één van de profielen. In totaal heeft OSB 2 WUS drie profielen. De andere twee endpoints zijn:

"<https://www.wus.cv.prod.osb.overheid.nl/ictu-ocvwus-ws/secure/OSB2W-be-S>"

"<https://www.wus.cv.osb.overheid.nl/ictu-ocvwus-ws/secure/OSB2W-be-SE>"

Het is de bedoeling om slechts met het endpoint te communiceren die de organisatie-client geïmplementeerd heeft. Het meest gangbare is het Digikoppeling2W-be profiel, dit komt tevens overeen met het profiel dat is beschreven in Digikoppeling Koppelvlakstandaard WUS 1.0. en 1.1 Alleen indien uw organisatie een web service dienst afneemt die het Digikoppeling2W-be-S of Digikoppeling2W-be-SE profiel vereist dient u ook op deze profielen een compliance test uit te voeren.

Indien een Digikoppeling web service binaire data gaat uitwisselen, is het aan te raden ook hiervoor eerst een compliancetest uit te voeren. Voor elk van de drie profielen is er een endpoint dat tevens de toepassing van MTOM ondersteunt:

"<https://www.wus.cv.osb.overheid.nl/ictu-ocvwus-ws/secure/OSB2W-be-MTOM>"

"<https://www.wus.cv.osb.overheid.nl/ictu-ocvwus-ws/secure/OSB2W-be-S-MTOM>"

"<https://www.wus.cv.osb.overheid.nl/ictu-ocvwus-ws/secure/OSB2W-be-SE-MTOM>"

De compliancevoorziening biedt 3 operaties waarvan alleen de "binData" operatie binaire data in de berichten heeft. Indien binaire data en dus het testen op MTOM/XOP van belang is, wordt aangeraden om deze operatie te gebruiken bij de compliance test.

2.1 Service of cliënt slechts eenmaal valideren

Is een implementatie van de web service of web service cliënt van de overheidsorganisatie eenmaal gevalideerd door de Digikoppeling Compliancevoorziening WUS, dan kan de organisatie bij andere implementaties dezelfde implementatie van de logistieke laag toepassen zonder die telkens te hoeven controleren.

2.2 Drie componenten

De Digikoppeling Compliancevoorziening WUS bestaat uit drie componenten met een gezamenlijke webinterface:

1. Service requester testvoorziening

Is een webservice. Deze verifieert of de webservice cliënt van de organisatie voldoet aan de Digikoppeling Koppelvlakstandaard WUS. Het vraag bericht wordt gevalideerd.

2. Service provider testvoorziening

Is een web service cliënt. Deze verifieert of de web service van de organisatie voldoet aan de Digikoppeling Koppelvlakstandaard WUS. Het antwoord bericht wordt gevalideerd.

3. Beheerfuncties

Beheer van rapporten en loggegevens.

De webinterface vindt u op <https://www.wus.cv.osb.overheid.nl/ictu-ocvwus-war/>.

2.3 PKIoverheid-certificaten

De Digikoppeling Koppelvlakstandaard WUS schrijft authenticatie voor met PKIoverheid-certificaten (Public Key Infrastructure). De compliancevoorziening maakt bij tweezijdige authenticatie gebruik van door programma OverheidsDienstenPlatform (ODP) uitgegeven testcertificaten. Meer informatie over certificaat gebruik binnen het Digikoppeling-domein kunt u vinden in het document Achtergrond Digikoppeling Certificaten.

3 Service requester testvoorziening

3.1 Voorbereiding

Bij het testen van de service requester implementatie moeten twee zaken zijn geregeld:

1. De transportlaag (TLS, Transport Layer Security) moet geconfigureerd zijn (trust- en keystores).
2. De compliance cliënt van uw organisatie moet geïmplementeerd zijn en het te valideren Digikoppeling WUS profiel ondersteunen.
3. Indien men het Digikoppeling2W-be-SE profiel toepast moet men de publieke sleutel (TLS certificaat) van het OCV SR endpoint gebruiken voor versleuteling. De OCV SR zal het certificaat dat is gebruikt voor ondertekening van requestbericht gebruiken voor versleuteling van het responsebericht.

De handelingen lichten we hieronder toe.

3.1.1 *Transportlaag*

TLS configuratie is implementatie specifiek. Er wordt hier alleen een test beschreven waarmee u kunt vaststellen of de Service requester testvoorziening het privatekeycertificaat van uw webservice cliënt accepteert.

Testen van TLS laag

Hierbij worden dus de testcertificaten gebruikt om vast te stellen of de compliancevoorziening uw client testcertificaat accepteert. U importeert de private key in uw browser. Voer deze test alleen uit om vast te stellen of problemen in de communicatie optreden doordat geen TLS/SSL-verbinding (Secure Socket Layer) tot stand komt.

Importeer het clientcertificaat (private key), inclusief de hele certificaathierarchie, in uw webbrowser. In Microsoft Internet Explorer kan dit via het menu Extra, Internetopties, tab 'Inhoud'. Vervolgens:

1. Ga naar de beveiligde locatie van de WSDL (zie hoofdstuk 2)
2. Wordt uw certificaat vertrouwd door de compliancevoorziening, dan het betreffende bestand (WSDL of XSD) weergegeven.
3. Krijgt u een foutmelding, bijvoorbeeld een 401-fout of 'not authenticated'? Dan gebruikt u mogelijk een verkeerd certificaat. Controleer of u een correct Digikoppeling-testcertificaat heeft. Krijgt u verschillende keren een foutmelding, neem dan contact op (zie contactgegevens).

3.1.2 *Service requester implementeren*

Er is helaas geen stappenplan voor het implementeren van de compliance client. Hoe dit werkt, hangt namelijk af van de keuzes die u bij het inrichten van de software maakt. Er bestaan veel toolkits die op basis van een WSDL een goede basisimplementatie verzorgen. Ervaringen kunnen leiden tot best practices die later beschikbaar komen.

Voorbeeldberichten

Als de implementatie van uw client correct is, zou u berichten moeten kunnen genereren die lijken op de berichten zoals weergegeven in bijlage

3.1.3

Service requester valideren

Om uw client te valideren, stuurt u een bericht naar de Digikoppeling Compliancevoorziening.

In de Digikoppeling Compliancevoorziening WSDL staan de volgende twee operaties gedefinieerd:

- **ping**
De service controleert het vraag bericht ping.
- **toUpperCase**
De service controleert het vraag bericht toUpperCase.
- **binData**
De service controleert het vraag bericht binData. Dit bericht is speciaal bedoeld voor het valideren van het toepassen van MTOM/XOP. Dit bericht bevat dan ook binaire data. Standaard wordt als binaire data het Digikoppeling logo in response meegestuurd.

De test bestaat uit het versturen van het ping, toUpperCase of het binData bericht volgens een van de drie Digikoppeling 2 profielen en ontvangen van het bijbehorende antwoord bericht. De drie Digikoppeling profielen worden beschreven in de betreffende koppelvlakstandaard. De Service requester testvoorziening biedt voor elk Digikoppeling WUS profiel een web service endpoint, i.e. Digikoppeling2W-be, Digikoppeling2W-be-S en Digikoppeling2W-be-SE. Hiermee moet rekening worden gehouden bij het uitvoeren van de test (stuur een requestbericht van een bepaald profiel naar het juiste endpoint).

Bij tests van het Digikoppeling2W-be-S en Digikoppeling2W-be-SE profiel, dus bij het ondertekenen en versleutelen moet rekening worden gehouden dat de te gebruiken certificaten ondertekend zijn door TEST Digikoppeling CSP CA (hiërarchie van de Digikoppeling testcertificaten). Hierbij worden dezelfde sleutels gebruikt als bij TLS/SSL. Voor ondertekenen de eigen private sleutel en voor versleutelen de publieke sleutel van de partner.

MTOM wordt door alle OCS SR endpoints (profielen) ondersteund. Het gebruik hiervan wordt bepaald door het request bericht (zie [KVS2]).

Nadat het antwoord bericht is ontvangen en hierin geen foutmeldingen staan kunt u in de webinterface van de compliancevoorziening het rapport bekijken en downloaden. Op basis van datum en tijd kunt u achterhalen welk rapport betrekking heeft op uw bericht.



OVERHEIDSSERVICEBUS

Home

Test met CVWUS-SP

WS-I rapporten Service Provider test

WS-I rapporten Service Requester test

Inloggen beheerder

Beheer WS-I Rapporten

WSI rapport	BSP rapport	Type test	wsa:from
18-05-2009 12:41:04		CWWUS_SR	
18-05-2009 12:40:08		CWWUS_SR	
18-05-2009 12:38:49		CWWUS_SR	
18-05-2009 12:37:19		CWWUS_SR	
18-05-2009 12:36:34		CWWUS_SR	
12-05-2009 14:57:11		CWWUS_SR	
04-05-2009 11:40:13		CWWUS_SR	
27-04-2009 13:53:16		CWWUS_SR	
27-04-2009 13:48:00		CWWUS_SR	
27-04-2009 13:22:22		CWWUS_SR	
27-04-2009 13:09:44		CWWUS_SR	
27-04-2009 13:07:35		CWWUS_SR	
23-04-2009 16:48:02		CWWUS_SR	
23-04-2009 16:47:39		CWWUS_SR	
23-04-2009 16:44:43		CWWUS_SR	
23-04-2009 16:30:08		CWWUS_SR	
23-04-2009 16:27:53		CWWUS_SR	
23-04-2009 16:25:32		CWWUS_SR	

Klik in het menu, links in het scherm, op 'WS-I rapporten Service requester test' om het rapport te downloaden.

Let op

Rapporten worden na verloop van tijd verwijderd. Maak dus een kopie voor uzelf.

3.2 Mogelijke fouten

Er kunnen een aantal zaken fout gaan, bijvoorbeeld:

- De Service requester krijgt geen bericht terug.
- De beveiligde verbinding wordt niet (goed) opgezet.

Het is ook mogelijk dat het antwoord bericht van de service een foutbericht (SOAPFault) naar uw client stuurt om een aan te geven dat een bepaald onderdeel niet conform Digikoppeling is. De volgende fouten worden mogelijk in het antwoord bericht aangegeven:

- Requestbericht structuur voldoet niet aan contract
- Invalide SOAP 1.1 envelope namespace
- Karaktercodering bericht niet volgens UTF-8
- Requestbericht inhoud boven 50 karakters
- Fout bij uitvoeren van operatie
- WS-I testrapport niet kunnen maken
- Ondertekening- of versleutelingsfouten

Afhankelijk van uw web service cliënt implementatie kunt u details van dit soort meldingen bekijken in uw logbestanden of via de (web)interface van uw cliënt. Als deze fouten niet optreden wordt er door de Service requester testvoorziening een testrapport opgesteld dat voor een groot deel gelijk is aan een WS-I Basic Profile 1.1 testrapport en bij toepassing van profiel DigikoppelingW2-be-S of DigikoppelingW2-be-SE ook WS-I Basic Security Profile 1.0.

4 Service provider testvoorziening

4.1 Voorbereiding

Deze voorziening dient voor het valideren van uw web service implementatie. Voordat u begint met het uitwisselen van berichten met de compliancevoorziening, moeten het volgende zijn geregeld:

- De compliance service van uw organisatie moet geïmplementeerd zijn.
- De key- en truststores zijn geconfigureerd
- Indien men het Digikoppeling2W-be-SE profiel toepast moet men de publieke sleutel (TLS certificaat) van organisatie-compliance service endpoint gebruiken voor versleuteling. De OCV SP zal het certificaat gebruiken voor ondertekening van het requestbericht gebruiken voor versleuteling van het responsebericht.

4.1.1 Service provider implementeren

Download de Digikoppeling Compliancevoorziening WUS WSDL om uw service in te richten (zie hoofdstuk 2 voor URL van WSDL).

Controle

U heeft wedermaal de keuze uit twee operaties:

- **Ping**
De Service provider testvoorziening controleert het antwoord bericht (pingResponse).
- **toUpperCase**
De Service provider testvoorziening controleert het antwoord bericht (toUpperCaseResponse).
- **binData**
De compliancevoorziening controleert het binData responsebericht. Dit bericht is speciaal bedoeld voor het valideren van het toepassen van MTOM/XOP (payload bevat {http://www.w3.org/2001/XMLSchema}base64Binary element). De OCV vult dit element standaard met het Digikoppeling logo plaatje (osb_logo.jpg).

4.2 Service provider valideren

Voor het valideren van een web service kunt u de web interface gebruiken. Deze interface vindt u op <https://www.wus.cv.osb.overheid.nl/ictu-ocvwus-war>

In het linker menu klikt u op "Test met CVWUS-SP". De gegevens die in dit scherm ingevoerd moeten worden dienen om een bericht te sturen naar uw web service.

Om uw compliancetest stapsgewijs uit te voeren, kunt u valideren via HTTP (Hypertext Transfer Protocol). Hiermee voorkomt u problemen die tweerichtingsauthenticatie via TLS (Transport Layer Security) met zich meebrengt. Na de HTTP-test, voert u een tweede controle uit, via HTTPS (Secure HTTP). Zo weet u zeker of tweerichtingsauthenticatie op basis van de PKI Overheid-certificaten werkt.

In de webinterface vult u gegevens in als de URL van de door u geïmplementeerde web service. Via de webinterface kiest u ook *één* van de operaties Ping, toUpperCase of binData.

Vul de volgende velden in en maak de benodigde selecties om een compliancetest uit te voeren:

Web service Endpoint

Inhoud van het bericht (voor ping en toUpperCase operaties)

Operatie:

- Ping
- toUpperCase
- binData (hierbij wordt inhoud van het bericht door het systeem bepaald)

Protocol (wel of niet tweezijdige SSL/TLS):

- HTTP
- HTTPS

Activeer MTOM (wel of niet volgens MTOM een bericht versturen):

- (de-) Activeer (Het request bericht wordt verstuurd met toepassing van de MTOM standaard. De service moet dit request kunnen accepteren en een response volgens MTOM kunnen geven.)

Selecteer het Digikoppeling profiel:

- Digikoppeling2W-be
- Digikoppeling2W-be-S
- Digikoppeling2W-be-SE

Encryptie certificaat (Publieke sleutel van paar dat de web service gebruikt om bericht te ontsleutelen)

Indien men het Digikoppeling2W-be-S profiel kiest, worden de berichtonderdelen versleuteld met de sleutel van het OCV sleutelpaar. Het publieke deel wordt meegestuurd in het bericht. De betreffende hiërarchie

van deze sleutel dient in de truststore te staan die gebruikt wordt bij verifiëren van de ondertekening. Deze is gelijk aan de hiërarchie van de Digikoppeling TLS testcertificaten.

Indien men het Digikoppeling2W-be-SE profiel kiest, dient de publieke sleutel ge-upload te worden van het sleutel paar dat de organisatie-compliance service gebruikt om het bericht te kunnen ontsleutelen.

Klik op 'Verstuur' om een bericht naar uw organisatie-compliance service te sturen.

Nadat het antwoord bericht is ontvangen wordt dit in het scherm aangegeven, eventueel kunt u ook in het linker menu op "WS-I rapporten Service Provider test" klikken en het rapport bekijken en eventueel opslaan.



The screenshot shows the 'OVERHEIDSSERVICEBUS' interface. It features a navigation menu on the left with options like 'Home', 'Test met CVWUS-SP', 'WS-I rapporten Service Provider test', 'WS-I rapporten Service Requester test', and 'Inloggen beheerder'. The main content area displays a table titled 'Beheer WS-I Rapporten' with columns for 'WSI rapport', 'BSP rapport', 'Type test', and 'wsa:From'. The table contains multiple rows of test results, each with a timestamp and a 'CVWUS_SR' identifier.

WSI rapport	BSP rapport	Type test	wsa:From
18-05-2009 12:41:04		CVWUS_SR	
18-05-2009 12:40:08		CVWUS_SR	
18-05-2009 12:38:49		CVWUS_SR	
18-05-2009 12:37:19		CVWUS_SR	
18-05-2009 12:36:34		CVWUS_SR	
12-05-2009 14:57:11		CVWUS_SR	
04-05-2009 11:40:13		CVWUS_SR	
27-04-2009 13:53:16		CVWUS_SR	
27-04-2009 13:48:00		CVWUS_SR	
27-04-2009 13:22:22		CVWUS_SR	
27-04-2009 13:09:44		CVWUS_SR	
27-04-2009 13:07:35		CVWUS_SR	
23-04-2009 16:48:02		CVWUS_SR	
23-04-2009 16:47:39		CVWUS_SR	
23-04-2009 16:44:43		CVWUS_SR	
23-04-2009 16:30:08		CVWUS_SR	
23-04-2009 16:27:53		CVWUS_SR	
23-04-2009 16:25:32		CVWUS_SR	

Let op:

Rapporten worden na verloop van tijd verwijderd. Maak dus een kopie voor uzelf.

4.3

Mogelijke fouten

Er kunnen een aantal zaken fout gaan, bijvoorbeeld:

- De compliancevoorziening krijgt geen bericht terug.
- De beveiligde verbinding wordt niet (goed) opgezet.

Over het algemeen zal in het rapport mogelijke fouten aangegeven worden. In aantal gevallen zal in het scherm van de OCV SP een foutmelding getoond worden, zoals bij TLS/SSL fouten.

Bijlage 1: Voorbeeldberichten

Profiel OSB2W-be ping request

```

POST /ictu-ocvwus-ws/OSB2W-be HTTP/1.1
Content-Length: 778
Content-Transfer-Encoding: binary
SOAPAction: ""
User-Agent: Mozilla/4.0 [en] (WinNT; I)
Content-Type: text/xml;charset="utf-8"
Accept: text/xml, multipart/related, text/html,
image/gif, image/jpeg, *; q=.2, */*; q=.2
User-Agent: JAX-WS RI 2.1.3-b02-
Host: 127.0.0.1:81
Connection: keep-alive

<?xml version="1.0" ?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <wsa:MessageID
xmlns:wsa="http://www.w3.org/2005/08/addressing"
      >00000120-e744-24df-0000-
0120e74424df@services.ictu.nl</wsa:MessageID>
    <wsa:To
xmlns:wsa="http://www.w3.org/2005/08/addressing"
      >http://nl/ictu/ocvwus/war/ComplianceServiceRequest</wsa
:To>
    <wsa:Action
xmlns:wsa="http://www.w3.org/2005/08/addressing"
      >http://service.compliance.osb.gbo.overheid.nl/wsdl/2009
/02/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest</wsa:Action>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <osb:ping
xmlns:osb="http://service.compliance.osb.gbo.overheid.nl
/200706/osb-compliancevoorziening.xsd">
      <osb:berichtIn>test</osb:berichtIn>
    </osb:ping>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Profiel OSB2W-be ping request MTOM

```

POST /ictu-ocvwus-ws/OSB2W-be-MTOM HTTP/1.1
Outer-Content-Type: multipart/related;
type="application/xop+xml"; start-info="text/xml"
Content-Length: 1055
Content-Transfer-Encoding: binary
Root-content-type: application/xop+xml; charset=UTF-8;
type="text/xml"
SOAPAction: ""
User-Agent: Mozilla/4.0 [en] (WinNT; I)
Content-Type:
multipart/related;start="<rootpart*25103086-a074-4868-
92cb-
4eaf8a1368ec@example.jaxws.sun.com>";type="application/x
op+xml";boundary="uuid:25103086-a074-4868-92cb-
4eaf8a1368ec";start-info="text/xml"
  Accept: text/xml, multipart/related, text/html,
image/gif, image/jpeg, *; q=.2, */*; q=.2
  User-Agent: JAX-WS RI 2.1.3-b02-
  Host: 127.0.0.1:81
  Connection: keep-alive

--uuid:25103086-a074-4868-92cb-4eaf8a1368ec
Content-Id: <rootpart*25103086-a074-4868-92cb-
4eaf8a1368ec@example.jaxws.sun.com>
Content-Type: application/xop+xml; charset=utf-
8; type="text/xml"
Content-Transfer-Encoding: binary

<?xml version="1.0" ?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <wsa:MessageID
xmlns:wsa="http://www.w3.org/2005/08/addressing"
    >00000120-e74f-b69a-0000-
0120e74fb69a@services.ictu.nl</wsa:MessageID>
    <wsa:To
xmlns:wsa="http://www.w3.org/2005/08/addressing"
>http://nl/ictu/ocvwus/war/ComplianceServiceRequest</wsa
:To>
    <wsa:Action
xmlns:wsa="http://www.w3.org/2005/08/addressing">
http://service.compliance.osb.gbo.overheid.nl/wsdl/2009/
02/compliancevoorziening-
v2/IOSB2ComplianceService/pingRequest</wsa:Action>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <osb:ping
xmlns:osb="http://service.compliance.osb.gbo.overheid.nl
/200706/osb-compliancevoorziening.xsd">
      <osb:berichtIn>test</osb:berichtIn>
    </osb:ping>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
--uuid:25103086-a074-4868-92cb-4eaf8a1368ec--

```

Profiel OSB2W-be ping response

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=97C0D60C125CF587B2C9AF89917234F1;
Path=/ictu-ocvwus-ws
Content-Type: text/xml; charset=utf-8
Transfer-Encoding: chunked
Date: Mon, 27 Apr 2009 11:09:44 GMT

382
<?xml version="1.0" ?>
<S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Header>
    <To xmlns="http://www.w3.org/2005/08/addressing"
>http://www.w3.org/2005/08/addressing/anonymous</To>
    <Action
xmlns="http://www.w3.org/2005/08/addressing"
>http://service.compliance.osb.gbo.overheid.nl/wsdl/2009
/02/compliancevoorziening-
v2/IOSB2ComplianceService/pingResponse</Action>
    <MessageID
xmlns="http://www.w3.org/2005/08/addressing"
>uuid:82200625-b18d-407b-9bd1-
b46a8158e291</MessageID>
    <RelatesTo
xmlns="http://www.w3.org/2005/08/addressing"
>00000120-e744-24df-0000-
0120e74424df@services.ictu.nl</RelatesTo>
  </S:Header>
  <S:Body>
    <pingResponse
xmlns="http://service.compliance.osb.gbo.overheid.nl/200
706/osb-compliancevoorziening.xsd"
xmlns:ns2="http://service.compliance.osb.gbo.overheid.nl
/xsd/2009/02/compliancevoorziening-v2">
      <berichtUit>Ping: test</berichtUit>
    </pingResponse>
  </S:Body>
</S:Envelope>
0

```

Profiel OSB2W-be response MTOM

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=50CDCFC5B18233389DB235326F93EE1F;
Path=/ictu-ocvwus-ws
Content-Type:
multipart/related;start="<rootpart*d4c5bc85-63a0-4d7b-
b359-
89147b786e2a@example.jaxws.sun.com>";type="application/x
op+xml";boundary="uuid:d4c5bc85-63a0-4d7b-b359-
89147b786e2a";start-info="text/xml"
  Transfer-Encoding: chunked
  Date: Mon, 27 Apr 2009 11:22:22 GMT

  468
  --uuid:d4c5bc85-63a0-4d7b-b359-89147b786e2a
  Content-Id: <rootpart*d4c5bc85-63a0-4d7b-b359-
  89147b786e2a@example.jaxws.sun.com>
  Content-Type: application/xop+xml;charset=utf-
  8;type="text/xml"
  Content-Transfer-Encoding: binary

  <?xml version="1.0" ?>
  <S:Envelope
  xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
    <S:Header>
      <To xmlns="http://www.w3.org/2005/08/addressing"

  >http://www.w3.org/2005/08/addressing/anonymous</To>
      <Action
  xmlns="http://www.w3.org/2005/08/addressing">
  http://service.compliance.osb.gbo.overheid.nl/wsdl/2009/
  02/compliancevoorziening-
  v2/IOSB2ComplianceService/pingResponse</Action>
      <MessageID
  xmlns="http://www.w3.org/2005/08/addressing"
  >uuid:c17722cd-7cfe-4c19-81c6-
  2e5eca61b9c8</MessageID>
      <RelatesTo
  xmlns="http://www.w3.org/2005/08/addressing"
  >00000120-e74f-b69a-0000-
  0120e74fb69a@services.ictu.nl</RelatesTo>
    </S:Header>
    <S:Body>
      <pingResponse

  xmlns="http://service.compliance.osb.gbo.overheid.nl/200
  706/osb-compliancevoorziening.xsd"

  xmlns:ns2="http://service.compliance.osb.gbo.overheid.nl
  /xsd/2009/02/compliancevoorziening-v2">
        <berichtUit>Ping: test</berichtUit>
      </pingResponse>
    </S:Body>
  </S:Envelope>
  2f
  --uuid:d4c5bc85-63a0-4d7b-b359-89147b786e2a--
  0

```

Profiel OSB2W-be-S ping request

Profiel OSB2W-be-S ping request MTOM

Profiel OSB2W-be-S ping response

Profiel OSB2W-be-S ping response MTOM

Profiel OSB2W-be-SE ping request

Profiel OSB2W-be-SE ping request MTOM

Profiel OSB2W-be-SE ping response

Profiel OSB2W-be-SE ping response MTOM