Bancaire Infrastructurele Voorziening

Implementatie conform koppelvlak WUS 2.0 Bedrijven

Versie	0.1
Datum	28 november 2017
Status	Definitief

Colofon

Projectnaam	SBR Banken – Bancaire Infrastructurele Voorziening
Versienummer	0.1
Organisatie	Financiële Rapportages Coöperatief B.A. Bijlmerdreef 24 ACT A.03.078 1102 CT Amsterdam frc-proces-en-infra@sbrbanken.nl
Bronnen	Dit document volgt het document Koppelvlakbeschrijving Digipoort WUS 2.0 Bedrijven versie 1.2, zowel in bewoording als in structuur.

Inhoudsopgave

1 Inleiding

1.1 Doel en doelgroep

Dit document beschrijft de afspraken met betrekking tot het elektronische berichtenverkeer bij banken via de Bancaire Infrastructurele Voorziening (BIV) van het Financieel Rapportages Coöperatief (FRC).

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

1.2 Leeswijzer

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

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

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

1.3 Status

Dit document beschrijft de afspraken met betrekking tot het bankenprofiel van het koppelvlak WUS 2.0 voor Bedrijven van de BIV. De verwachting is dat de gebruikte open standaarden zich de komende jaren verder zullen ontwikkelen en dat de communicatiebehoefte ook aan verandering onderhevig zal zijn. Het gevolg hiervan is dat de komende jaren nieuwe releases van de BIV in gebruik zullen worden genomen. Dat kan gevolgen hebben voor het koppelvlak.

Het FRC streeft ernaar om nieuwe releases in nauw overleg met de markt te realiseren. Om het voor marktpartijen snel en eenvoudig mogelijk te maken om gebruik te maken van de BIV, is er voor gekozen zoveel mogelijk open standaarden en bestaande voorzieningen te gebruiken. Voorbeelden daarvan zijn het gebruik van SOAP en de toepassing van PKIoverheidcertificaten.

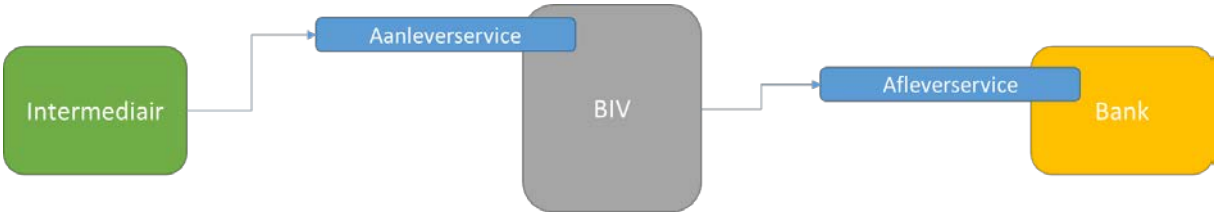
Aanvullende informatie met betrekking tot ondersteuning bij het gebruik van de services van de BIV is beschikbaar op de website: http://www.sbrbanken.nl/.

2 Berichtenverkeer

2.1 Inleiding

De BIV kent services gericht op intermediairs en op aangesloten banken. Deze services kunnen worden gebruikt voor het aanleveren van diverse financiële reportages, zoals bijvoorbeeld kredietrapportages, vastgoedrapportages, etc.

In onderstaande afbeelding zijn de services schematisch weergegeven.



Figuur 1: Services binnen de BIV

Deze koppelvlakbeschrijving vormt de basis voor de services die de BIV biedt aan bedrijven. Binnen de BIV, in tegenstelling tot Digipoort, omvatten deze services vooralsnog alleen de Aanleverservice. De details van de Aanleverservice zijn beschreven in een afzonderlijk document.

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

2.2 Beveiliging

2.2.1 Transportniveau

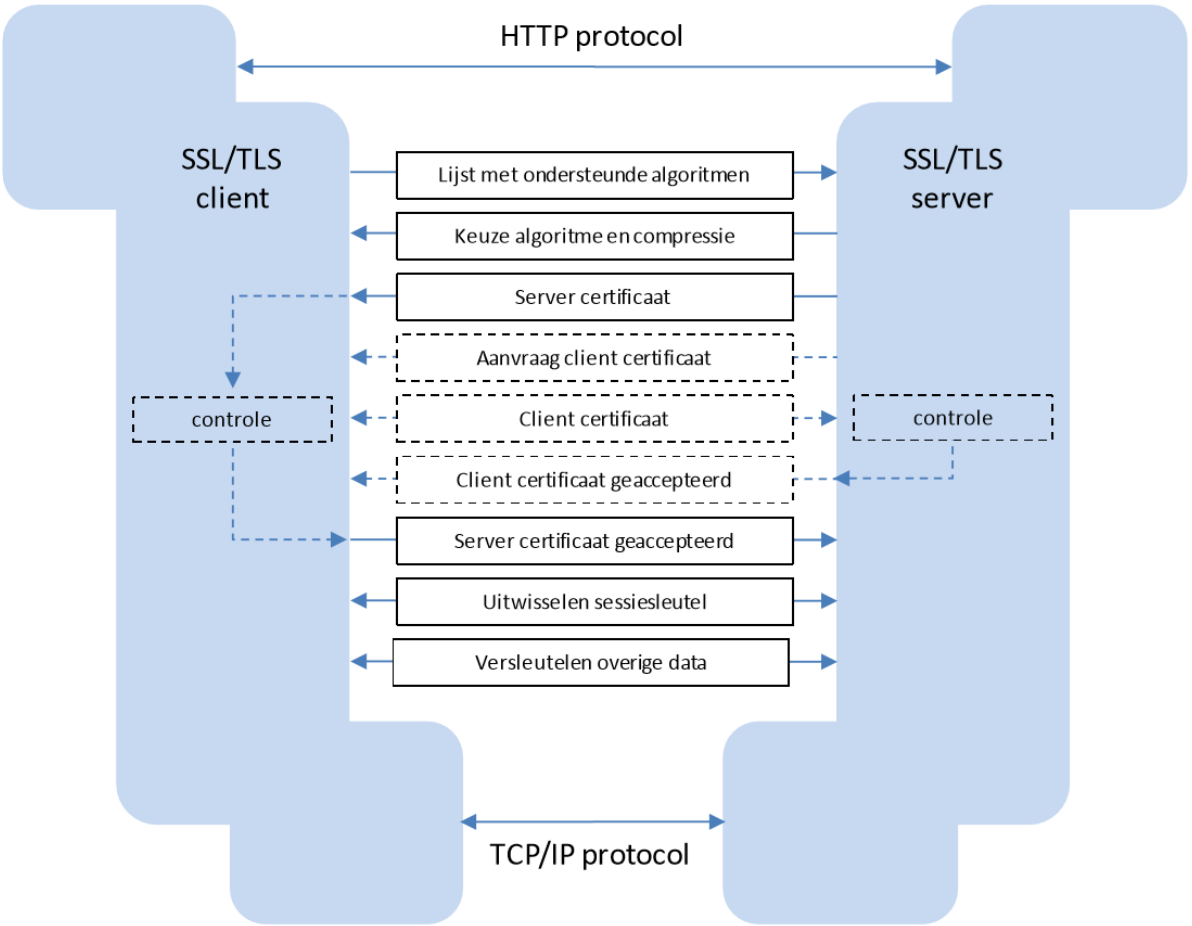
De authenticiteit van systemen in de BIV en van de gebruikers van een service moet door alle deelnemende partijen vastgesteld kunnen worden voordat een datacommunicatiesessie wordt gestart. De authenticiteit van systemen wordt met behulp van PKIoverheid-certificaten gecontroleerd.

Voor een aansluiting op de BIV bent u verplicht gebruik te maken van een PKIoverheid-certificaat (X.509). Dit certificaat waarborgt de veiligheid en betrouwbaarheid van de verbinding tussen uw systeem en de BIV.
In software zal de intermediair een eigen PKIoverheidscertificaat (kantoorcertificaat) moeten gebruiken voor communicatie met de BIV. Dit certificaat moet ook worden opgenomen op de whitelist van de BIV. Dit geldt zowel voor de acceptatie- als de productieomgeving van de BIV. Het aanmelden en registreren van het certificaat kan via https://aansluiten.frcportaal.nl/.

U kunt een PKIoverheid-certificaat aanvragen via een Certificate Service Provider (CSP). Een overzicht van de huidige CSP's is te vinden op de website van Logius, zie https://www.logius.nl/diensten/pkioverheid/aanschaffen/. Wegens de doorlooptijd van de aanvraag, adviseren wij u een PKIoverheid-certificaat vroegtijdig aan te vragen.

Feitelijk wordt de authenticiteit van bedrijven bepaald aan de hand van het PKIoverheid-clientcertificaat dat zich op het cliëntsysteem bevindt. Met behulp van dit certificaat opent de client een verbinding volgens het TLS-protocol (voorheen SSL, zie het overzicht in figuur 2). Dit protocol biedt naast authenticatie ook encryptie op transportniveau.

De geldigheid van het clientcertificaat wordt aan de hand van de gegevens in het certificaat gecontroleerd. Tevens wordt gecontroleerd of het certificaat voor gebruik binnen de BIV is goedgekeurd middels een whitelist.



Figuur 2: TLS/SSL Communicatie

Op transportniveau is de partij die wordt geauthenticeerd de partij waarmee de TLS-verbinding tot stand komt. Dit zal in de praktijk een intermediair zijn die voor één of meerdere bedrijven de verbinding met de BIV verzorgt. Op transportniveau is het dus niet noodzakelijkerwijs de 'eigenaar' van de berichten (het bedrijf namens wie de rapportage wordt verstuurd) wiens identiteit wordt gecontroleerd.

2.2.2 Berichtniveau

Op berichtniveau wordt beveiliging toegepast door gebruik van WS-Security. Het bericht dient beveiligd te zijn met een handtekening over de SOAP body- en de SOAP header-elementen. Het

certificaat dat hiervoor gebruikt wordt, moet aan dezelfde eisen voldoen als het certificaat dat gebruikt wordt op transportniveau. Het hoeft echter niet hetzelfde certificaat te zijn.

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

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

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

3 Sessieverloop

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

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

Elke service bestaat tenminste uit de volgende onderdelen:

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

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

3.1 Controleren verzoek

SOAP-berichten die aan de BIV worden aangeboden en SOAP-berichten die door de BIV naar een intermediair worden verstuurd, zijn opgemaakt conform een voorgedefinieerde structuur (SOAP request). Deze structuur is vastgelegd in een XML Schema (XSD), dat op zijn beurt is opgenomen in de WSDL die de webservice formeel beschrijft. Bij de beschrijving van elke service zijn WSDL en XSD bijgevoegd.

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

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

3.2 Ontvangen verzoek

Elk verzoek aan een service van de BIV wordt vastgelegd in de auditlog. De auditlog fungeert binnen de BIV als audit trail. De berichten zelf worden niet opgeslagen, enkel de metadata. Op dezelfde wijze kan de intermediair verzoeken van de BIV vastleggen in een eigen berichtenadministratie.

3.3 Versturen antwoord

Wanneer het verzoek voldoet aan alle gestelde eisen, wordt het antwoord verstuurd. Elk antwoord van de BIV wordt vastgelegd in de auditlog.

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

De deelnemende banken hebben strenge beveiligingseisen gesteld aan de BIV. Zo mag er geen informatie opgeslagen worden (afgezien van tijdelijke opslag voor directe verwerking). Hierdoor kan de BIV nu geen gebruik maken van een wachtrij (queue) voor de opslag van berichten totdat ze verwerkt kunnen worden. Evenmin kunnen gedetailleerde foutmeldingen opgeslagen worden tot het moment waarop de initiële verzender het resultaat zou opvragen.

De BIV maakt dus gebruik van synchrone verwerking in plaats van asynchrone verwerking zoals op Digipoort wordt toegepast. Op het moment van aflevering blijft de verbinding in stand totdat de validatie en verwerking zijn afgerond en het resultaat als SOAP response is teruggestuurd. Het opvragen van de status via een Statusinformatieservice is momenteel dan ook overbodig.

Meer informatie over de verschillen met Digipoort zijn te vinden in de documentatie over de Aanleverservice.

4 SOAP-bericht

Het bankenprofiel van het koppelvlak ‘WUS 2.0 voor Bedrijven’ maakt gebruik van de SOAP 1.1-standaard voor de samenstelling van elektronische berichten. SOAP is een gebruikelijke standaard bij elektronisch berichtenverkeer op basis van services.

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

4.1 Structuur

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

Onder koppelvlakversie 1.2 maken de services gebruik van een generiek schema (XSD), waarin alle berichttypen zijn gespecificeerd. Deze XSD is als aparte bijlage in de documentatieset opgenomen.

4.2 Adressering

BIV-services onder het ‘WUS 2.0 voor Bedrijven’-koppelvlak maken gebruik van WS-Addressing, waarmee het mogelijk is om berichten te routeren onafhankelijk van het gebruikte transportprotocol.

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

4.3 Ondertekening bericht (WS-Security)

Berichten dienen digitaal te worden ondertekend. Hiervoor wordt gebruik gemaakt van de ‘WS-Security’-standaard. Ondertekenen geldt voor zowel request- als responsberichten.

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

4.4 Message Transmission Optimization Mechanism (MTOM)

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

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

Bij het toepassen van MTOM wordt ook wel gesproken van een geoptimaliseerd bericht. MTOM is beschreven in WS-I Basic Profile 1.2 (zie http://www.w3.org/TR/soap12-mtom/). De meeste gangbare toolkits kunnen MTOM-berichten ontvangen en versturen. Het wel of niet toepassen van MTOM kan in de regel worden aangegeven middels een configuratiebestand of vanuit de code. Op deze manier wordt aan de webservice meegegeven of deze MTOM gebruikt dan wel kan gebruiken bij het ontvangen en versturen van berichten.

Het daadwerkelijke gebruik van MTOM wordt feitelijk door de service requester bepaald; de service requester neemt hierin het initiatief. Indien een op MTOM ingerichte webservice een geoptimaliseerd bericht ontvangt, zal de respons ook geoptimaliseerd worden teruggestuurd. Indien het request niet was geoptimaliseerd (geen gebruik van MTOM) wordt ook de respons niet geoptimaliseerd.

5 WS-Addressing

De BIV maakt gebruik van WS-Addressing 1.0 met namespace http://www.w3.org/2005/08/addressing.

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

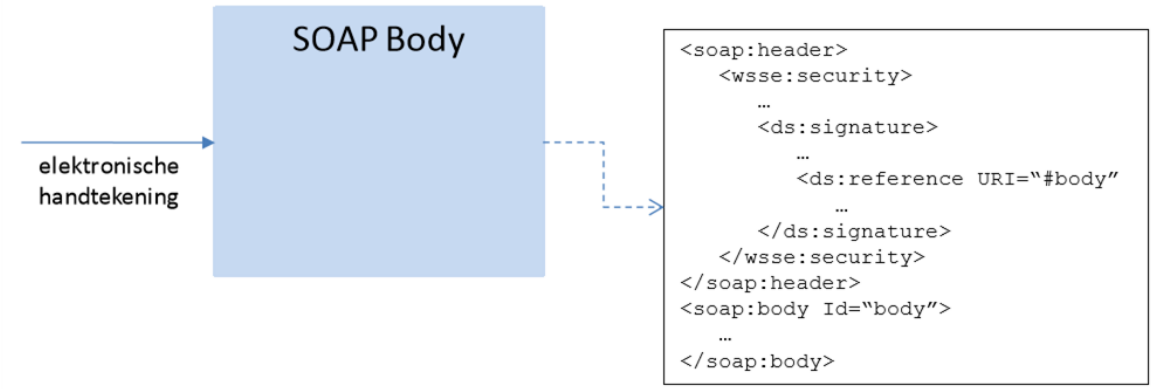
Element	Toelichting	Verplicht
wsa:To	De WSDL-waarde (request) of http://www.w3.org/2005/08/addressing/none of http://www.w3.org/2005/08/addressing/anonymous (response)	Ja
wsa:Action	Deze waarde wordt gebruikt om een specifieke operatie aan te roepen.	Ja
wsa:MessageID	Het unieke id voor dit bericht als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

6 WS-Security

Een bedrijf of intermediair dient onderdelen van een SOAP-bericht te tekenen[1]. Deze onderdelen worden als het ware voorzien van een elektronische handtekening door er een versleuteling op toe te passen middels een PKIoverheid-certificaat.

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

Voorbeeld (ondertekenen Body):



Figuur 3: Digitaal ondertekenen volgens WS-Security

Het toepassen van WS-Security levert het volgende op:

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

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

6.1 Tekenen van het bericht

De volgende onderdelen worden ondertekend:

- soap-env:Body
- het header-onderdeel Timestamp
- het header-onderdeel WS-Addressing (alle elementen)

[1] Dit geldt voor request- en response-berichten. SOAP fault-berichten worden niet ondertekend.

De volgende eisen gelden voor de WS-Security elementen:

http://www.w3.org/2000/09/xmldsig#

Stap 1: Canonicalization

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

Stap 2: Digest

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

Stap 3: Signature

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

6.2 Tijdstempel Aangemaakt

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

Voorbeeld:

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

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

Element	TimeStamp
Verplicht	Ja

Element	Created
Verplicht	Ja
Type	DateTime in UTC

Element	Expires
Verplicht	Nee
Type	DateTime in UTC

7 Algemene afspraken

7.1 Communicatiestandaarden

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

Laag	Standaard
Applicatielaag	SOAP
	XML
Sessielaag	HTTP
Transportlaag	TCP
Netwerklaag	IP

7.2 Prefixen

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

Prefix	Specificatie	Namespace URI
ns	WUS 2.0 versie 1.2	http://logius.nl/digipoort/koppelvlakservices/1.2/
soapenv	SOAP 1.1	http://schemas.xmlsoap.org/soap/envelope/
wsdl	WSDL 1.1	http://schemas.xmlsoap.org/wsdl
ds	XML Signature 1.0	http://www.w3.org/2000/09/xmldsig#
xsd	XML Schema 1.0	http://www.w3.org/2001/XMLSchema
wsse	WS-Security 1.0	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsu	WS-Security 1.0	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
wsa	WS-Addressing 1.0	http://www.w3.org/2005/08/addressing
wsam	WS-Addressing 1.0 – Metadata	http://www.w3.org/2007/05/addressing/metadata
wsp	Web Services Policy 1.2	http://schemas.xmlsoap.org/ws/2004/09/policy
sp	Security Policy 1.1	http://schemas.xmlsoap.org/ws/2005/07/securitypolicy

7.3 Karaktercodering en karakterset

De ondersteunde karaktercodering is UTF-8. De ondersteunde karakterset is ISO-8859-1.

7.4 Datum en tijd

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

7.5 Gebruikte standaarden

Voor deze standaarden worden dezelfde keuzes gemaakt als voor de Digikoppeling-standaard WUS 2.0 versie 1.2 die van toepassing is op de Nederlandse overheid. Zie https://www.logius.nl/diensten/digikoppeling/.

Overheidsstandaarden:

- PKI overheid 1.1

WS-I standaarden:

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

W3C standaard:

- MTOM 1.0