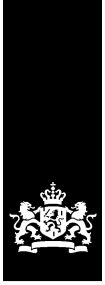


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakbeschrijving Digipoort
Webservices Overheden – Digikoppeling ebMS

Koppelvlakversie 1.2

Versie	1.0
Datum	10 juli 2012
Status	Definitief

Colofon

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

Inhoud

Inleiding

Doel en doelgroep
Dit document beschrijft de afspraken met betrekking tot het elektronische berichtenverkeer bij de overheid via Digipoort.

Dit document is bestemd voor ontwikkelaars van programmatuur ten behoeve van elektronisch berichtenverkeer tussen Digipoort en overheid via versie 1.2 van het koppelvlak dat is ingericht conform Digikoppeling ebMS 2. Het kan hierbij gaan om het afleveren van berichten van Digipoort aan een overheid, het aanleveren van berichten van een overheid aan Digipoort en het verstrekken van statusinformatie door een overheid.

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

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

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

Status
Dit document beschrijft de afspraken met betrekking tot het Digikoppeling ebMS 2.0 koppelvlak van Digipoort. De verwachting is dat de gebruikte open standaarden zich de komende jaren verder zullen ontwikkelen en dat de communicatiebehoefte ook aan verandering onderhevig zal zijn. Het gevolg hiervan is dat de komende jaren nieuwe releases van Digipoort in gebruik zullen worden genomen. Dat kan gevolgen hebben voor het koppelvlak. Logius streeft ernaar om nieuwe releases in nauw overleg met de markt te realiseren. Om het voor marktpartijen snel en eenvoudig mogelijk te maken om gebruik te maken van Digipoort, is er voor gekozen zoveel mogelijk open standaarden en bestaande voorzieningen te gebruiken. Voorbeelden daarvan zijn het gebruik van het SOAP-protocol en de toepassing van PKIOverheid-certificaten.

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

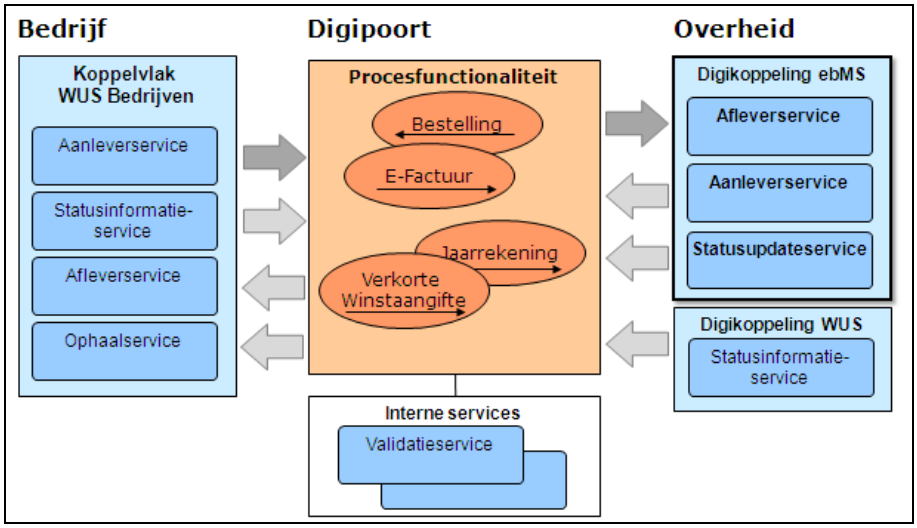
1 Berichtenverkeer

1.1 Inleiding

Digipoort biedt verschillende koppelvlakken voor bedrijven enerzijds en overheden anderzijds, waaronder FTP, SOAP, WUS en ebMS. Via deze koppelvlakken worden diverse berichtstromen van en naar de overheid mogelijk gemaakt, zoals ziekmeldingen, statistiekberichten, facturen, bestellingen, etc. Het koppelvlak 'Digikoppeling ebMS 2.0' is bedoeld voor betrouwbaar berichtenverkeer ('meldingen') tussen Digipoort en overheid en vice versa (voor 'bevragingen' maken overheden gebruik van het 'Digikoppeling WUS 2.0'-koppelvlak).

Ieder Digipoort-koppelvlak biedt meerdere services. Afhankelijk van het koppelvlak kan zo'n service door bedrijven worden gebruikt of door overheden. Digipoort biedt daarnaast 'interne' services die ondersteunend zijn bij de uitvoering van de verwerkingsprocessen, zoals een validatieservice.

In onderstaande afbeelding zijn de services die beschikbaar zijn voor bedrijven enerzijds en overheden anderzijds schematisch weergegeven.



Figuur 1: overzicht Digipoort-services voor bedrijven en overheden (koppelvlak 1.2)

Deze koppelvlakbeschrijving vormt de basis voor de services die Digipoort biedt aan overheden conform het koppelvlak 'ebMS Digikoppeling 2.0' . Het gaat hier om drie services: Afleverservice, Aanleverservice en Statusupdate-service.

De services zijn ingericht conform de 'Digikoppeling 2.0 Koppelvlak-standaard ebMS'[1], die de logistiek van asynchroon berichtenverkeer tussen overheden beschrijft (zie voor meer informatie paragraaf 1.2). Dit

1 Voor meer informatie over deze koppelvlakstandaard, zie www.logius.nl/producten/gegevensuitwisseling/digikoppeling/documentatie/koppelvlakken

document is een toelichting op de toepassing van deze standaard binnen Digipoort.

Overheden kunnen naast bovengenoemde services ook gebruik maken van een Statusinformatieservice. Deze maakt geen onderdeel uit van het ebMS-koppelvlak, maar is ingericht conform Digikoppeling WUS. In het geval van de Statusinformatieservice gaat het namelijk om synchroon berichtenverkeer ("bevraging").

De servicespecificaties voor alle genoemde services worden gepubliceerd onder Digipoort en zijn terug te vinden in het Digikoppeling Service Register. De details van de verschillende services zijn beschreven in afzonderlijke documenten: de Servicebeschrijvingen.

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

1.2 Berichtenverkeer op basis van ebMS

De Koppelvlakstandaard ebMS wordt gebruikt voor asynchroon berichtenverkeer tussen overheden. Het betreft hier berichten waarop vaak niet direct een respons kan worden gegeven, omdat hiervoor aan de kant van de ontvanger een proces moet worden doorlopen waarvan de doorlooptijd op voorhand niet bekend is. Bij dergelijk berichtenverkeer is het wel van belang dat de verzender de zekerheid krijgt dat het bericht is aangekomen bij de beoogde ontvanger. Deze 'reliability' is een standaardonderdeel van het ebMS-protocol waarmee wordt gegarandeerd dat een ontvanger een bericht '*once-and-once-only'* ontvangt. De ontvangende partij stuurt een ontvangstbevestiging ('acknowledgement message') naar de verzender indien het bericht door de ebMS-adapter is ontvangen.

Het ebMS-koppelvlak voorziet onder meer in een 'contract' tussen de twee partijen die onderling elektronische berichten willen uitwisselen (in dit geval Digipoort en de overheidsdeelnemer). In dit contract, de zogenoemde 'Collaboration Protocol Agreement' (CPA), zijn zaken als berichttypen, wijze van uitwisseling en beveiliging vastgelegd. Voor iedere service moet een aparte CPA worden gemaakt en opgenomen in de ebMS-adapter van beide partijen. Meer details hierover zijn te vinden in de afzonderlijke Servicebeschrijvingen, in het document *Koppelvlakstandaard ebMS voor Digikoppeling 2.0* en in Bijlage 1.

De Koppelvlakstandaard ebMS stelt onder meer uitdrukkelijke eisen aan de beveiliging van het berichtenverkeer. In de volgende paragrafen wordt kort beschreven hoe deze voor Digipoort is ingericht.

1.3 Beveiliging

1.3.1 Transportniveau

De authenticiteit van systemen in Digipoort en van de gebruikers van een service moet door alle deelnemende partijen vastgesteld kunnen worden voordat een datacommunicatiesessie wordt gestart. De authenticiteit van systemen wordt middels PKIoverheid-certificaten gecontroleerd[2]. Deze certificaten worden gebruikt bij het opzetten van een beveiligde verbinding tussen de systemen van de communicerende partijen volgens

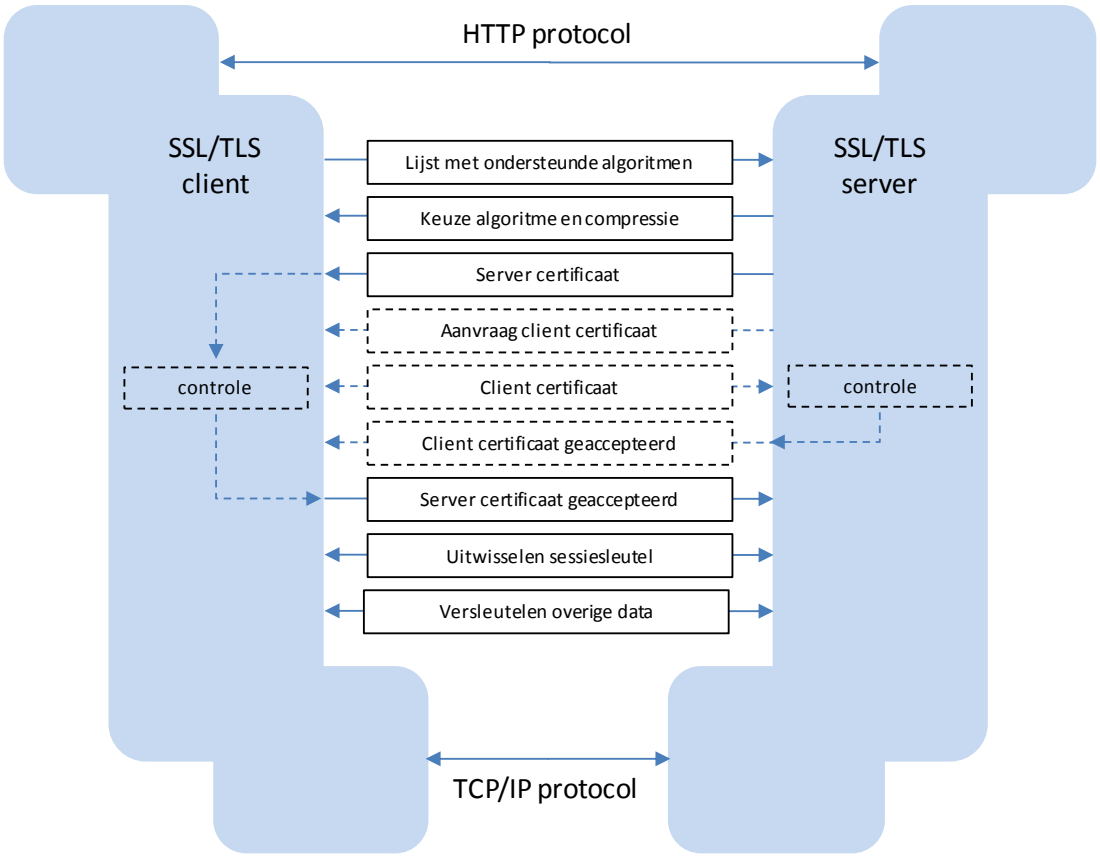
2 Voor testomgevingen *worden Logius-testcertificaten of PKItrial-certificaten gebruikt.*

het zogenoemde TLS/SSL-protocol. Wederzijdse authenticatie vindt plaats door de afzonderlijke certificaten, die door de communicatiepartners worden aangeboden, te verifiëren tegen een lijst van vertrouwde certificaten. Na succesvolle authenticatie wordt met behulp van de certificaten een versleutelde verbinding geopend.

De wijze waarop TLS/SSL-verbinding tot stand komt, wordt schematisch weergegeven in figuur 2.

De wederzijdse endpoints, via welke de beveiligde verbinding tot stand komt, zijn opgenomen in de CPA.

Merk op dat voor berichtenverkeer (ebMS en WUS) gebruik wordt gemaakt van het HTTPS-protocol. De poort die hiervoor standaard wordt gebruikt, is poort 443. Dit is de enige poort waarmee met Digipoort verbinding kan worden gemaakt en tevens de enige poort waarmee Digipoort communiceert.



Figuur 2 TLS/SSL-communicatie

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

De identiteit van overheden die gebruik maken van het ebMS-koppelvlak van Digipoort bepaald aan de hand van het OIN (OverheidsIdentificatie-Nummer), dat is opgenomen in het PKIoverheid-certificaat waarmee de overheid zich authenticeert. Door dit OIN wordt een overheidsorganisatie uniek geïdentificeerd.

Het Koppelvlak gaat er van uit dat het identificerend nummer van de partij waarmee wordt gecommuniceerd (OIN), is opgenomen in de gebruikte certificaten, en wel in het veld 'subject.serialnumber'.

Op transportniveau is de partij die wordt geauthenticeerd de partij waarmee de TLS-verbinding tot stand wordt gebracht. Dit kan ook een gemeenschappelijke serviceorganisatie zijn die voor een of meerdere overheden de verbinding met Digipoort verzorgt. Op transportniveau is het dus niet noodzakelijkerwijs de 'eigenaar' dan wel 'belanghebbende' van de berichten (de overheid namens wie de offerteaanvraag e.d. wordt verstuurd) wiens identiteit wordt gecontroleerd.

Certificaatinformatie wordt in de regel opgenomen in de CPA.

1.3.2 Berichtniveau

Afhankelijk van het geselecteerde Digikoppeling-profiel wordt ook op berichtniveau beveiliging toegepast. Is dat het geval, dan wordt beveiliging toegepast door middel van digitale ondertekening (en mogelijk encryptie) van het bericht conform de 'XML-Signature'-standaard[3]. 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 (PKIoverheid voor productieberichten, testcertificaat voor niet-productieberichten). 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 ondertekeninginformatie met het bericht bewaard.

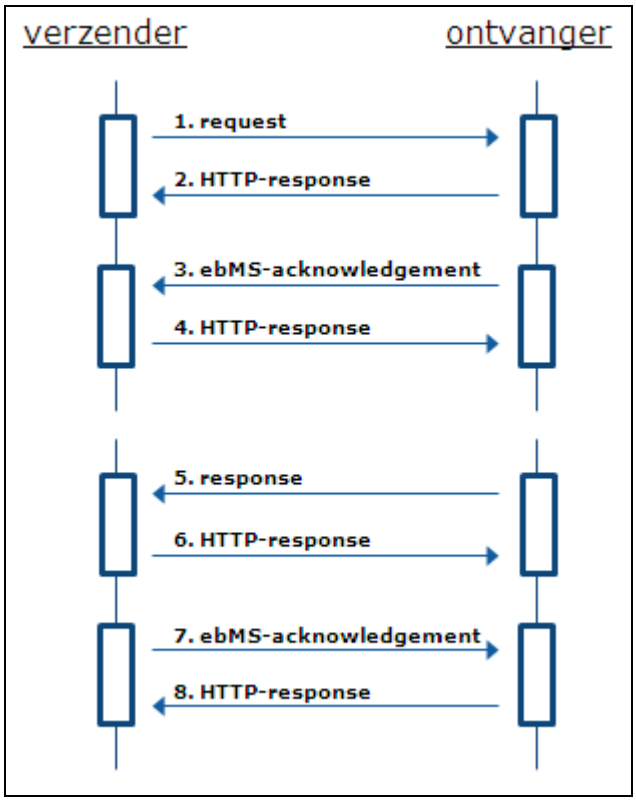
3 Ook bekend onder de naam XMLDsig, XML-Dsig en XML-sig.

2 Sessieverloop

Een sessie tussen communicatiepartners wordt in ebMS-termen een 'conversatie' genoemd. In dit hoofdstuk wordt beschreven hoe zo'n ebMS-conversatie eruit ziet.

2.1 Overzicht ebMS-conversatie

Een ebMS-converstatie wordt geïnitieerd door een partij die we hier 'verzender' noemen. De verzender maakt een TLS/SSL-verbinding met een webservice van de ontvangende communicatiepartner. Over deze verbinding worden SOAP-requestberichten verzonden die zijn opgemaakt conform de ebMS-berichtspecificatie (zie hoofdstuk 3 voor meer informatie over de opbouw van het SOAP-bericht). Voor de duidelijkheid zullen we deze berichten 'ebMS-berichten' noemen.



Figuur 3: overzicht ebMS-conversatie ('happy flow')

Figuur 3 toont een voorbeeld van een ebMS-conversatie. In de figuur is te zien dat een conversatie wordt opgebouwd uit een aantal achtereenvolgende http-sessies (stappen 1, 3, 5 en 7 vormen steeds de start van een separate http-sessie). In essentie wordt hier het asynchrone karakter van een ebMS-conversatie geïllustreerd.

De verzender stuurt een request-bericht (verzoek) naar de ontvangende software, die hierop reageert met de passende http response (bij succesvolle communicatie wordt een 'status 200' teruggegeven).

Indien het bericht correct door de ontvangende ebMS-adapter is ontvangen (het bericht voldoet dan aan de afspraken zoals die in de CPA zijn vastgelegd), wordt een 'acknowledgement'-bericht teruggestuurd ('reliable messaging'). Hiertoe start de ontvanger een nieuwe http-sessie. Wanneer een bericht *niet* door de ebMS-adapter kan worden geaccepteerd, wordt een error-bericht teruggestuurd.

> In het geval dat noch acknowledgement noch error wordt ontvangen, moet de verzender ervan uitgaan dat het bericht de ontvanger niet heeft bereikt. Het ebMS-protocol voorziet in dit geval in een 'retry schema', waarbij binnen een vastgestelde periode een vast aantal malen wordt geprobeerd om het bericht alsnog afgeleverd te krijgen.

Het sturen van een acknowledgement betekent niet dat het bericht daarmee ook door de achterliggende software correct verwerkt is of correct verwerkt kan worden. Om ook informatie over verdere verwerking terug te geven, kan de ontvanger een apart 'response-bericht' sturen (stap 5 t/m 8 in figuur 3). Alle op Digipoort beschikbare ebMS-services bieden de mogelijkheid om zo'n functioneel response-bericht in de conversatie op te nemen.

ebMS-adapters en response-berichten

In de praktijk is gebleken dat niet alle ebMS-adapters die in de markt worden aangeboden, effectief kunnen omgaan met response-berichten. De afleverservice, via welke berichten vanuit Digipoort worden aangeboden, kent daarom ook de mogelijkheid om de conversatie af te sluiten zonder expliciet response-bericht. De ontvanger beëindigt in dit geval de conversatie met het acknowledgement-bericht (indien het bericht correct is ontvangen).

Op berichten die via ebMS op Digipoort worden *aangeleverd*, wordt altijd een response-bericht teruggegeven. De response volgt na interne validatie van het bericht. Als het bericht niet voldoet aan de berichtspecificatie wordt er een foutmelding teruggestuurd. Als het bericht wel voldoet aan de eisen, dan wordt het verder verwerkt. Ook in het geval dat de verwerking niet correct kan worden uitgevoerd, wordt er een foutmelding teruggestuurd. Indien de verwerking succesvol verlopen is, wordt er een responsebericht teruggestuurd.

Of op berichten die door Digipoort worden *afgeleverd* een response wordt gegegeven (afgezien van acknowledgement of ebMS-error) hangt mede af van de mogelijkheid die de ebMS-adapter daartoe biedt (zie kader).

2.1.1 Status verwerkingsproces

In Digipoort wordt de status bijgehouden van het proces waarbinnen een bericht wordt verwerkt. Een proces zal alleen status 'succesvol' krijgen indien het bericht succesvol is afgeleverd bij de beoogde ontvanger. Digipoort moet hiertoe een bevestiging hebben gekregen vanuit de ontvanger (positive afleverResponse of, indien de ontvanger een dergelijk bericht niet teruggeeft, een acknowledgement-bericht).

De status is door de aanleverende partij op te vragen middels de Statusinformatieservice.

2.2 Service-taken

Elke service voert tenminste de volgende taken uit:

- Controleren verzoek
- Ontvangen verzoek
- Verzenden antwoord

Naast bovengenoemde onderdelen kunnen per service andere onderdelen zijn opgenomen. Deze zijn uitgewerkt in de Servicebeschrijving behorend bij de service.

2.2.1 Controleren verzoek

Elk verzoek dat bij Digipoort binnenkomt, wordt eerst door Digipoort gevalideerd. Hierbij wordt gekeken of het bericht voldoet aan de koppelvlakspecificaties (o.a. berichtgrootte, ondertekening – indien van toepassing - en berichtstructuur worden gevalideerd).

Om ebMS-berichten aan Digipoort aan te kunnen bieden of wanneer Digipoort ebMS-berichten naar de overheidsdeelnemer verstuurt, wordt gebruik gemaakt van een 'verzoek' met een voorgedefinieerde structuur. Deze structuur is vastgelegd in een XML Schema (XSD). Bij de beschrijving van elke service zijn de relevante XSD's bijgevoegd[4].

Nadat een verzoek (in de vorm van een ebMS-bericht) bij Digipoort aangekomen, worden de volgende zaken gecontroleerd:

Controle	**Toelichting**
Is een element aanwezig?	Hierbij wordt gecontroleerd of alle verplichte elementen zoals beschreven in de XSD voorkomen in het verzoek.
Is er geen onbekend element aanwezig?	Hierbij wordt gecontroleerd of in het verzoek geen elementen voorkomen, die niet in de XSD 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 XSD.

4 Merk op dat deze XSD niet het inhoudelijke bericht (de 'functionele gegevens' die middels het bericht worden verstuurd) specificeert. Deze wordt in een aparte specificatie, vaak ook een XSD, beschreven.

2.2.2 Ontvangen verzoek

Wanneer het verzoek door Digipoort is gecontroleerd en correct bevonden, kan het daadwerkelijk worden 'ontvangen' en verder verwerkt. Aan het verzoek wordt door Digipoort een uniek kenmerk toegekend.

Elk correct verzoek aan een service van Digipoort wordt vastgelegd in de berichtenadministratie. De berichtenadministratie fungeert binnen Digipoort als audit trail. Op dezelfde wijze kan een overheidsdeelnemer verzoeken van Digipoort vastleggen in een eigen berichtenadministratie.

2.2.3 Versturen antwoord

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

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

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

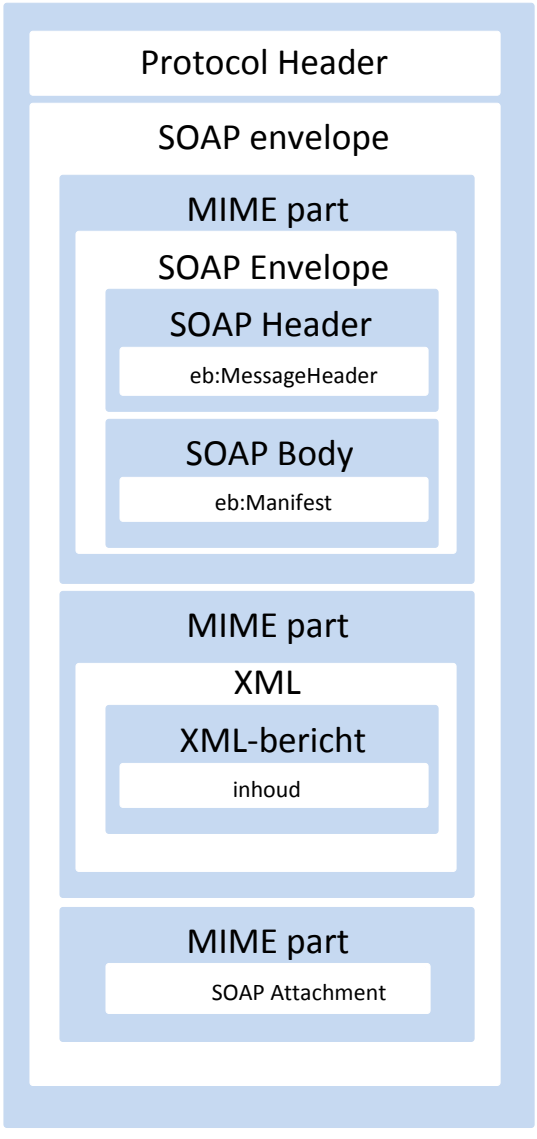
Indien voor verzending van het verzoek gebruik is gemaakt van berichtbeveiliging, zal ook het antwoord volgens de standaard 'XML Signature' ondertekend zijn. Zie voor meer informatie hoofdstuk 4.

3 SOAP-bericht (ebMS)

Het ebMS-koppelvlak 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. In het geval van ebMS wordt daarbij gebruik gemaakt van bepaalde uitbreidingen op SOAP (*SOAP extensions*) waardoor het SOAP-bericht er wat anders uitziet dan in het geval van bijvoorbeeld een WUS-implementatie. De verschillen worden hieronder in meer detail uitgeengezet.

3.1 Structuur van een SOAP-bericht onder ebMS

In onderstaande figuur wordt de opbouw van een SOAP-bericht getoond zoals dat eruit kan zien in geval van ebMS-berichtenverkeer:



Figuur 4: opbouw SOAP-bericht onder ebMS

Het bericht is opgebouwd uit:

- De transportprotocol-header (HTTP); ebMS stelt specifieke eisen aan de op te nemen HTTP-headers. Zie voor meer informatie *Koppelvlakstandaard ebMS voor Digikoppeling 2.0* en de ebMS 2.0 specificatie[5].

- De SOAP envelope in een MIME part[6] met daarbinnen:
  - de SOAP header (bevat ook de ebMS headers (MessageHeader): meta-informatie met betrekking tot *transport/routering* van het bericht, zoals de identificatie van de verzendende en ontvangende partij, en het unieke conversatie-ID van het bericht);
  - de SOAP body (bevat de verwijzing naar de feitelijke inhoud (*payload*) van het bericht). In het geval van een 'SOAP fault' bevat de body de foutdetails. In het geval van een 'acknowledgement' (ebMS-ontvangstbevestiging) is de SOAP body leeg.

- Optioneel: een MIME part met daarin[7]:
  - XML-bericht (*payload*); zie paragraaf 3.3 voor details.

- Optioneel: een of meer MIME parts met daarin:
  - berichtbijlage (*payload/attachment*) (afhankelijk van de dienst/berichtsoort).

3.1.1 Header-elementen (ebMS)

Er wordt gebruik gemaakt van standaard ebMS headers zoals deze zijn gespecificeerd in de Digikoppeling Koppelvlakstandaard ebMS.

Afhankelijk van het gekozen profiel (zie 4.1) kan de header bijvoorbeeld ook *Digital Signature* gegevens bevatten (zie Hoofdstuk 4 voor details).

3.1.2 Payload: request- en response-berichten

Request- en response-berichten bevatten een aparte MIME part waarin de zogenoemde payload is opgenomen. De payload is een XML-document dat de inhoudelijke informatie bevat die via het SOAP-bericht wordt verzonden. In het geval van een ebMS-bericht is dit XML-document opgebouwd uit een aantal vaste elementen, waaronder de aanduiding van de berichtsoort, de verzendende partij, de ontvangende partij, etc. Het feitelijke inhoudelijke bericht dat wordt verstuurd (bijv. e-factuur, bestelling, rapportage,etc.) is opgenomen onder een apart element. Ook eventuele bijlagen zijn onder een apart element opgenomen.

De elementen waaruit het XML-document is opgebouwd, zijn gespecificeerd in een XML Schema (XSD). Deze XSD is opgenomen in de koppelvlakdocumentatie.

---

5 OASIS: ebXML Message Service Specification Version 2.0 (1 April 2002); Appendix B.2.

6 SOAP-berichten zijn onder ebMS opgebouwd volgens de 'SOAP Messages with Attachments'-specificatie, en bestaan derhalve uit meerdere 'parts' in een enkele ' SOAP message package'.

7 'SOAP fault'-berichten en ebMS acknowledgements bevatten geen payload.

Het inhoudelijke bericht dat is opgenomen in het XML-document zal in de regel zelf ook weer een XML-document zijn, dat gecodeerd (Base64 encoded) in het bovenliggende document is opgenomen.

De koppelvlakdocumentatie bevat voorbeeldberichten waarin bovenstaande structuur wordt geïllustreerd.

3.1.3 Payload: bijlagen

Bijlagen (bijgevoegde bestanden) kunnen middels een of meer aparte MIME parts worden meegegeven of worden opgenomen in het SOAP-bericht. De response-berichten voor de services onder het Digipoort ebMS-koppelvlak zijn gespecificeerd volgens die laatste optie (bijlagen worden opgenomen in het element 'berichtBijlagen' in het SOAP-bericht).

In beginsel zijn alle bestandsformaten als bijlage mogelijk[8].

De totale grootte van de payload (bericht inclusief bijlagen) is beperkt tot 20 Mb (Base64 encoded).

8 *Ook bijlagen met MIME types behorend bij Microsoft-bestandtypen als .docx, .xlsx, etc.zijn mogelijk. In de 'digipoort-koppelvlak-1.2.xsd is hiertoe de lengte van het element* berichtInhoudType *uitgebreid (van oorspronkelijk 40) naar max.255 karakters.*

4 Berichtbeveiliging

4.1 Profielen

Het ebMS-koppelvlak biedt een drietal verschillende beveilingsprofielen. Het gaat hierbij om beveiliging op berichtniveau. Op transportniveau is beveiliging voor alle profielen ingericht op basis van dubbelzijdig TLS/SSL (zie hoofdstuk 1.3.1).

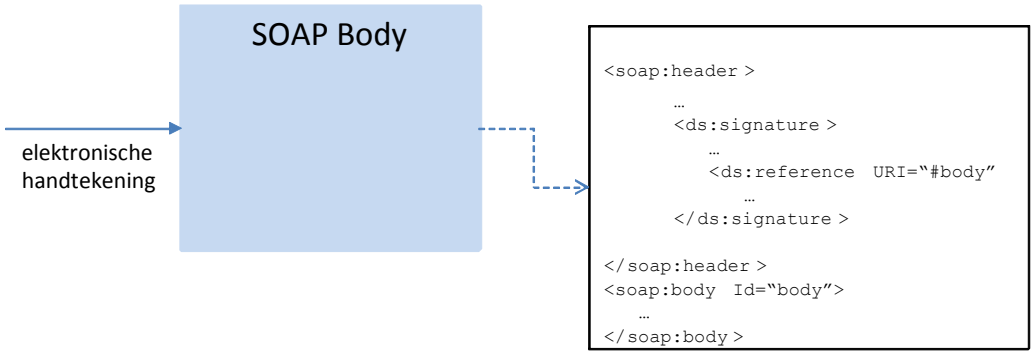
De profielen zijn:

- Digitale ondertekening van het bericht (profiel osb-rm-s);
- Versleuteling (encryptie) van het bericht (profiel osb-rm-s);
- Geen ondertekening of versleuteling (osb-rm).

Het profiel komt terug in de CPA en is gespecificeerd in de ebMS Service Specificatie (ESS) die voor het genereren van de CPA kan worden gebruikt (zie Bijlage 1 voor meer informatie).

Indien een profiel wordt gebruikt waarbij ebMS-berichten ondertekend moeten worden, moet dit gebeuren conform de 'XML Signature'-standaard. Het ondertekenen moet geschieden middels een door een CSP uitgegeven PKIoverheid-certificaat[9]. Het certificaat (publieke sleutel), de handtekening en de gebruikte algoritmes dienen in de bericht-header opgenomen te worden.

Voorbeeld:



Figuur 5 Handtekening volgens XML Signature

XML Signature levert het volgende:

- De mogelijkheid op het controleren van de integriteit van het bericht;
- De garantie van de identiteit van de verzender van het bericht;
- De garantie op het in het ebMS-bericht opgenomen tijdstempel; Dit tijdstempel geeft aan wanneer een bericht is ontvangen bij Digipoort. Hiermee kan ook onder meer worden voorkomen dat er aanvallen worden uitgevoerd op Digipoort.

9 In de preproductieomgeving kunnen ook voor ondertekening testcertificaten *worden gebruikt.*

4.2 Tekenen van het bericht

In geval van ondertekening moeten de volgende berichtonderdelen worden ondertekend:

- header-onderdeel Timestamp
- soap-env:Body
- payload (inhoudelijk bericht) inclusief eventuele bijlagen

NB: ook de ebMS-bevestiging van het bericht ('acknowledgement') moet worden ondertekend (dezelfde onderdelen als hierboven genoemd, voor zover relevant).

De volgende eisen gelden ten aanzien van het gebruik van XML Signature:

http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

Stap 1: Canonicalization
http://www.w3.org/TR/2001/REC-xml-c14n-20010315

Stap 2: Digest
http://www.w3.org/2000/09/xmldsig#sha1

Stap 3: Signature
http://www.w3.org/2000/09/xmldsig#rsa-sha1

5 Algemene afspraken

5.1 Communicatiestandaarden

De communicatie tussen Digipoort en aangesloten overheidspartij verloopt conform de afspraken zoals die zijn vastgelegd in de 'Digikoppeling ebMS 2.0'-koppelvlakstandaard.

Zie het document *Koppelvlakstandaard ebMS voor Digikoppeling 2.0* voor meer informatie.

5.2 Prefixen

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

Prefix	Specificatie	Namespace URI
tns	digipoort-koppelvlak-1.2.xsd	http://logius.nl/digipoort/koppelvlakservices/1.2/
soapenv	SOAP 1.1	http://schemas.xmlsoap.org/soap/envelope/
eb	ebXML SOAP Envelope extensions	http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
ds	XML Signature 1.0	http://www.w3.org/2000/09/xmldsig#
xsd	XML Schema 1.0	http://www.w3.org/2001/XMLSchema

5.3 Karaktercodering en karakterset

De ondersteunde karakterset is UTF-8.

5.4 Datum en tijd

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

5.5 Gebruikte standaarden

Overheidsstandaarden:

- Digikoppeling ebMS 2.0
- PKI overheid 1.1

ebXML-standaarden

- ebXML Messaging Service (ebMS) 2.0

Bijlage 1: CPA genereren

Het ebMS-koppelvlak voorziet onder meer in een 'contract' tussen de twee partijen die onderling elektronische berichten willen uitwisselen (in dit geval Digipoort en de overheidsdeelnemer). In dit contract, de zogenoemde 'Collaboration Protocol Agreement' (CPA), zijn zaken als berichttypen, wijze van uitwisseling en beveiliging vastgelegd. Voor iedere service moet een aparte CPA worden gemaakt en opgenomen in de ebMS-adapter van beide partijen.

Logius biedt een voorziening waarmee CPA's op relatief eenvoudige wijze kunnen worden gegenereerd. Deze CPA-Creatievoorziening is een webapplicatie, toegankelijk via internet. Het genereren van CPA's is beschreven in de *Aansluithandleiding Digipoort (t.b.v. DigiInkoop en E-Factureren) voor overheden*, die te vinden is op de Logius-website.

De Creatievoorziening maakt gebruik van twee specifieke XML-bestanden waarin de gegevens van de respectievelijke partners zijn opgenomen. De *ebMS Service Specificatie* (ESS) bevat de gegevens van de partij die de servicegegevens publiceert (ook *service provider* genoemd). Voor iedere variant van alle ebMS-services die onder Digipoort wordt aangeboden, is een ESS beschikbaar. Deze ESS-bestanden zijn gepubliceerd in het Digikoppeling Service Register onder de betreffende ebMS-service en een overzicht van deze bestanden (inclusief de ID's die moeten worden ingevoerd in de CPA-Creatievoorziening) is opgenomen in de koppelvlakdocumentatie (Servicebeschrijvingen, zie Bijlage aldaar).

De gegevens van de andere partij moeten worden opgenomen in de *ebMS Consumer Specificatie (*ECS). Deze ECS moet door de overheidsorganisatie zelf worden gecreëerd op basis van de parameters die in de ESS zijn gespecificeerd. In bovengenoemde Aansluithandleiding wordt een gedetailleerd voorbeeld van een ECS gegeven.

De ESS is door de service provider opgenomen in de CPA-Creatievoorziening. Door in deze voorziening de bijbehorende ECS te uploaden, kan een CPA worden gegenereerd waarin de gegevens uit zowel ESS als ECS worden opgenomen.