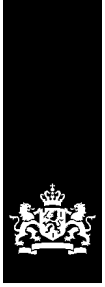


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakstandaard ebMS
Digikoppeling 2.0

Versie 2.5

Datum 09/06/2014
Status Definitief

Colofon

Logius Servicecentrum:
Postbus 96810
2509 JE Den Haag

t. 0900 555 4555 (10 ct p/m)
e. servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
22/11/2011	2.4	Logius	-
09/06/2014	2.5	Logius	Redactionele wijzigingen

Inhoud

1 Inleiding

1.1 Doel en doelgroep

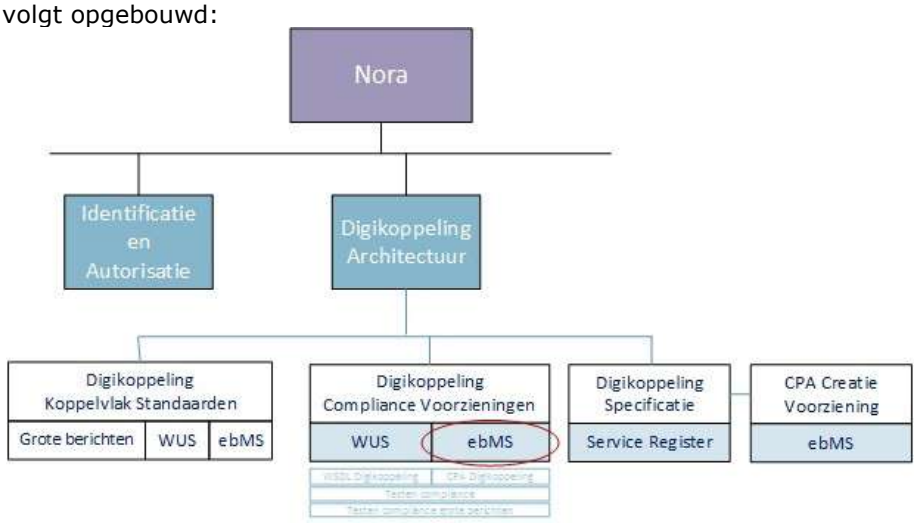
Dit document beschrijft de functionele specificaties voor Digikoppeling ebMS Deployment Profile, onderdeel van Digikoppeling 2.0.

Het document is bestemd voor architecten en ontwikkelaars die op basis van ebMS gegeven willen uitwisselen via Digikoppeling. Zie onderstaande tabel bij welke taken dit document ondersteunt. Alle Digikoppeling webservices die op ebMS gebaseerd zijn, moeten conformeren aan de koppelvlakstandaard ebMS. Deze wordt tot in detail in dit document gespecificeerd. Het doel van dit document is ontwikkelaars te informeren wat deze koppelvlakstandaard nu precies inhoudt en waar zij zich aan moeten conformeren. Het gaat hierbij om zowel service aanbieders als service afnemers.

Afkorting	Rol	Taak	Doelgroep?
[MT]	Management	Bevoegdheid om namens organisatie (strategische) besluiten te nemen.	**Nee**
[PL]	Projectleiding	Verzorgen van de aansturing van projecten.	**Nee**
[A&D]	Analyseren & ontwerpen (design)	Analyseren en ontwerpen van oplossings-richtingen. Het verbinden van Business aan de IT.	**Ja**
[OT&B]	Ontwikkelen, testen en beheer	Ontwikkelt, bouwt en configureert de techniek conform specificaties. Zorgen voor beheer na ingebruikname.	**Ja**

1.2 Opbouw Digikoppeling documentatie

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



Figuur 1: Opbouw documentatie Digikoppeling

1.3 Doel en scope van Digikoppeling

Digikoppeling biedt de mogelijkheid om op een sterk gestandaardiseerde wijze berichten uit te wisselen tussen service aanbieders en service afnemers. De uitwisseling tussen partijen wordt in drie lagen opgedeeld:

- Inhoud: Op deze laag worden de afspraken gemaakt de inhoud van het uit te wisselen bericht, dus de structuur, semantiek en waardebereiken. 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 Digikoppeling-laag.**
- Transport: deze laag verzorgt het daadwerkelijke transport van het bericht.

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

1.3.1 Leidend principe

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.

De architectuur voor toepassing van Digikoppeling versie 2.0 is beschreven in het document "Digikoppeling_2.0_Architectuur_vx.x"[1] en voor Digikoppeling versie 3.0 "Digikoppeling_3.0_Architectuur_vx.x".

1.4 Koppelvlak & koppelvlakstandaard

Een koppelvlak is een interface die volgens vergaande standaards de gegevensuitwisseling verzorgt. Het werken met vaste standaards 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.

Een van de belangrijkste eisen die door de overheid gesteld wordt 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 standaards, die door "alle" leveranciers interoperabel zijn geïmplementeerd. Een andere eis is dat met name afnemers gebruik kunnen maken van één "stekker" (één logistiek koppelpunt).

1.4.1 Specificatie van de koppelvlakstandaard

De koppelvlakspecificatie beschrijft de eisen waar de adapters aan moeten voldoen om interoperabel met elkaar te kunnen communiceren. Digikoppeling gaat over logistiek, dus over de envelop en niet over de inhoud. De hele set info die tezamen nodig is voor een complete generieke Digikoppeling koppelvlakdefinitie (Raamwerk Specificatie genoemd) bestaat uit:

[1] Met "vx.x" wordt de laatst gepubliceerde versie op de Logius website bedoeld

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

1.5 Opbouw van dit document

Hoofdstuk 1 bevat een aantal algemene inleidende onderwerpen.
Hoofdstuk 2 bevat de kern van de standaard met achtergrond en gebruik van de ebMS Deployment Profile.
Hoofdstukken 3 tot en met 5 beschrijven de parameters van het ebMS profiel zoals dat gekozen is voor Digikoppeling.

Begrippen en afkortingen worden toegelicht in het document “Digikoppeling_3.0_Architectuur_vx.x.pdf”. Deze zit in de Digikoppeling aansluitkit.

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

2 Koppelvlakstandaard ebMS

2.1 Inleiding

Dit document specificeert de Koppelvlakstandaard ebMS voor berichtenuitwisseling over Digikoppeling (voorheen OverheidsServiceBus) als een toepassing van de ISO 15000-2 standaard, de ebXML Message Service Specification versie 2.0 [ISO 15000-2]. Digikoppeling is bedoeld als generieke infrastructuur voor een grote variëteit aan diensten. Deze Standaard is daardoor eveneens generiek en dient nader gespecialiseerd te worden voor specifieke berichtstromen en diensten.

EbXML Messaging [ISO 15000-2] is bedoeld voor verschillende toepassingen en faciliteert die diversiteit door een scala aan configureerbare features en opties te bieden. Elk gebruik van ebXML Messaging in een bepaalde keten of binnen een bepaalde gemeenschap vereist in de praktijk een bepaalde mate van aanvullende standaardisatie. Aangezien veel van de configuratiefeatures in de standaard optioneel zijn, moet precies gedocumenteerd worden welke onderdelen ervan op welke manier toegepast zijn, om op de verschillende relevante niveaus interoperabiliteit te realiseren. Die informatie is hier verzameld en gepubliceerd als configuratiegids voor de gebruikers van Digikoppeling. Het legt de overeengekomen conventies vast voor het gebruik van ebXML message service handlers, de functionaliteit die van een implementatie verwacht wordt en de details voor het gebruik van de standaard.

Een deployment specificatie is niet hetzelfde als een ebXML samenwerkingsprotocol overeenkomst (ook wel aangeduid met een “Collaboration Protocol Profile and Agreement) [ISO 15000-1]. Wel hebben sommige onderdelen van een deployment specificatie gevolgen voor de specifieke invulling van CPA elementen.

2.2 Terminologie in dit document

Dit document biedt organisaties die gebruik gaan maken van Digikoppeling de basis voor de configuratie van de ebXML Messaging software. Een correcte configuratie is van belang voor het uitwisselen van berichten. Mocht er voor een bepaald onderdeel geen specifieke richtlijn gegeven zijn, dan wordt dit aangegeven met één van de volgende waardes:

- Not Applicable. Dit is voor onderdelen die niet relevant zijn voor Digikoppeling, of voor mogelijkheden die niet gebruikt worden.
- No Recommendation: geeft aan dat er geen wijziging of voorkeur voor een bepaalde invulling van het onderdeel is op het algemene niveau waar dit document zich op richt. Specifieke toepassingen van deze specificatie (voor specifieke berichtstromen) zullen hier in sommige gevallen wel nog aanvullende eisen voor stellen.
- Pending: voor onderdelen die nog nader onderzocht worden en mogelijk in toekomstige versies nader uitgewerkt worden.

In de Engelse tekst dienen de woorden “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” te worden geïnterpreteerd.

2.3 Ondersteunde varianten

De ebXML Messaging 2.0-standaard is de basis van deze specificatie. Deze standaard biedt een hogere mate van configureerbaarheid dan in Digikoppeling-praktijk wenselijk is. Om redenen van interoperabiliteit, eenvoud en overzichtelijkheid onderscheidt deze koppelvlakstandaard een drietal varianten van uitwisselingen. Elke variant veronderstelt bepaalde voorgedefinieerde keuzen voor parameters als synchroniciteit, beveiliging en betrouwbaarheid en is daarmee een “profiel” voor ebXML Messaging.

Elke uitwisseling op basis van het ebXML Messaging versie 2.0 protocol over Digikoppeling 2.0 zal moeten voldoen aan één van de volgende Digikoppeling ebMS profielen:

- Best Effort: dit zijn asynchrone 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.
- Reliable Messaging: asynchrone uitwisseling met ontvangst bevestigingen en duplicaateliminatie door de ontvangende message handler. Dit profiel is onder meer geschikt voor alle berichtenstromen die leiden tot updates van gegevensverzamelingen.
- End-to-End Security: op basis van Reliable Messaging of Best Effort 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 Consumer organisatie, 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 gebruik gemaakt van XML digitale handtekening [XMLDSIG] en XML versleuteling [XML Encryption], conform ebMS 2.0.

NB. De versies Digikoppeling 1.0 en Digikoppeling 1.1 ondersteunen alleen Best Effort en 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 ondersteunen 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 wordt dus ook verplicht verklaard op Digikoppeling 2.0 versie.)
  - Voor End-to-End Security, door middel van signing (ondertekening) en (optioneel) encryptie (versleuteling) op bericht-niveau (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 berichtenuitwisseling is asynchroon: een business request wordt in een eigen synchrone HTTP request/response sessie verzonden, terwijl

de acknowledgements en optionele business responses via een separaat HTTP request/response sessie verzonden worden.

De onderstaande tabel geeft in essentie de eigenschappen van de verschillende Digikoppeling 2.0 profielen weer. Ten behoeve van de CPA creatievoorziening is de kolom 'CPA Creation' toegevoegd. Voor alle profielen wordt twee-zijdig TLS gebruikt op transport nivo (HTTPS).

Profile Names			**Transport characteristics**				
Digikoppeling 2.0 ebMS		**CPA Creation**	**2-zijdig TLS**	**Reliable**	**Signed**	**Encrypted**	**Attachments**
Best Effort		**osb-be**	√	n.a.	–	–	**Optional**
Reliable Messaging		**osb-rm**	√	√	–	–	**Optional**
End-to-End Security.	**Best Effort – Signed**	**osb-be-s**	√	n.a.	√	–	**Optional**
	Reliable – Signed	**osb-rm-s**	√	√	√	–	**Optional**
	Best Effort – Encrypted	**osb-be-e**	√	n.a.	√	√	**Optional**
	Reliable – Encrypted	**osb-rm-e**	√	√	√	√	**Optional**

n.a. = Not Applicable.

Met betrekking tot CPA creatie: zie hoofdstuk 5.1 Deployment and processing and requirements for CPAs.
Om een goed overzicht te verschaffen wordt de onderstaande tabel gegeven waarin alleen Digikoppeling 1.0 en Digikoppeling 1.1 profielen aangegeven zijn.

Profile Names		**Transport characteristics**				
Digikoppeling 1.0 & Digikoppeling 1.1	**CPA Creation**	**2-zijdig TLS**	**Reliable**	**Signed**	**Encrypted**	**Attachments**
Best Effort	**osb-be**	√	n.a.	–	–	–
Reliable Messaging	**osb-rm**	√	√	–	–	–

n.a. = Not Applicable.

2.4 Berichtuitwisselpatronen

Deze specificatie ondersteunt zowel One Way als Two Way bericht-uitwisselpatronen (message exchange patterns, terminologie ontleend aan [ebMS3]). One Way uitwisselingen ondersteunen bedrijfstransacties voor informatie-verspreiding en notificaties, die geen antwoordbericht veronderstellen. Two Way uitwisselingen ondersteunen bedrijfstransacties

van het type Vraag-Antwoord, Verzoek-Bevestig, Verzoek-Antwoord en Handelstransacties (zie [UMMR10], [UMMUG] voor informatie over het concept bedrijfstransactie patronen). In het geval van tweewegsverkeer leggen de ebXML headervelden (1.1.1 MessageId, RefToMessagId en ConversationId) de relatie tussen request berichten en de corresponderende response berichten vast.

Deze specificatie gebruikt uitsluitend een Push binding aan het HTTPS protocol. Dat wil zeggen dat het retourbericht in een tweewegscommunicatie via een afzonderlijke HTTPS connectie verloopt, die is geïnitieerd vanuit de verzender (=de beantwoorder). Het initiële bericht is dan verzonden in een eerdere HTTPS connectie, die afgesloten is na succesvolle overdracht van het heengaande bericht.

De keuze van het te gebruiken profiel is onafhankelijk van het uitwisselpatroon. Het heengaande bericht en (in een tweewegsuitwisseling) het teruggaande bericht kunnen naar keuze gebruik maken van het Best Effort profiel of het Reliable Messaging profiel.

2.5 Beveiligingsaspecten

Deze specificatie maakt gebruik een aantal standaarden op het gebied van beveiliging en voldoet op het moment van schrijven aan geldende richtlijnen en best practices. Aangezien in de loop der tijd kwetsbaarheden kunnen worden ontdekt in de cryptografische algoritmen waarop deze standaarden zijn gebaseerd, is het van belang dat deze specificatie regelmatig op geldigheid hiervan wordt bezien. De specifieke toegepaste referenties zijn:

- Advanced Encryption Standard 256-cbc [FIPS 197]
- NIST richtlijnen voor sleutelbeheer [NIST-Keys]
- RSA-SHA1 [RFC 2437]
- Transport Level Security 1.0 [RFC 2246]

2.6 Format van dit document

Het OASIS Implementation, Interoperability en Conformance (IIC) Technical Committee (TC) heeft voor deployment specificaties een sjabloon opgesteld [Deployment Guide 1.1]. Dat sjabloon is al eerder toegepast door bepaalde sectoren zoals handel (GS1) en gezondheidszorg (HL7), en wordt daarmee een standaard manier van het beschrijven van configuraties. Dit document is opgesteld aan de hand van dat sjabloon. Het is slechts een summiere beschrijving van het specifieke gebruik van ebXML Messaging en bevat geen achtergrondinformatie, motivatie, voorbeelden en andere informatie die nuttig is voor het in de praktijk toepassen van deze specificatie.

Dit document is direct afgeleid van [Deployment Guide 1.1] en om praktische redenen (grotendeels) in het Engels opgesteld. Leveranciers van producten en diensten rond ebXML Messaging zijn bekend met dit sjabloon doordat het ook in andere sectoren wordt gebruikt. Leveranciers kunnen aan de hand van dit sjabloon eenvoudig nagaan in hoeverre hun product voldoet aan de gestelde eisen.

Dit document is niet (geheel) zelfstandig te lezen maar bedoeld om geraadpleegd te worden samen met de technische specificatie [ISO 15000-2].

3 Profiling the Modules of ebMS 2.0

3.1 Core Modules

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**Core Extension Elements [ebMS 2.0] Section 3**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile>. Profiled: <yes / no>	Support for the Core Extension Elements of ebXML Messaging 2.0 is required.
Notes		

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**Security Module [ebMS 2.0] Section 4.1**	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling Status	Usage: <required / optional / never used	The Security Module is required in this profile. Security profile 3 [ebMS 2.0 Appendix C] must be used: "Sending MSH authenticates and both MSH's negotiate a secure channel to transmit data". The HTTPS connection uses encryption to provide in transit confidentiality of the complete ebXML message		

	in this profile> Profiled: <yes / no>	and performs both certificate-based Client and Server authentication during the TLS handshake.	
			Security profile 8 [ebMS 2.0 Appendix C] must be used: "Sending MSH applies XML/DSIG structures to message and passes in secure communications channel. Sending MSH applies XML/DSIG structures to message and Receiving MSH returns a signed receipt." Security profile 14 [ebMS 2.0 Appendix C] is optional: "Sending MSH applies XML/DSIG structures to message and applies confidentiality structures (XML-Encryption) and Receiving MSH returns a signed receipt".

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**SyncReply Module [ebMS 2.0] Section 4.3**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	SyncReply is never used in these profiles. All messages, including acknowledgments and error messages, are sent asynchronously.
Notes		Asynchronous messaging does not preclude fast response times, as is required to support interactive applications. Asynchronous messaging supports higher levels of scalability and supports scenarios where a response message may be sent minutes, hours or days after the initial request message. Asynchronous messaging may be combined transparently with store-and-forward intermediaries.

3.2 Additional Modules

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**Reliable Messaging Module [ebMS 2.0] Section 6**	**Best Effort**	**Reliable Messaging**	**End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Never used in this profile. Reliable messaging profile 8, Best Effort.	Required in this profile. Reliable Messaging profile 2, Once-And-Only-Once Reliable Messaging at the End-To-End level only based upon end-to-end retransmission.	Optional in this profile. See profile Best Effort or profile Reliable Messaging for details.

Notes		The ebXML reliable messaging protocol is not used. Acknowledgment Messages must not be sent or requested, and the receiver should not eliminate duplicate messages.	In this profile the FromParty MSH (message origination) must request, and the ToParty MSH (message final destination) must send an acknowledgment message. The ToParty MSH must also filter any duplicate messages based on ebXML 1.1.1 MessageId. Any intermediate NextMSH ebXML-aware nodes (see caveat in section 'Multi-Hop Module' in this chapter) have no reliable messaging functionality. Acknowledgment messages must not be consumed by any such intermediary but routed like any ebXML Message back to the original (true) sender.	

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**Message Status Service** **[ebMS 2.0] Section 7**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Optional. Message Status Service is not required in these profiles.
Notes		

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0

Name and Reference	**Ping Service** **[ebMS 2.0] Section 8**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Optional. Ping Service is not required in these profiles.
Notes		

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**Message Order** **[ebMS 2.0] Section 9**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Optional. Message Order is strongly discouraged in these profiles.
Notes		Many organisations use message handlers that do not support this functionality. Therefore it can only be used if communicating parties agree to this option in advance. This specification is limited to message service handler order functionality and does not preclude application-level in-order processing if sequence information is somehow provided at the business document level.

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0

Name and Reference	**Multi-Hop Module** **[ebMS 2.0] Section 10**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Never used in this profile.
Notes	Multi-hop is the process of passing the message through one or more intermediary nodes or MSH's. An Intermediary is any node or MSH where the message is received, but is not the Sending or Receiving MSH endpoint. This node is called an Intermediary.	These profiles use asynchronous communication for business messages, acknowledgments and error messages. This protocol is therefore compatible with asynchronous, transparent, store-and-forward ebXML Messaging (or other SOAP-based) intermediaries. However, this document only specifies functionality between ebXML Message endpoints. (See also caveat in the section 'Reliable Messaging Module' in this chapter.)

3.3 Communication Protocol Bindings

3.3.1 Profile Requirement Item: Transport Protocol

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[EbMS 2.0] Appendix B**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is HTTP a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.)	**Never used** in this profile. HTTPS is used instead.
Profiling (b)	Is HTTPS a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.)	HTTPS is the **required** transport protocol.

Profiling (c)	Is (E)SMTP a required or allowed transfer protocol? (See section B.3 for specifics of this protocol.)	(E)SMTP is **never used** in this profile.
Profiling (d)	If SMTP, What is needed in addition to the ebMS minimum requirements for SMTP?	Not applicable
Profiling (e)	Are any transfer protocols other than HTTP and SMTP allowed or required? If so, describe the protocol binding to be used.	No other protocols are supported.
Alignment		
Test References		
Notes		

4 Profile Requirements Details

4.1 Module: Core Extension Elements

4.1.1 Profile Requirement Item: PartyId

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	[ebMS 2.0] Section 3.1.1.1 PartyId Element Header elements: SOAP:Header/eb:MessageHeader/eb:From/eb:PartyId /SOAP:Header/eb:MessageHeader/eb:To/eb:PartyId	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is a specific standard used for party identification? Provide details. Example - EAN•UCC Global Location Number. Ref.: ISO6523 - ICD0088.	Partners who are going to use ebMS for the first time **must** use an **OIN** (Overheids Identificatie Nummer) for identification. Partners who are already using ebMS and are using other identification schemes are allowed to use their identification: the type attribute must identify their identification scheme and must be different from urn:osb:oin. The use of their own identification should be temporary: the partner should start using OIN at a certain moment for identification using Digikoppeling. For non-production environments a suffix is allowed after the OIN to distinguish it from production (e.g. "_OTA" or "_T"). **OIN** stands for Overheids Identificatie Nummer and is maintained by Logius in the Digikoppeling Serviceregister (DSR). The number is unique and allows identification of partners, even if they are not themselves legal entities, but departments or units of larger organizations. The OIN used for PartyId must be the same as the OIN from the end-party and should not contain the OIN from an

		intermediate party. In case the end-party is the same party that performs TLS, signing and/or encryption the OIN used for PartyId should be identical to the OIN used for the TLS-, signing- and/or encryption-certificate respectively. Hence if the end-party does not perform TLS, signing and/or encryption the corresponding OIN's may differ.
Profiling (b)	Should multiple PartyId elements be present in From and To elements?	
Profiling (c)	Is the type attribute needed for each PartyId, and if so, what must it contain? Example – within the EAN•UCC system, the PartyId element and type are represented using Global Location Number. <eb:PartyId eb:type="http:/www.iso.int/schemas/eanucc/gln">1234567890128</eb:PartyId>	The type attribute **must** be present and **should** have the fixed value. The following type attribute value has to be used in case of an OIN is used by the partner: **urn:osb:oin**
Alignment	appears as PartyId element in CPA. (c) appears as PartyId/@type in CPA	
Test References		
Notes		ISO 6523 is an international standard registry of agencies issuing codes. Value 0106 in this registry identifies the Association of Chambers of Commerce and Industry in the Netherlands. The prefix urn:oasis:names:tc:ebxml-cppa:PartyId-type is used to indicate the issuing agency is an ISO 6523 registered agency. The type attribute allows unique identification of the agency that issues the number or code that identifies the partner. In theory, this mechanism allows multiple identification systems to be used in parallel, with no

		requirement that the codes in those systems do not overlap.

4.1.2 Profile Requirement Item: Role

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.1.2 Role Element** **Header elements:** /SOAP:Header/eb:MessageHeader/eb:From/eb:Role /SOAP:Header/eb:MessageHeader/eb:To/eb: Role	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Are Roles defined for each party of each business process? List them, or provide a reference to the source of these values. Example – within the EAN•UCC system, approved values are specified by the EAN•UCC Message Service Implementation Guide. <eb:Role>http:/www.ean-ucc.org/roles/seller</eb:Role>	Business process is out of scope for (this version of the) Digikoppeling. Within a single contract (CPA) between two Partners: - A Partner **must** fulfill one and only one role (a Partner cannot change its role within one contract). - A Partner can send messages (one or more) and/or receive messages (one or more). In case a Partner wants to use different roles, different contracts (CPA's) must be used.
Alignment	[Per-process; may reference Role values in BPSS [BPSS] definitions. Appears as Role/@name in CPA.]	
Test References		

Notes		

4.1.3 Profile Requirement Item: CPAId

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.2 CPAId Element** Header elements: /SOAP:Header/eb:MessageHeader/eb:CPAId	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	What identification scheme is used for the CPAId, and what form should it take? If it is a URI, how is it constructed? Does it reference a real CPA, or is it just a symbolic identifier? Example – within the EAN•UCC system, the value of the CPAId is the concatenation of the Sender and Receiver GLNs followed by a four digit serial number. 1234567890128 - GLN Party A 3456789012340 - GLN Party B 0001 - CPA Number between parties A and B	The proposed EAN•UCC is recommended as a good practice.
Alignment	Appears as CollaborationProtocolAgreement/@cpaid in CPA.	
Test References		
Notes		

4.1.4 Profile Requirement Item: ConversationId

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.3 ConversationId Element** Header elements: /SOAP:Header/eb:MessageHeader/eb:ConversationId	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	What is the user definition of a Conversation? What is the business criterion used to correlate messages considered parts of the same conversation?	[ISO 15000-2] requires that request messages, response messages, and any acknowledgments and error messages have the same value for ConversationId.
Profiling (b)	In case the MSH implementation gives exposure of the ConversationId as it appears in the header, what identification scheme should be used for its value, and what format should it have? If it is a URI, how is it constructed? In case the ConversationId is not directly exposed, but only a handle that allows applications to associate messages to conversations, if the value of this handle is under control of the application, what format should it have?	No recommendation made.
Alignment	If BPSS is used, ConversationId typically maps to a business transaction. Is that the case? Does it map to a business collaboration instead?	No recommendation made. Business process is out of scope for Digikoppeling.
Test References		
Notes		ConversationId is a required ebXML message header element.

4.1.5 Profile Requirement Item: MessageId

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.6.1 1.1.1 MessageId Element** Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:1.1.1 MessageId	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Although there is no requirement for an MSH to give control about 1.1.1 MessageId to an application, some implementations may allow this. In this case, is there any requirement on the source of this ID? Any length and format restrictions whenthe ID is generated?	No recommendation made. The value of 1.1.1 MessageId does not need to meet any requirements beyond the string format specified in [ISO 15000-2] and the global uniqueness constraint of [RFC 2822].
Alignment		
Test References		
Notes		

4.1.6 Profile Requirement Item: Service

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.4 Service Element** Header elements: /SOAP:Header/eb:MessageHeader/eb:Service **/SOAP:Header/eb:MessageHeader/eb:Service/@type**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Are Services (related groups of Actions) defined for each party of each business process? List them, or provide a reference to the source of these values. [Per-process; absent from BPSS definitions.] Is there a URI format scheme for this element?	No recommendation made.
Profiling (b)	Is there a defined "type" for Service elements? If so, what value must the type attribute contain?	The text content of the Service element **must not** contain white space.
Alignment	Appears as Service element in CPA Appears as Service/@type in CPA	
Test References		
Notes		

4.1.7 Profile Requirement Item: Action

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.5 Action Element** Header elements: /SOAP:Header/eb:MessageHeader/eb:Action	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Are actions defined for each party to each business process? List them, or provide a reference to the source of these values. [Per-process; may reference BusinessAction values in BPSS definitions. Example – within the EAN•UCC system, approved values are specified by the EAN•UCC Message Service Implementation Guide. <eb:Action>Confirmation</eb:Action>	No recommendation made.
Alignment	Appears as ThisPartyActionBinding/@action in CPA.]	
Test References		
Notes		The text content of the Action element in the header **must not** contain white space.

4.1.8 Profile Requirement Item: Timestamp

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.6.2, 6.3.2.2, 6.4.5, 7.3.2** Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:Timestamp /SOAP:Header/eb:MessageHeader/ eb:Acknowledgment/eb:Timestamp	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Must Timestamp include the 'Z' (UTC) identifier?	Timestamps **must** include the 'Z' (UTC) identifier.
Alignment		
Test References		
Notes		

4.1.9 Profile Requirement Item: Description

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.1.8 Description Element** Header elements: **/SOAP:Header/eb:MessageHeader/eb:Description**	**Best effort & Reliable messaging & End-to-End Security**
Profiling	Are one or more Message Header Description elements required? In what language(s)? Is there a convention for its contents?	No recommendation made. Description elements are not required. Message handlers **may** ignore Description elements.
Alignment		
Test References		
Notes		

4.1.10 Profile Requirement Item: Manifest

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.2.2 Manifest Validation** Header elements: /SOAP:Body/eb:Manifest	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	How many Manifest elements must be present, and what must they reference? Does the order of Manifest elements have to match the order of the referenced MIME attachments? Any restriction on the range of value for xlink:reference (e.g. nothing other than content id references)?	Manifest elements **must** only reference business documents or other payloads that are included in the ebXML message as a MIME part allows for references to external message payloads (for instance, using HTTP URIs), which are logically part of the message, but not as a physical entity in the MIME envelope. This is **never used** in these profiles.
Profiling (b)	Must a URI whichcannot be resolved be reported as an error?	A Content Id URI reference that cannot be resolved **must** be treated as an error.
Alignment		
Test References		
Notes		XML or other business documents can have references to other resources which are not part of the ebXML message. It is up to the receiving application to interpret any such references.

4.1.11 Profile Requirement Item: Reference

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.2.1 Reference Element** Header elements: /SOAP:Body/eb:Manifest/eb:Reference	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is the xlink:role attribute required? What is its value?	Not applicable. The xlink:role attribute is not required.
Profiling (b)	Are any other namespace-qualified attributes required?	Not applicable. No other namespace-qualified attributes are allowed.
Alignment		
Test References		
Notes		Only the Content Id reference mechanism [RFC 2392] is allowed.

4.1.12 Profile Requirement Item: Reference/Schema

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.2.1.1 Schema Element** Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Schema	**Best effort & Reliable Messaging & End-to-End Security**

Profiling	Are there any Schema elements required? If so, what are their location and version attributes?	Schema elements are not required. The Digikoppeling does not perform XML schema validation.
Alignment		
Test References		
Notes		

4.1.13 Profile Requirement Item: Reference/Description

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 3.2.1.2 Description Element** Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Description	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Are any Description elements required? If so, what are their contents?	Description elements are optional. They **may** be ignored by any receiving message service handler.
Alignment		
Test References		
Notes		

4.2 Module: Security

4.2.1 Profile Requirement Item: Signature generation

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 4.1.4.1 Persistent Digital Signature** Header elements: /SOAP:Header/Signature	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling (a)	Must messages be digitally signed? [Yes, for Security Services Profiles 1, 6-21.]	Not applicable. These profiles do not support XML Digital Signatures at the message handler level.		**Required** in this profile.
Profiling (b)	Are additional Signature elements required, by whom, and what should they reference?	Not applicable.		**Never used** in this profile.
Profiling (c)	What canonicalization method(s) must be applied to the data to be signed?	Not applicable.		The use of XML canonicalization is **required**. [XML Canonicalization]
Profiling (d)	What canonicalization method(s) must be applied to each payload object, if different from above?	Not applicable.		

Profiling (e)	What signature method(s) must be applied?	Not applicable.	The use of **RSA-SHA-1** is **required**. [XMLDSIG], [RFC 2437].
Profiling (f)	What Certificate Authorities (issuers) are allowed or required for signing certificates?	Not applicable.	The use of PKI Overheid certificates is **required** in which an OIN is used in the Subject.serialNumber. [PKI en OIN]
Profiling (g)	Are direct-trusted (or self-signed) signing certificates allowed?	Not applicable.	This profile is **never used**.
Profiling (h)	What certificate verification policies and procedures must be followed?	The requirements as stated by the PKIOverheid [PKI.Policy] have to be used. The use of certificate revocation lists (CRL) from the trusted CA's is required.	
Alignment	(a) Appears as BusinessTransactionCharacteristics/@isAuthenticated=persistent and BusinessTransactionCharacteristics/@isTamperProof=persistent in CPA		
Test References			
Notes		Applications submitting data to, or receiving data from, Digikoppeling ebXML Message service handlers can perform signing at the message payload level. The ebXML Messaging protocol is payload-neutral and therefore supports signed payloads. In that case, the	The use of SHA-1 is secure. For the long term, use of more advanced algorithms will be considered. [FIPS 180-3]

		Digikoppeling is not aware of the presence of signatures and does not perform signature verification.	

4.2.2 *Profile Requirement Item: Persistent Signed Receipt*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 4.1.4.2 Persistent Signed Receipt** Header elements: /SOAP:Header/eb:Signature	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling (a)	Is a digitally signed Acknowledgment Message required? [Yes, for Security Services Profiles 7, 8, 10, 12, 14, 15, 17, 19-21. See the items beginning with Section 4.1.4.1 for specific Signature requirements.]	Not applicable.		Signing acknowledgements is **required**.
Profiling (b)	If so, what is the Acknowledgment or Receipt schema?	Not applicable.		[XMLDSIG]
Alignment	Appears as BusinessTransactionCharacteristics/@isNonRepudiationReceiptRequired=persistent in CPA.			
Test References				
Notes				

4.2.3 Profile Requirement Item: Non Persistent Authentication

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] S ection 4.1.4.3 Non Persistent Authentication** Header elements: /SOAP:Header/eb:Signature	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Are communication channel authentication methods required? [Yes, for Security Services Profiles 2-5.] Which methods are allowed or required?	Client and Server authentication is required using HTTPS and TLS 1.0 [RFC 2246]. Message service handlers **should NOT** be able to operate in SSL v3 backward compatibility mode.
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthenticated=transient in CPA.]	
Test References		
Notes		

4.2.4 *Profile Requirement Item: Non Persistent Integrity*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 4.1.4.4 Non Persistent Integrity** Header elements: /SOAP:Header/eb:Signature	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Are communication channel integrity methods required? [Yes, for Security Services Profile 4.] Which methods are allowed or required?	Not applicable
Alignment	[Appears as BusinessTransactionCharacteristics/@isTamperproof=transient in CPA.]	
Test References		
Notes		

4.2.5 *Profile Requirement Item: Persistent Confidentiality*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and	**[ebMS 2.0] Section 4.1.4.5 Persistent**			

Reference	**Confidentiality** Header elements: /SOAP:Header/eb:Signature	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling (a)	Is selective confidentiality of elements within an ebXML Message SOAP Header required? If so, how is this to be accomplished? [Not addressed by Messaging Specification 2.0.]	Not applicable.		
Profiling (b)	Is payload confidentiality (encryption) required? [Yes, for Security Services Profiles 13, 14, 16, 17, 21, 22.] Which methods are allowed or required?	Not applicable.		Payload confidentiality is **optional**. Whenever used, the [FIPS 179] standard (AES 256-cbc) is used by the [XML Encryption].
Alignment	(b) [Appears as BusinessTransactionCharacteristics/@isConfidential=persistent in CPA.]			
Test References				
Notes		Applications submitting data to, or receiving data from, Digikoppeling message handlers can perform encryption at the payload processing level. The ebXML Messaging protocol is payload-neutral and therefore supports transport of encrypted payloads. However, any encryption and decryption of payloads is out of scope for these profiles..		

4.2.6 Profile Requirement Item: Non Persistent Confidentiality

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] S ection 4.1.4.6 Non Persistent Confidentiality** Header elements: /SOAP:Header/eb:Signature	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Are communication channel confidentiality methods required? [Yes, for Security Services Profiles 3, 6, 8, 11, 12.] Which methods are allowed or required?	The use of HTTPS using TLS 1.0 [RFC 2246] is required. Message service handlers **should NOT** support SSL v3 compatibility mode.
Alignment	[Appears as BusinessTransactionCharacteristics/@isConfidential=transient in CPA.]	
Test References		
Notes		

4.2.7 Profile Requirement Item: Persistent Authorization

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 4.1.4.7 Persistent Authorization** Header elements: /SOAP:Header/eb:Signature	**Best effort & Reliable messaging & End-to-End Security**
Profiling	Are persistent authorization methods required? [Yes, for Security Services Profiles 18-21.] Which methods are allowed or required?	Not applicable
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequired =persistent in CPA.]	
Test References		
Notes		

4.2.8 Profile Requirement Item: Non Persistent Authorization

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] S ection 4.1.4.8 Non Persistent Authorization** Header elements: /SOAP:Header/eb:Signature	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Are communication channel authorization methods required? [Yes, for Security Services Profile 2.] Which methods are allowed or required?	TLS [RFC 2246] client and server authentication is **required** as described in section in 4.2.3.
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequired =transient in CPA.]	
Test References		
Notes		

4.2.9 *Profile Requirement Item: Trusted Timestamp*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 4.1.4.9 Trusted Timestamp** Header elements: /SOAP:Header/eb:Signature	**Best effort & Reliable messaging & End-to-End Security**
Profiling	Is a trusted timestamp required? [Yes, for Security Services Profiles 9-12, 15-17, 20, 21.] If so, provide details regarding its usage.	Not applicable
Alignment		
Test References		
Notes		Applications submitting data to, or receiving data from, Digikoppeling message handlers can perform timestamping. The ebXML Messaging protocol is payload-neutral and therefore supports timestamped payloads. However, this timestamping functionality is not part of the Digikoppeling functionality. Any valid ebXML Message must contain an eb:TimeStamp as part of the eb:MessageData.

4.3 Module : Error Handling

4.3.1 Profile Requirement Item

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 4.2.3.2 Error Element** Header elements: /SOAP:Header/eb:ErrorList/eb:Error /SOAP:Header/eb:ErrorList/ eb:Error/@codeContext /SOAP:Header/eb:ErrorList/ eb:Error/@errorCode	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is an alternative codeContext used? If so, specify	Not applicable
Profiling (b)	If an alternative codeContext is used, what is its errorCode list?	
Profiling (c)	When errors should be reported to the sending application, how should this be notified (e.g. using a logging mechanism or a proactive callback)?	Not applicable
Alignment		
Test References		
Notes		

4.4 Module : SyncReply

4.4.1 Profile Requirement Item: SyncReply

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 4.3 SyncReply** Header elements: /SOAP:Header/eb:SyncReply/	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is SyncReply mode allowed, disallowed, or required, and under what circumstances? [May be process-specific.]	Not applicable. SyncReply is **not supported** in this specification.
Profiling (b)	If SyncReply mode is used, are MSH signals, business messages or both expected synchronously?	
Alignment	[Affects setting of 6.4.7 syncReplyMode element. Appears as MessagingCharacteristics/@syncReplyMode in CPA.]	
Test References		
Notes		Asynchronous messaging does not preclude support of a "near real time" response quality of service required for e.g. interactive applications. The ebXML 1.1.1 MessageId and RefTo1.1.1 MessageId header elements encode correlation of request and response messages.

4.5 Module : Reliable Messaging

4.5.1 Profile Requirement Item: SOAP Actor attribute

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 6.3.1.1 SOAP Actor attribute** Header elements: /SOAP:Header/eb:AckRequested/	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling (a)	SOAP Actor attribute: Are point-to-point (nextMSH) MSH Acknowledgments to be requested? [Yes, for RM Combinations 1, 3, 5, 7; refer to ebMS section 6.6. Appears as MessagingCharacteristics/@ackRequested with @actor=nextMSH in CPA.]	Not applicable.		
Profiling (b)	Are end-to-end (toParty) MSH Acknowledgments to be requested? [Yes, for RM Combinations 1, 2, 5, 6. Appears as MessagingCharacteristics/@ackRequested with @actor=toPartyMSH in CPA.]	Not applicable.	It is **required** that the final recipient MSH returns a receipt acknowledgment message.	**Optional**: See profiles Best Effort or Reliable Messaging for details.
Test References				
Notes				

4.5.2 *Profile Requirement Item: Signed attribute*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 6.3.1.2 Signed attribute** Header elements: /SOAP:Header/eb:AckRequested/	**Best effort**	**Reliable messaging**	**End-to-End Security**
Profiling	Must MSH Acknowledgments be (requested to be) signed ?	Not applicable.		Signing of acknowledgements is **required**.
Alignment	[Appears as MessagingCharacteristics/ @ackSignatureRequested in CPA.]			
Test References				
Notes				

4.5.3 *Profile Requirement Item: DuplicateElimination*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 6.4.1** Header elements: /SOAP:Header/eb:AckRequested/	**Best effort**	**Reliable messaging**	**End-to-End Security**
Profiling (a)	Is elimination of duplicate messages required? [Yes, for RM Combinations 1-4.]	Duplicate Elimination is	Duplicate Elimination is **required**.	Duplicate Elimination is optional. See profiles Best Effort or Reliable Messaging for details.

		never used.		
Profiling (b)	What is the expected scope in time of duplicate elimination? In other words, how long should messages or message ID's be kept in persistent storage for this purpose?		Message ID's **should** minimally be kept in persistent storage to prevent duplicate delivery during the time interval in which the From Party MSH may be attempting to resend unacknowledged messages. This interval is (1+Retries)*RetryInterval.	
Alignment	Appears as MessagingCharacteristics/ @duplicateElimination in CPA			
Test References				
Notes			Message ID's in ebXML are based on [RFC 2822], and must therefore be globally unique, which in theory prevents accidental re-use of ID's for distinct messages. Factors like system load, disk space, database table limitations, period maintenance schedules **may** be used in message purging policies. Cleaning message ID stores often (temporarily) affects	

			responsiveness of a system.	

4.5.4 *Profile Requirement Item: Retries and RetryInterval*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 6.4.3, 6.4.4 Retries and RetryInterval** Header elements: /SOAP:Header/eb:AckRequested/	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling (a)	If reliable messaging is used, how many times must an MSH attempt to redeliver an unacknowledged message?	Not applicable	Some organizations using the Digikoppeling may not have 24x7 support for their ebXML Messaging services. A system crash may not be remedied until the next working day. Where possible, the values of Retries and RetryInterval **should** be set to allow reliable delivery of messages even after prolonged unavailability. If no value is defined by the parties, a value of 5 days is used.	Depends on the use of best effort or reliable messaging.
Profiling (b)	What is the minimum time a Sending MSH should wait between retries of an unacknowledged message?			
Alignment	(a) [Appears as ReliableMessaging/Retries in CPA.]			

	(b) [Appears as ReliableMessaging/RetryInterval in CPA.]	
Test References		
Notes		If **reliable messaging** is used: Some ebXML messaging software products have a transport retry mechanism, in addition to the ebXML retry mechanism. In this case the ebXML retry interval **should** be set in such a way that any such transport retries have been completed first.

4.5.5 Profile Requirement Item: PersistDuration

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 6.4.6 PersistDuration**	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling	How long must data from a reliably sent message be kept in persistent storage by a receiving MSH, for the purpose of retransmission?	Not applicable	Depends on the retry interval as defined in the particular collaboration, defined by the involved parties. If no value is defined by the parties, a value of 5 days is used.	Depends on the use of best effort or reliable messaging.
Alignment	[Appears as ReliableMessaging/PersistDuration in CPA.]			
Test References				

Notes				

4.5.6 *Profile Requirement Item: Reliability Protocol*

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
Name and Reference	**[ebMS 2.0] Section 6.5.3, 6.5.7**	**Best effort**	**Reliable Messaging**	**End-to-End Security**
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	**Never** used in this profile.	The Reliable Messaging Protocol in [ISO 15000-2] must be used.	**Optional** in this profile: depends on the use of best effort or reliable messaging.
Profiling (a)	Must a response to a received message be included with the acknowledgment of the received message? Are they to be separate, or are both forms allowed?	Not applicable	Receipt acknowledgment messages are standalone messages. They **must** not to be bundled with business response messages or other ebXML messages.	
Profiling (b)	If a DeliveryFailure error message cannot be delivered successfully, how must the error message's destination party be informed of the problem?	Each collaborating party is responsible for defining procedures for handling these issues.		
Alignment				
Test References				
Notes				

4.6 Module : Message Status

4.6.1 Profile Requirement Item: Status Request message

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 7.1.1 Message Status Request Message** Header elements: Eb:MessageHeader/eb:StatusRequest	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	If used, must Message Status Request Messages be digitally signed?	Not applicable.
Profiling (b)	Must unauthorized Message Status Request messages be ignored, rather than responded to, due to security concerns?	Not applicable.
Alignment		
Test References		
Notes		

4.6.2 Profile Requirement Item: Status Response message

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 7.1.2 Message Status Response Message** Header elements: Eb:MessageHeader/eb:StatusResponse	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	If used, must Message Status Response Messages be digitally signed?	Not applicable.
Alignment		
Test References		
Notes		

4.7 Module : Ping Service

4.7.1 Profile Requirement Item: Ping-Pong Security

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 8.1, 8.2 Message Service Handler Ping/Pong Message** Header elements: Eb:MessageHeader/eb:Service Eb:MessageHeader/eb:Action	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	If used, must Ping Messages be digitally signed?	If Ping-Pong is used, it is **optional** for Ping messages to be digitally signed.
Profiling (b)	If used, must Pong Messages be digitally signed?	If Ping-Pong is used, it is b for Pong messages to be digitally signed.
Profiling (c)	Under what circumstances must a Pong Message not be sent?	No recommendation made.
Profiling (d)	If not supported or unauthorized, must the MSH receiving a Ping respond with an error message, or ignore it due to security concerns?	No recommendation made
Alignment		
Test References		

Notes		

4.8 Module : Multi-Hop

4.8.1 Profile Requirement Item: Use of intermediaries

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**Header elements:** **[ebMS 2.0] Section 10**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Are any store-and-forward intermediary MSH nodes present on the message path?	Endpoints connecting to the Digikoppeling **must** be able to operate in Endpoint mode. They attempt to deliver inbound messages locally, and **may** treat any exceptions as failures. They are **not required** to support any forwarding of ebXML Messages to other business partners.
Profiling (b)	What are the values of Retry and RetryInterval between intermediate MSH nodes?	Not applicable. Any Digikoppeling-level intermediaries must not support reliable messaging, in order to not interfere with end-to-end reliable message delivery. Message handlers **must not** request nextMSH receipt acknowledgments and such requests **should** be ignored by any ebXML intermediary. The ebXML intermediaries also **should not** filter duplicate messages. As with business messages, any Digikoppeling-level ebXML intermediaries **should** attempt to forward end-to-end receipts and errors.
Alignment		

Test References		
Notes		In case **Best Effort** is used: Any Digikoppeling-level ebXML intermediary may support transport retries, for instance to handle temporary TCP or HTTP transport level errors. This is not required. In case **Reliable messaging** is used: This profile uses end-to-end reliable messaging. This allows the Digikoppeling to recover from any temporary processing failures at the level of intermediaries. Upcoming versions of the Digikoppeling **may** support store and forward ebXML intermediaries at an infrastructure level. The functionality of these intermediaries is likely be limited to fully transparent, asynchronous store-and-forward routing of ebXML Messages. In that case, no special processing is required of endpoints in the presence of any such intermediaries, as compared to direct point-to-point connections, other than supporting connection to/from the URL and client and server TLS authentication details for the intermediary rather than the "true" sender/recipient. In case **End-to-End Security** is used: see the notes for Best effort of Reliable messaging.

4.8.2 Profile Requirement Item: Acknowledgements

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 10.1.1, 10.1.3** Header elements: Eb:MessageHeader/	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Must each intermediary request acknowledgment from the next MSH?	Not applicable. There is **no support** for ebXML next MSH acknowledgments.

Profiling (b)	Must each intermediary return an Intermediate Acknowledgment Message synchronously?	Not applicable. There is **no support** for ebXML next MSH acknowledgments.
Profiling (c)	If both intermediary (multi-hop) and endpoint acknowledgments are requested of the To Party, must they both be sent in the same message?	Not applicable. There is **no support** for ebXML next MSH acknowledgments.
Alignment		
Test References		
Notes		

4.9 SOAP Extensions

4.9.1 Profile Requirement Item: #wildCard, Id

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 2.3.6, 2.3.7, 2.3.8**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	**(Section 2.3.6)** #wildcard Element Content: Are additional namespace-qualified extension elements required? If so, specify.	Not applicable. No additional namespace-qualified extension elements are required. The toPartyMSH and any intermediaries **must** ignore any extension elements.

Profiling (b)	**(Section 2.3.7)** Is a unique "id" attribute required for each (or any) ebXML SOAP extension element, for the purpose of referencing it alone in a digital signature?	Not applicable. Digital Signing is **not supported.**
Profiling (c)	**(Section 2.3.8)** Is a version other than "2.0" allowed or required for any extension elements?	These profiles are limited to ebXML Messaging version 2.0 [ISO 15000-2].
Alignment		
Test References		
Notes		

4.10 MIME Header Container

4.10.1 Profile Requirement Item: charset

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Section 2.1.3.2** MIME Header elements: Content-Type	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Is the "charset" parameter of Content-Type header necessary? If so, what is the (sub)set of allowed values? Example: Content-Type: text/xml; charset="UTF-8"	UTF-8
Alignment		
Test References		
Notes		

4.11 HTTP Binding

4.11.1 Profile Requirement Item: HTTP Headers

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Appendix B.2.2 Sending ebXML Service messages over HTTP** Header elements, MIME parts	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is a (non-identity) content-transfer-encoding required for any of the MIME multipart entities?	Content transfer encoding **should not** be used.
Profiling (b)	If other than "ebXML" what must the SOAPAction HTTP header field contain?	The value of the SOAPAction HTTP header field MUST be “ebXML”
Profiling (c)	What additional MIME-like headers must be included among the HTTP headers?	Additional MIME-like headers **should not** be included with the HTTP header. Any ebXML MSH **should** ignore any such additional HTTP header.
Alignment		
Test References		
Notes		

4.11.2 Profile Requirement Item: HTTP Response Codes

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Appendix B.2.3 HTTP Response Codes** Header elements, MIME parts	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	What client behaviors should result when 3xx, 4xx or 5xx HTTP error codes are received?	In the event of an HTTP 5xx error code, the MSH **must** behave according to the recommendations specified in [SOAP1.1]. An HTTP 503 error code **should** be treated as a recoverable error (i.e. **should not** terminate any reliable messaging retries). Codes in the 3xx and 4xx ranges **must** be interpreted as errors.
Alignment		
Test References		
Notes		

4.11.3 Profile Requirement Item: HTTP Access Control

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Appendix B.2.6 Access Control** Header elements, MIME parts	**Best effort & Reliable Messaging & End-to-End Security**
Profiling	Which HTTP access control mechanism(s) are required or allowed?	Access control is based on client certificate information only.

	[Basic, Digest, or client certificate (the latter only if transport-layer security is used), for example. Refer to item 4.1.4.8 in Security section.	HTTP Basic or Digest authentication are **not supported**.
Alignment	Appears as AccessAuthentication elements in CPA.	
Test References		
Notes		

4.11.4 Profile Requirement Item: HTTP Confidentiality and Security

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Appendix B.2.7 Confidentiality and Transport Protocol Level Security** Header elements, MIME parts	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is HTTP transport-layer encryption required? What protocol version(s)? [SSLv3, TLSv1, for example. Refer to item 4.1.4.6 in Security section.]	Encryption based on HTTPS using TLS 1.0 [RFC 2246] is **required**. TLS implementations **must NOT** support SSL v3 backwards compatiblity mode.
Profiling (b)	What encryption algorithm(s) and minimum key lengths are required?	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
Profiling (c)	What Certificate Authorities are acceptable for server certificate authentication?	PKI overheid maintains a list of approved certificate service providers [PKI-CA].
Profiling (d)	Are direct-trust (self-signed) server certificates allowed?	Self-signed certificates are only allowed in test cases.
Profiling (e)	Is client-side certificate-based authentication allowed or required?	Client-side authentication is required.
Profiling (f)	What client Certificate Authorities are acceptable?	PKI overheid maintains a list of approved certificate service [PKI-CA].
Profiling (g)	What certificate verification policies and procedures must be followed?	PKI overheid procedures are described in [PKI-Policy]. The use of certificate revocation lists (CRL) from the trusted CA's is required.
Alignment		
Test References		
Notes		

4.12 SMTP Binding

4.12.1 Profile Requirement Item: MIME Headers

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0

Name and Reference	**[ebMS 2.0] Appendix B.3.2 Sending ebXML Messages over SMTP**	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	Is any specific content-transfer-encoding required, for MIME body parts which must conform to a 7-bit data path? [Base64 or quoted-printable, for example.]	Not Applicable. This specification only supports the HTTP transport protocol.
Profiling (b)	If other than "ebXML" what must the SOAPAction SMTP header field contain?	Not Applicable. This specification only supports the HTTP transport protocol.
Profiling (c)	What additional MIME headers must be included amongst the SMTP headers?	Not Applicable. This specification only supports the HTTP transport protocol.
Alignment		
Test References		
Notes		

4.13 Profile Requirement Item: SMTP Confidentiality and Security

		Digikoppeling 2.0 profiles for ebXML Messaging 2.0
Name and Reference	**[ebMS 2.0] Appendix B.3.4, B.3.5** Header elements, MIME parts	**Best effort & Reliable Messaging & End-to-End Security**
Profiling (a)	What SMTP access control mechanisms are required? [Refer to item 4.1.4.8 in Security section.]	Not applicable. This specification only supports the HTTP transport protocol.
Profiling (b)	Is transport-layer security required for SMTP, and what are the specifics of its use? [Refer to item 4.1.4.6 in Security section.]	Not applicable. This specification only supports the HTTP transport protocol.
Alignment		
Test References		
Notes		

5 Operational Profile

This section defines the operational aspect of the profile: type of deployment with which the profile which is mentioned above is supposed to operate with, expected or required conditions of operations, usage context, etc.

5.1 Deployment and Processing requirements for CPAs

	Digikoppeling 2.0 profiles for ebXML Messaging 2.0
	Best effort & Reliable Messaging & End-to-End Security
Is a specific registry for storing CPA's required? If so, provide details.	Pending.
Is there a set of predefined CPA templates that can be used to create given Parties' CPA's?	It is **highly recommended** to use the Digikoppeling CPA Creation facility. A web-based program is available by which CPA's are created. See http://www.logius.nl/digikoppeling/documentatie for information about the CPA Creation facility (document is written in Dutch). In addition to this there is a **Best Practices** document with information about the use of CPA's.
Is there a particular format for file names of CPA's, in case that file name is different from CPA-ID value?	No recommendation.
Others	It is **required** to specify the resulting ebMS collaboration with a CPA.

	It is **required** that all actions within a CPA make use of (one and) the same default channel for sending acknowledgements. This default channel can only support **one specific profile** within a CPA (for instance either osb-rm-s or osb-rm, not both within one CPA). As a result, when there are actions which are based on different profiles (for instance osb-rm-s and osb-be) and the profiles for the acknowledgements are different as well (for instance osb-rm-s and osb-be), multiple CPA's must be created.

5.2 Security Profile

	Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
	Best effort	**Reliable Messaging**	**End-to-End Security**
Which security profiles are used, and under what circumstances (for which Business Processes)? [Refer to Appendix C of Message Service Specification. May be partially captured by BPSS isConfidential, is Tamperproof, isAuthenticated definitions.]	Security profile 3 [ebMS 2.0] Appendix C]: "Sending MSH authenticates and both MSHs negotiate a secure channel to transmit data" **must be** applied. The HTTPS connection uses encryption to provide in transit confidentiality regarding the complete ebXML message and performs **both** certificate-based Client and Server authentication during the TLS handshake.		
			Security profile 8 [ebMS 2.0 Appendix C] **must be** used: "Sending MSH applies XML/DSIG structures to message and passes in a secure communications channel. Sending MSH applies XML/DSIG structures to send messagesand Receiving MSH returns a signed receipt." Security profile 14 [ebMS 2.0 Appendix C] is **optional**: "Sending MSH applies XML/DSIG structures to message **and** applies confidentiality structures (XML-Encryption) and Receiving MSH returns a signed receipt".

(section 4.1.5) Are any recommendations given, with respect to protection or proper handling of MIME headers within an ebXML Message?	Not applicable. No additional recommendations made.	
Are any specific third-party security packages approved or required?	No recommendation made.	
Whichsecurity and management policies and practices are recommended?	Pending.	
Any particular procedure for doing HTTP authentication, e.g. if exchanging name and password, how?	Besides the client authentication in HTTPS, no additional procedures are applied.	
Others		

5.3 Reliability Profile

	Digikoppeling 2.0 profiles for ebXML Messaging 2.0		
	Best effort	**Reliable Messaging**	**End-to-End Security**
If reliable messaging is required, by what method(s) may it be implemented? [The ebXML Reliable Messaging protocol, or an alternative reliable messaging or transfer protocol.]	Not applicable	The ebXML reliable messaging protocol **must be** used.	**Optional**. Depends on the use of best effort or reliable messaging.

Which Reliable Messaging feature combinations are required? [Refer to Section 6.6 of Message Service Specification.]		Reliable Messaging profile 2: Duplicate elimination Yes AckRequested ToPartyMSH Yes AckRequested NextMSH No	
Others			

5.4 Error Handling Profile

	Digikoppeling 2.0 profiles for ebXML Messaging 2.0
	Best effort & Reliable Messaging & End-to-End Security
(Section 4.2.4.2) Should errors be reported to a URI which is different from the one identified within the From element? What are the requirements for the error reporting URI and the policy for defining it?	No recommendation made
What is the policy for error reporting? In case an error message cannot be delivered, what other means are used to notify the party, if any?	Pending.
(Appendix B.4) What communication protocol-level error recovery is required, before deferring to Reliable Messaging recovery? [For example, how many retries should occur in the case of failures in DNS, TCP connection, server errors, timeouts; and at what interval?]	Pending.
Others	

Message Payload and Flow Profile

	Digikoppeling 2.0 profiles for ebXML Messaging 2.0
	Best effort & Reliable Messaging & End-to-End Security
What are typical and maximum message payload sizes which must be handled? (maximum, average)	Some ebXML Messaging products have performance and scalability issues with payloads larger than a (single digit) megabyte in size. Some partners may need to bridge incoming ebXML Message flows to other (enterprise) messaging protocols whichhave message size limits. Firewalls and other networking equipment may also (implicitly) impose size limits.
What are typical communication bandwidth and processing capabilities of an MSH for these Services?	No recommendation made.
Expected Volume of Message flow (throughput): maximum (peak), average?	No recommendation made.
(Section 2.1.4) How many Payload Containers must be present?	Messages other than standalone receipt acknowledgement messages and error messages must contain one container with the actual xml payload and optional one or more containers for the attachments (one container for each attachment). This option is provided to facilitate bridging to other protocols at the enterprise level that may or may not support multiple payloads natively. If there is only and only one container, this profile (section) is Digikoppeling 1.0 and Digikoppeling 1.1 compliant.

What is the structure and content of each container? [List MIME Content-Types and other process-specific requirements.] Are there restrictions on the MIME types allowed for attachments?	The first payload container must be of type “application/xml”. I.e. for the Digikoppeling the first container consists of a single XML business document (the Digikoppeling 'payload'). If there are additional containers, each container will get a MIME type reflecting the type of the Digikoppeling 'attachment' it contains.
How is each container distinguished from the others? [By a fixed ordering of containers, a fixed Manifest ordering, or specific Content-ID values.]. Any expected relative order of attachments of various types?	No recommendation made.
Others	

5.5 Additional Messaging Features beyond ebMS Specification

	Digikoppeling 2.0 profiles for ebXML Messaging 2.0
	Best effort & Reliable Messaging & End-to-End Security
Are there additional features out of specification scope, whichare part of this messaging profile, as an extension to the ebMS profiling?	No.

5.6 Additional Deployment or Operational Requirements

	Digikoppeling 2.0 profiles for ebXML Messaging 2.0

	Best effort & Reliable Messaging & End-to-End Security
Operational or deployment aspects which are object to further requirements or recommendations.	Pending.

6 References

6.1 Normative

[FIPS 197] NIST FIPS 197. Advanced Encryption Standard (AES). URL http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[ETSI TS 102 176-1] Electronic Signatures and Infrastructures (ESI). Algorithms and Parameters for Securie Electronic Signatures. Part 1: hash functions and asymmetric algoritms.
URL http://www.etsi.org/

[ISO 15000-2] ISO 15000-2 ebXML Message Service Specification. URL http://www.oasis-open.org/specs/index.php#ebxmlmsgv2 .

[PKI-CA] PKI Overheid toegetreden certificatiehouders.
URL http://www.pkioverheid.nl/

[PKI-Policy] PKI Overheid Programma van Eisen Deel 2. Toetreden en Toezicht. URL www.logius.nl/pkioverheid, zoekterm "deel 2".

[PKI en OIN] Wijziging PvE juli 2008 cumulatief, URL http://www.pkioverheid.nl.

[RFC2119] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[RFC 2246] The TLS Protocol.
URL http://www.ietf.org/rfc/rfc2246.txt?number=2246

[RFC 2392] Content-ID and Message-ID Uniform Resource Locators
URL http://www.ietf.org/rfc/rfc2392.txt

[RFC 2437] PKCS #1: RSA Cryptography Specifications. IETF RFC 2437.
URL http://www.ietf.org/rfc/rfc2437.txt.

[RFC 2822] Internet Message Format. IETF RFC 2822.
URL http://www.ietf.org/rfc/rfc2822.txt.

[SOAP1.1] Simple Object Access Protocol (SOAP) v1.1. W3C Note 08 May 2000.
URL http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

[XMLDSIG] Joint W3C/IETF XML-Signature Syntax and Processing specification. URL http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.

[XML Encryption] XML Encryption Syntax and Processing. W3C Recommendation.
URI http://www.w3.org/TR/xmlenc-core/

[XML Canonicalization] Recommended method is "http://www.w3.org/TR/2001/REC-xml-c14n-20010315". Canonical XML.
URI http://www.w3.org/TR/xml-c14n

6.2 Non-normative

[Deployment Guide 1.1] Pete Wenzel, Jacques Durand. Deployment Profile Template For OASIS ebXML Message Service 2.0. OASIS Committee Draft 1.1, 20 June 2005.
URL http://www.oasis-open.org/apps/org/workgroup/ebxml-iic-deployment-profile-template-intro-100406.doc**.** Een account kan vereist zijn.

[ebMS3] OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features
URL http://www.oasis-open.org/committees/download.php/21534/ebms_core-3.0-spec-wd-16.pdf

[ebBP] ebXML Business Process Specification Schema Technical Specification
URL http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-bp#technical.

[FIPS 180-2] NIST FIPS 180-2 Secure Hash Standard
URL http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[FIPS 180-3] Announcing Approval of Federal Information Processing Standard (FIPS) Publication 180–3, Secure Hash Standard, a Revision of FIPS 180–2, Secure Hash Standard. URL
http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

[ISO 15000-1] ISO 15000-1 ebXML Collaboration Protocol Profile and Agreement Specification. OASIS ebXML Collaboration Protocol Profile and Agreement Specification (2.0).
URL http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf

[NIST-Keys] NIST Key Management Guideline. .
URL http://csrc.nist.gov/groups/ST/toolkit/key_management.html

[SBG-IBS] Expertteam Framework Draft Intersectorale Berichtenstandaard. Deel B. Technische Specificatie. Programma Stroomlijnen Basisgegevens.

[UMMR10] UMM Revision 10.
URL http://www.unece.org/cefact/umm/umm_index.html

[UMMUG] UMM User Guide
URL
http://www.unece.org/fileadmin/DAM/cefact/umm/UMM_userguide_220606.pdf