Logius - Standaard

Digikoppeling Koppelvlakstandaard ebMS2 3.3

Logius Standaard
Vastgestelde versie 16 mei 2019

Deze versie:
https://publicatie.centrumvoorstandaarden.nl/dk/ebms/3.3

Laatst gepubliceerde versie:
https://publicatie.centrumvoorstandaarden.nl/dk/ebms/

Laatste werkversie:
https://logius-standaarden.github.io/Digikoppeling-Koppelvlakstandaard-ebMS2/

Redacteur:
Logius Centrum voor Standaarden (Logius)

Auteur:
Logius Centrum voor Standaarden

Doe mee:
GitHub Logius-standaarden/Digikoppeling-Koppelvlakstandaard-ebMS2
Dien een melding in
Revisiehistorie
Pull requests

This document is also available in this non-normative format: pdf

Samenvatting

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 ebMS2. 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.

Status van dit document

Dit is de definitieve versie van de standaard. Wijzigingen naar aanleiding van consultaties zijn doorgevoerd.

Het OBDO heeft op advies van het Forum Standaardisatie deze versie vastgesteld.

Inhoudsopgave

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
22-11-2011	2.4	Logius	-
09-06-2014	2.5	Logius	Redactionele wijzigingen
28-01-2015	3.0	Logius	TLS 1.0 t/m TLS 1.2
04-04-2016	3.1	Logius	Referenties naar Beveiligingsvoorschriften aangepast naar nieuwe Document Digikoppeling beveiligingsvoorsch Requirement Item 4.1.8 (‘Z’ identifier) verwijderd
01-10-2017	3.2	Logius	Restrictie 1st payload aangepast
16-05-2019	3.3	Logius	Gebruik van SyncReplyMode verruimd

Colofon

Logius Servicecentrum:	Postbus 96810 2509 JE Den Haag t. 0900 555 4555 (10 ct p/m) e.servicecentrum@logius.nl

1. Inleiding §

1.1 Doel en doelgroep §

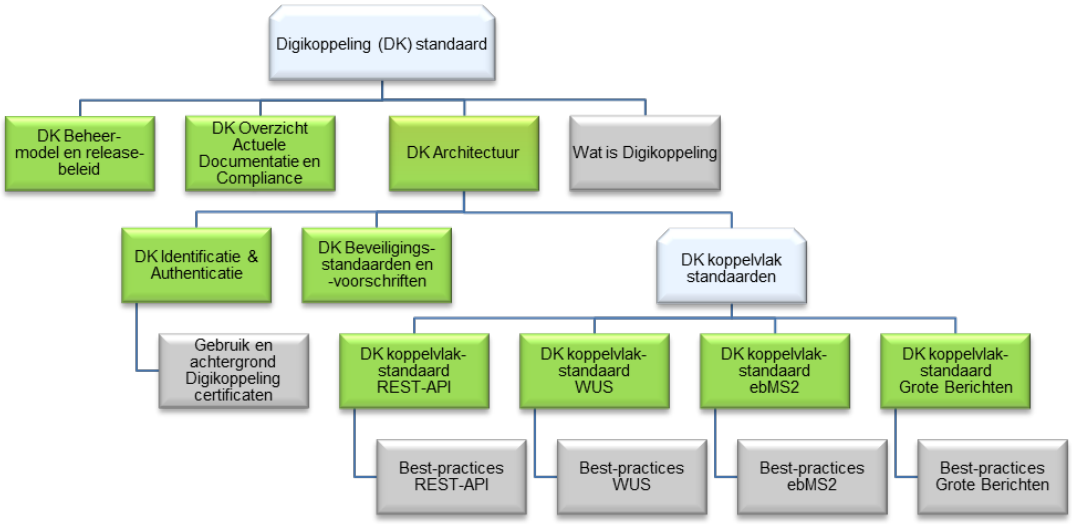
Dit document beschrijft de functionele specificaties voor Digikoppeling ebMS Deployment Profile, onderdeel van Digikoppeling.

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 ebMS2. 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
[MT]	Management	Bevoegdheid om namens organisatie (strategische) besluiten te nemen.
[PL]	Projectleiding	Verzorgen van de aansturing van projecten.
[A&D]	Analyseren & ontwerpen (design)	Analyseren en ontwerpen van oplossings-richtingen. Het verbinden van Business aan de IT.
[OT&B]	Ontwikkelen, testen en beheer	Ontwikkelt, bouwt en configureert de techniek conform specificaties. Zorgen voor beheer na ingebruikname.

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 Leidende principes §

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 is beschreven in het document [Digikoppeling Architectuur].

1.4 Koppelvlak & koppelvlakstandaard §

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

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

Dit doel kan bereikt (benaderd) worden doordat gekozen wordt voor internationale (de jure of de facto) vastgelegde standaarden, die door “alle” leveranciers interoperabel zijn geïmplementeerd. Een andere eis is dat met name afnemers gebruik kunnen maken van één “stekker” (één logistiek koppelpunt).

1.4.1 Specificatie van de koppelvlakstandaard §

De koppelvlakstandaard 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:

- 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 ebMS2 profiel zoals dat gekozen is voor Digikoppeling.

Begrippen en afkortingen worden toegelicht in het document [Digikoppeling Architectuur]. Deze zit in de Digikoppeling standaarddocumentatie.

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

2. Koppelvlakstandaard ebMS2 §

2.1 Inleiding §

Dit document specificeert de Koppelvlakstandaard ebMS2 voor berichtenuitwisseling over Digikoppeling (voorheen OverheidsServiceBus) als een toepassing van de EBXML-MSG standaard, de ebXML Message Service Specification versie 2.0 [EBXML-MSG]. 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 [EBXML-MSG] 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.

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 zal moeten voldoen aan één van de volgende Digikoppeling ebMS2 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.

*: In bepaalde gevallen mag een acknowledgement synchroon verstuurd worden. Zie par 4.4

- 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 onderweg. Voor de authenticatie en encryptie wordt gebruik gemaakt van XML digitale handtekening [xmldsig-core-20020212] en XML-versleuteling [xmlenc-core], conform ebMS2.0.

Voor alle profielen gelden de volgende eigenschappen:

- 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 bij gebruik van security op berichtniveau.)
- Voor End-to-End Security, door middel van signing (ondertekening) en (optioneel) encryptie (versleuteling) op bericht-niveau in combinatie met (point-to-point) twee-zijdig TLS in het HTTP kanaal.
- De berichtenuitwisseling is *in principe* asynchroon: een business request wordt in een eigen synchrone HTTP request/response sessie verzonden, terwijl de acknowledgement en optionele business response via een separaat HTTP request/response sessie verzonden worden. In bepaalde gevallen (zie 4.4) mag een acknowledgement of een error synchroon verstuurd worden, Business*responses* worden altijd asynchroon, in een separaat HTTP sessie verzonden.

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

Profile Names	Transport characteristics					
Digikoppeling ebMS2	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.	√	—
	Reliable – Signed	osb-rm-s	√	√	√	—
	Best Effort – Encrypted	osb-be-e	√	n.a.	√	√
	Reliable – Encrypted	osb-rm-e	√	√	√	√

n.a. = Not applicable.

Met betrekking tot CPA-creatie: zie hoofdstuk todo 5.1 Deployment and processing and requirements for CPAs.

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 informatieverspreiding 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 (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 beschreven in het [Digikoppeling Beveiligingsdocument].

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 [EBXML-MSG].

3. Profiling the Modules of ebMS 2.0 §

3.1 Core Modules §

3.1.1 Core Extension Elements [ebMS 2.0] Section 3 §

Profile(s)	Usage: required/optional/never used in this profile
Best effort **Reliable Messaging** **End-to-End Security**	Support is **required**.

3.1.2 Security Module [ebMS 2.0] Section 4.1 §

Profile(s)	Usage: required/optional/never used in this profile
Best effort, **Reliable Messaging**, **End-to-End Security**	The Security Module is **required** in this profile. Security profile 3 [EBXML-MSG]/Appendix C **must be used**: "Sending MSH authenticates and both MSH's negotiate a secure char transmit data". The HTTPS connection uses encryption to provide in transit confidentiality of the complete ebXML message and per certificate-based Client and Server authentication during the TLS handshake.
End-to-End Security	Security profile 8 [EBXML-MSG]/Appendix C **must be used**: "Sending MSH applies XML/DSIG structures to message and passes communications channel. Sending MSH applies XML/DSIG structures to message and Receiving MSH returns a signed receipt."

3.1.3 SyncReply Module [ebMS 2.0] Section 4.3 §

Profile(s)	Usage: required/optional/never used in this profile	Notes
Best effort	**Never used** in this profile	(empty)
Reliable Messaging	**Optional used** in this profile. All messages, including acknowledgments and error messages, are sent asynchronously, with the exception of cases as described in par 4.4.1. Only in specific cases can MSH signals (acknowledgements, errors) sent synchronously. See 4.4.1 for conditions.	Asynchronous messaging does not preclude fast response times, as is to support interactive applications. Asynchronous messaging supports levels of scalability and supports scenarios where a response messag sent minutes, hours or days after the initial request message. Asynchr messaging may be combined transparently with store-and-forward inte
End-to-End Security	**Optional used** in this profile. See profile Best Effort or profile Reliable Messaging for details	(empty)

3.2 Additional Modules §

3.2.1 Reliable Messaging Module [ebMS 2.0] Section 6 §

Profile(s)	Usage: required/optional/never used in this profile	Notes
Best effort	**Never used** in this profile.	The ebXML reliable messaging protocol is not used. Acknowledgment Messages must not be sen requested, and the receiver should not eliminate duplicate messages.
Reliable Messaging	**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.	In this profile the FromParty MSH (message origination) must request, and the ToParty MSH (mes destination) must send an acknowledgment message. The ToParty MSH must also filter any dupli messages based on ebXML MessageId. Any intermediate NextMSH ebXML-aware nodes (see ca section 'Multi-Hop Module' in this chapter) have no reliable messaging functionality. Acknowledgm messages must not be consumed by any such intermediary but routed like any ebXML Message t original (true) sender.
End-to-End Security	**Optional used** in this profile. See profile Best Effort or profile Reliable Messaging for details.	(empty)

3.2.2 Message Status Service [ebMS 2.0] Section 7 §

Profile(s)	Usage: required/optional/never used in this profile	No
Best effort, **Reliable Messaging**, **End-to-End Security**	**Optional**. Message Status Service is not required in these profiles.	(e

3.2.3 Ping Service [ebMS 2.0] Section 8 §

Profile(s)	Usage: required/optional/never used in this profile	Notes
Best effort, **Reliable Messaging**, **End-to-End Security**	Ping Service is **not required** in these profiles.	(emp

3.2.4 Message Order [ebMS 2.0] Section 9 §

Profile(s)	Usage: required/optional/never used in this profile	Notes
Best effort, **Reliable Messaging**, **End-to-End Security**	**Optional**. Message Order is *strongly discouraged* in these profiles.	Many organisations use message handlers that do not support this functionality. Therefore, it can only be communicating parties agree to this option in advance. This specification is limited to message service h order functionality and does not preclude application-level in-order processing if sequence information is provided at the business document level.

3.2.5 Multi-Hop Module [ebMS 2.0] Section 10 §

Profile(s)	Usage: required/optional/never used in this profile	Notes
Best effort, **Reliable Messaging**, **End-to-End Security**	**Never used** in this profile.	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 MS endpoint. This node is called an Intermediary.

4. Communication Protocol Bindings §

4.1 Profile Requirement Item: Transport Protocol §

[EBXML-MSG] Appendix B	Best effort, Reliable Messaging, End-to-End Security
Is *HTTP* a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.)	**Never used** in this profile. HTTPS instead.
Is HTTP a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.	HTTPS is the **required** transport
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 pr
If SMTP, What is needed in addition to the ebMS minimum requirements for SMTP?	**Not applicable**
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	(empty)
Test References	(empty)
Notes	(empty)

5. Profile Requirements Details §

5.1 Module: Core Extension Elements §

5.1.1 Profile Requirement Item: PartyId §

[EBXML-MSG] Section 3.1.1.1	All profiles: Best effort, Reliable Messaging, End-to-End Security

PartyId Element	Header elements:
	`SOAP:Header/eb:MessageHeader/eb:From/eb:PartyI`
	`SOAP:Header/eb:MessageHeader/eb:To/eb:PartyId`

[EBXML-MSG] Section 3.1.1.1	All profiles: Best effort, Reliable Messaging, End-to-End Security
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 **mus** **OIN** (Organisatie Identificatie Nummer) for identification. P who are already using ebMS and are using other identifica schemes are allowed to use their identification: the type at must identify their identification scheme and must be differ urn:osb:oin. The use of their own identification should be t the partner should start using OIN at a certain moment for identification using Digikoppeling. For non-production envi suffix is allowed after the OIN to distinguish it from product "_OTA" or "_T") **OIN** stands for Organisatie Identificatie Nummer and is ma Logius in the *COR (Centrale OIN Raadpleegvoorziening)*. number is unique and allows identification of partners, eve are not themselves legal entities, but departments or units organizations. The OIN used for PartyId must be the same as the OIN fro party and should not contain the OIN from an intermediate case the end-party is the same party that performs TLS, si and/or encryption the OIN used for PartyId should be ident OIN used for the TLS-, signing- and/or encryption-certifica respectively. Hence, if the end-party does not perform TLS and/or encryption the corresponding OIN's may differ.
Should multiple PartyId elements be present in From and To elements?	(empty)
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 f The following type attribute value has to be used in case o used by the partner: **urn:osb:oin**
alignment	appears as PartyId element in CPA. (c) appears as PartyId/@type in CPA
Test References	(empty)
notes	ISO 6523 is an international standard registry of agencies codes. Value 0106 in this registry identifies the Associatior Chambers of Commerce and Industry in the Netherlands. urn:oasis:names:tc:ebxml-cppa:PartyId-type is used to ind issuing agency is an ISO 6523 registered agency. The typ allows unique identification of the agency that issues the n code that identifies the partner. In theory, this mechanism multiple identification systems to be used in parallel, with r requirement that the codes in those systems do not overla

5.1.2 Profile Requirement Item: Role §

[EBXML-MSG] Section 3.1.1.2 Role Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	/SOAP:Header/eb:MessageHeader/eb:From/eb:Role /SOAP:Header/eb:MessageHeader/eb:To/eb:Role
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. Withi contract (CPA) between two Partners: - A Partner **must** fulfill one and only o Partner cannot change its role within one contract). - A Partner can send me (one or more) and/or receive messages (one or more). In case a Partner wa different roles, different contracts (CPA's) must be used.
Alignment	[Per-process; may reference Role values in BPSS [BPSS] definitions. Appea Role/@name in CPA.]
Test References	(empty)
Notes	(empty)

5.1.3 Profile Requirement Item: CPAId §

[EBXML-MSG] Section 3.1.2 CPAId Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	/SOAP:Header/eb:MessageHeader
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 recomme good practice.
Alignment	Appears as CollaborationProtocolAgreement/@c CPA.
Test References	(empty)
Notes	(empty)

5.1.4 Profile Requirement Item: ConversationId §

[EBXML-MSG] Section 3.1.3 ConversationId Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	/SOAP:Header/eb:MessageHeader/eb:Conve
What is the user definition of a Conversation? What is the business criterion used to correlate messages considered parts of the same conversation?	[EBXML-MSG] requires that request messages, messages, and any acknowledgments and error have the same value for ConversationId.
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.
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 scope for Digikoppeling.
Test References	(empty)
Notes	ConversationId is a required ebXML message h element.

5.1.5 Profile Requirement Item: MessageId §

[EBXML-MSG] Section 3.1.6.1	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	/SOAP:Header/eb:MessageHeader/eb:MessageData/eb:
Although there is no requirement for an MSH to give control about 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 when the ID is generated?	No recommendation made. The value of MessageId does no meet any requirements beyond the string format specified in MSG] and the global uniqueness constraint of [rfc5322].
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.1.6 Profile Requirement Item: Service §

[EBXML-MSG] Section 3.1.4 Service Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	/SOAP:Header/eb:MessageHeader/eb:Servi /SOAP:Header/eb:MessageHeader/eb:Servi

[EBXML-MSG] Section 3.1.4 Service Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
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.
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 n** white space.
Alignment	Appears as Service element in CPA Appears as Service/@type in CPA
Test References	(empty)
Notes	(empty)

5.1.7 Profile Requirement Item: Action §

[EBXML-MSG] Section 3.1.5 Action Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	`/SOAP:Header/eb:MessageHeader/`
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/@ CPA.]
Test References	(empty)
Notes	The text content of the Action element header **must not** contain white space.

5.1.8 Profile Requirement Item: Timestamp (removed) §

This item is no longer required.

5.1.9 Profile Requirement Item: Description §

[EBXML-MSG] Section 3.1.8 Description Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	`/SOAP:Header/eb:MessageHeader/eb:Description`
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 require Message handlers **may** ignore Description elements.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.1.10 Profile Requirement Item: Manifest §

[EBXML-MSG] Section 3.2.2 Manifest Validation	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	`/SOAP:Body/eb:Manifest`
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 payl are included in the ebXML message as a MIME part allows for references message payloads (for instance, using HTTP URIs), which are logically pa message, but not as a physical entity in the MIME envelope. This is **never** these profiles.

[EBXML-MSG] Section 3.2.2 Manifest Validation	All profiles: Best effort, Reliable Messaging, End-to-End Security
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
Alignment	(empty)
Test References	(empty)
Notes	XML or other business documents can have references to other resources not part of the ebXML message. It is up to the receiving application to inter such references.

5.1.11 Profile Requirement Item: Reference §

[EBXML-MSG] Section 3.2.1 Reference Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`/SOAP:Body/eb:Manifest/eb:Reference`
Is the xlink:role attribute required? What is its value?	**Not applicable**. The xlink:role attribute is not required.
Are any other namespace-qualified attributes required?	**Not applicable**. No other namespace-qualified attributes are allowed.
Alignment	(empty)
Test References	(empty)
Notes	Only the Content Id reference mechanism [rfc2392] is allowed.

5.1.12 Profile Requirement Item: Reference/Schema §

[EBXML-MSG]	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`/SOAP:Body/eb:Manifest/eb:Reference/eb:Schema`
Are there any Schema elements required? If so, what are their location and version attributes?	Schema elements are not required. Digikoppeling does not perfo schema validation.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.1.13 Profile Requirement Item: Reference/Description §

[EBXML-MSG] Section 3.2.1.2 Description Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`/SOAP:Body/eb:Manifest/eb:Reference/eb:Description`
Are any Description elements required? If so, what are their contents?	Description elements are optional. They **may** be ignored by any receiving mess handler.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.2 Module: Security §

5.2.1 Profile Requirement Item: Signature generation §

[EBXML-MSG] Section 4.1.4.1 Persistent Digital Signature	Best effort Reliable Messaging	End-to-End Security

[EBXML-MSG] Section 4.1.4.1 Persistent Digital Signature	Best effort Reliable Messaging	End-to-End Security
Header elements: SOAP:Header/Signature		
(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.
Are additional Signature elements required, by whom, and what should they reference?	**Not applicable**.	**Never used** in this profile
What canonicalization method(s) must be applied to the data to be signed?	**Not applicable**.	The use of XML canonica **required**. [xml-exc-c14n]
What canonicalization method(s) must be applied to each payload object, if different from above?	**Not applicable**.	**Not applicable**.
What signature method(s) must be applied?	**Not applicable**.	The applied signature me described in [Digikoppelin Beveiligingsdocument]
What Certificate Authorities (issuers) are allowed or required for signing certificates?	**Not applicable**.	The use of PKI Overheid is **required** in which an O in the Subject.serialNumb [Digikoppeling Beveiligingsdocument]
Are direct-trusted (or self-signed) signing certificates allowed?	**Not applicable**.	This profile is **never used** used in testing and Proof environments
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.	The requirements as state PKIOverheid [PKI Policy] used. The use of certificat revocation lists (CRL) fror trusted CA's is required.
Alignment	(a) Appears as BusinessTransactionCharacteristics/@isAuthenticated=persistent and BusinessTransactionCharacteristics/@isTamperProof=persistent in CPA	
Test References	(empty)	(empty)
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 Digikoppeling is not aware of the presence of signatures and does not perform signature verification.	for more information see [Digikoppeling Beveiligingsdocument]

5.2.2 Profile Requirement Item: Persistent Signed Receipt §

[EBXML-MSG] Section 4.1.4.2 Persistent Signed Receipt	Best effort Reliable Messaging	End-to-E Security
Header elements: `/SOAP:Header/eb:Signature`		
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 acknowl is **requi**
If so, what is the Acknowledgment or Receipt schema?	**Not applicable**.	[xmldsig 200202
Alignment	Appears as BusinessTransactionCharacteristics/@isNonRepudiationReceiptRequired=persistent in CPA.	
Test References	(empty)	(empty)
Notes	(empty)	(empty)

[EBXML-MSG] Section 4.1.4.2 Persistent Signed Receipt	Best effort Reliable Messaging	End-to-E Security

5.2.3 Profile Requirement Item: Non Persistent Authentication §

[EBXML-MSG]Section 4.1.4.3 Non Persistent Authentication	All profiles: Best effort, Reliable Messaging, End-to-End Security
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. The currently allowed pr versions for TLS are described in the [Digikoppeling Beveiligingsdocument] `Note:` Message handlers **should NOT** be able to operate in SSL v3 backward compatibility mode.
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthenticated=transient in CPA.]
Test References	(empty)
Notes	for more information see [Digikoppeling Beveiligingsdocument]

5.2.4 Profile Requirement Item: Non Persistent Integrity §

[EBXML-MSG] Section 4.1.4.4 Non Persistent Integrity	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`/SOAP:Header/eb:Signature`
Are communication channel integrity methods required? [Yes, for Security Services Profile 4.] Which methods are allowed or required?	**Not applicable**
Alignment	[Appears as BusinessTransactionCharacteristics/@isTamperproo in CPA.]
Test References	(empty)
Notes	(empty)

5.2.5 Profile Requirement Item: Persistent Confidentiality §

[EBXML-MSG] Section 4.1.4.1 Section 4.1.4.5 Persistent Confidentiality	Best effort Reliable Messaging	E S
Header elements: `/SOAP:Header/eb:Signature`		
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**.	
Alignment	[Appears as BusinessTransactionCharacteristics/@isConfidential=persistent in CPA.]	
Test References	(empty)	
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.	

5.2.6 Profile Requirement Item: Non Persistent Confidentiality §

[EBXML-MSG] Section 4.1.4.6 Non Persistent Confidentiality	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`/SOAP:Header/eb:Signature`
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 and TLS is required. The currently allowed protocol versions described in the [Digikoppeling Beveiligingsdocument] Message service handlers **NOT** support SSL v3 compatibility mode.
Alignment	[Appears as BusinessTransactionCharacteristics/@isConfidential=transient in CP
Test References	(empty)
Notes	For more information see [Digikoppeling Beveiligingsdocument]

5.2.7 Profile Requirement Item: Persistent Authorization §

[EBXML-MSG] Section 4.1.4.7 Persistent Authorization	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	/SOAP:Header/eb:Signature
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 in CPA.]
Test References	(empty)
Notes	(empty)

5.2.8 Profile Requirement Item: Non Persistent Authorization §

[EBXML-MSG] Section 4.1.4.8 Non Persistent Authorization	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	/SOAP:Header/eb:Signature
Are communication channel authorization methods required? [Yes, for Security Services Profile 2.] Which methods are allowed or required?	TLS client and server authentication is **required** as described in 4.2.3.
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequire in CPA.]
Test References	(empty)
Notes	(empty)

5.2.9 Profile Requirement Item: Trusted Timestamp §

[EBXML-MSG] Section 4.1.4.9 Trusted Timestamp	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	/SOAP:Header/eb:Signature
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	(empty)
Test References	(empty)
Notes	Applications submitting data to, or receiving data from, Digikoppeling message handlers can perform times The ebXML Messaging protocol is payload-neutral and therefore supports timestamped payloads. Howeve timestamping functionality is not part of the Digikoppeling functionality. Any valid ebXML Message must co eb:TimeStamp as part of the eb:MessageData.

5.3 Module : Error Handling §

5.3.1 Profile Requirement Item §

[EBXML-MSG] Section 4.2.3.2 Error Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	/SOAP:Header/eb:ErrorList/eb:Error /SOAP:Header/eb:ErrorList/ eb:Error/\@codeContext /SOAP:Header/eb:ErrorList/ eb:Error/\@errorCode
Is an alternative codeContext used? If so, specify	**Not applicable**

[EBXML-MSG] Section 4.2.3.2 Error Element	All profiles: Best effort, Reliable Messaging, End-to-End Security
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 mechanism or a proactive callback)?
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.4 Module : SyncReply §

5.4.1 Profile Requirement Item: SyncReply §

[EBXML-MSG] Section 4.3 SyncReply	Best effort	Reliable Messaging	E S
Header elements: `SOAP:Header/eb:SyncReply`			
Is SyncReply mode allowed, disallowed, or required, and under what circumstances? [May be process-specific.]	**Not applicable**.	SyncReply is restricted to **none** (default) or **mshSignalsOnly** (on condition) Condition for usage of msghSignalsOnly mode is: both parties MSH are able to activate syncReplyMode=msghSignalsOnly see also [Best Practice]	S E o R M fo
If SyncReply mode is used, are MSH signals, business messages or both expected synchronously?	**Not applicable**	If SyncReply mode used only MSH signals are expected synchronously	S R M fo
Alignment	[Affects setting of 6.4.7 syncReplyMode element. Appears as MessagingCharacteristics/@syncReplyMode in CPA.]		
Test References	(empty)		
Notes		Asynchronous messaging does not preclude support of a “near real time” response quality of service required for e.g. interactive applications. The ebXML MessageId and RefTo MessageId header elements encode correlation of request and response messages.	

5.5 Module : Reliable Messaging §

5.5.1 Profile Requirement Item: SOAP Actor attribute §

[EBXML-MSG] Section 6.3.1.1 SOAP Actor attribute	Best effort	Reliable Messaging	End-to-E
Header elements: /SOAP:Header/eb:AckRequested/			
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**.	**Not applicable**	**Not appl**
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.	**Optiona** profiles E or Reliab Messagi details.
Test References	(empty)		
Notes	(empty)		

5.5.2 Profile Requirement Item: Signed attribute §

[EBXML-MSG] Section 6.3.1.2 Signed attribute	All profiles: Best effort Reliable Messaging	End-to-E Security
Header elements: /SOAP:Header/eb:AckRequested/		
Must MSH Acknowledgments be (requested to be) signed?	**Not applicable**.	**Not app**
Alignment	[Appears as MessagingCharacteristics/ @ackSignatureRequested in CPA.]	
Test References	(empty)	
Notes	(empty)	

5.5.3 Profile Requirement Item: DuplicateElimination §

[EBXML-MSG] Section 6.4.1	Best effort	Reliable Messaging	End-to-End Security
Header elements: /SOAP:Header/eb:AckRequested/			
Is elimination of duplicate messages required? [Yes, for RM Combinations 1-4.]	Duplicate Elimination is **never used**.	Duplicate Elimination is **required**	Duplicate Elimination is optional. See pro Effort or Reliable Messaging for details.
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?	(empty)	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. The minimum is (1+Retries)*RetryInterval.	(empty)
Alignment	Appears as MessagingCharacteristics/ @duplicateElimination in CPA		
Test References	(empty)		
Notes			Message ID's in ebXML are based on [rfc must therefore be globally unique, which prevents accidental re-use of ID's for dist messages. Factors like system load, disk database table limitations, period mainter schedules **may** be used in message purg policies. Cleaning message ID stores ofte (temporarily) affects responsiveness of a

5.5.4 Profile Requirement Item: Retries and RetryInterval §

[EBXML-MSG]Section 6.4.3, 6.4.4 Retries and RetryInterval	Best effort	Reliable Messaging	E S
Header elements: /SOAP:Header/eb:AckRequested/			
(a) If reliable messaging is used, how many times must an MSH attempt to redeliver an unacknowledged message? (b) What is the minimum time a Sending MSH should wait between retries of 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.	
Alignment	(a) [Appears as ReliableMessaging/Retries in CPA.] (b) [Appears as ReliableMessaging/RetryInterval in CPA.]		
Test References	(empty)		

[EBXML-MSG]Section 6.4.3, 6.4.4 Retries and RetryInterval	Best effort	Reliable Messaging	E S
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.	

5.5.5 Profile Requirement Item: PersistDuration §

[EBXML-MSG]Section 6.4.6 PersistDuration	Best effort	Reliable Messaging	End- Secu
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.	Dep the effo relia mes
Alignment	[Appears as ReliableMessaging/PersistDuration in CPA.]		
Test References	(empty)		
Notes	(empty)		

5.5.6 Profile Requirement Item: Reliability Protocol §

[EBXML-MSG]Section 6.5.3, 6.5.7	Best effort	Reliable Messaging	End-to-End S
Usage: required/optional/never used in this profile, Profiled: yes / no	**Never** used in this profile.	The Reliable Messaging Protocol in [EBXML-MSG] must be used.	**Optional** in t depends on best effort or messaging.
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.	
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	(empty)		
Test References	(empty)		
Notes	(empty)		

5.6 Module : Message Status §

5.6.1 Profile Requirement Item: Status Request message §

[EBXML-MSG] Section 7.1.1 Message Status Request	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`Eb:MessageHeader/eb:Stat`
If used, must Message Status Request Messages be digitally signed?	**Not applicable**.
Must unauthorized Message Status Request messages be ignored, rather than responded to, due to security concerns?	**Not applicable**.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.6.2 Profile Requirement Item: Status Response message §

[EBXML-MSG] Section 7.1.2 Message Status Response	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`Eb:MessageHeader/eb:StatusResponse`
If used, must Message Status Response Messages be digitally signed?	**Not applicable**.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.7 Module : Ping Service §

5.7.1 Profile Requirement Item: Ping-Pong Security §

[EBXML-MSG] Section 8.1, 8.2 Message Service Handler Ping/Pong Message	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`Eb:MessageHeader/eb:Service`
If used, must Ping Messages be digitally signed?	If Ping-Pong is used, it is **optional** for Ping n to be digitally signed.
If used, must Pong Messages be digitally signed?	If Ping-Pong is used, it is **optional** for Pong r to be digitally signed.
Under what circumstances must a Pong Message not be sent?	No recommendation made.
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	(empty)
Test References	(empty)
Notes	(empty)

5.8 Module : Multi-Hop §

5.8.1 Profile Requirement Item: Use of intermediaries §

[EBXML-MSG] Section 10	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	
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 l **may** treat any exceptions as failures. They are **not required** to support any forwarding of ebXML Messages to other business parti
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-er message delivery. Message handlers **must not** request nextMSH receipt acknowledgments and such requests **should** be ignored ebXML intermediary. The ebXML intermediaries also **should not** filter duplicate messages. As with business messages, any Digik level ebXML intermediaries **should** attempt to forward end-to-end receipts and errors.
Alignment	(empty)
Test References	(empty)

[EBXML-MSG] Section 10	All profiles: Best effort, Reliable Messaging, End-to-End Security
Notes	In case **Best Effort** is used: Any Digikoppeling-level ebXML intermediary may support transport retries, for instance to handle temp or HTTP transport level errors. This is not required. In case **Reliable messaging** is used: This profile uses end-to-end reliable mes This allows the Digikoppeling to recover from any temporary processing failures at the level of intermediaries. Upcoming versions o Digikoppeling **may** support store and forward ebXML intermediaries at an infrastructure level. The functionality of these intermediar be limited to fully transparent, asynchronous store-and-forward routing of ebXML Messages, with the exception of cases as describ 4.4.1. In the default asynchronous case, no special processing is required of endpoints in the presence of any such intermediaries, compared to direct point-to-point connections, other than supporting connection to/from the URL and client and server TLS authent details for the intermediary rather than the “true” sender/recipient. In case **End-to-End Security** is used: see the notes for Best effo Reliable messaging.

5.8.2 Profile Requirement Item: Acknowledgements §

[EBXML-MSG] Section 10.1.1, 10.1.3	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header element(s)	`Eb:MessageHeader/`
Must each intermediary request acknowledgment from the next MSH?	**Not applicable**. There is **no support** for eb MSH acknowledgments.
Must each intermediary return an Intermediate Acknowledgment Message synchronously?	**Not applicable**. There is **no support** for eb MSH acknowledgments.
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 eb MSH acknowledgments.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.9 SOAP Extensions §

5.9.1 Profile Requirement Item: #wildCard, Id §

[EBXML-MSG] Section 2.3.6, 2.3.7, 2.3.8	All profiles: Best effort, Reliable Messaging, End-to-End Security
(Section 2.3.6) #wildcard Element Content: Are additional namespace-qualified extension elements required? If so, specify.	**Not applicable**. No additional namespace-qualified extension elem required. The toPartyMSH and any intermediaries **must** ignore any elements.
(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.**
(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 [EBXMI
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.10 MIME Header Container §

5.10.1 Profile Requirement Item: charset §

[EBXML-MSG] Section 2.1.3.2	All pro Best e Reliab Messa End-t Secur

[EBXML-MSG] Section 2.1.3.2	All pro Best e Reliab Messa End-to Secur
MIME Header elements	Conte
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	(empt
Test References	(empt
Notes	(empt

5.11 HTTP Binding §

5.11.1 Profile Requirement Item: HTTP Headers §

[EBXML-MSG] Appendix B.2.2 Sending ebXML Service messages over HTTP	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	MIME parts
Is a (non-identity) content-transfer-encoding required for any of the MIME multipart entities?	Content transfer encoding **should not** be used.
If other than "ebXML" what must the SOAPAction HTTP header field contain?	The value of the SOAPAction HTTP header field MUST be “ebXML”
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 e **should** ignore any such additional HTTP header.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.11.2 Profile Requirement Item: HTTP Response Codes §

[EBXML-MSG] Appendix B.2.3 HTTP Response Codes	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	MIME parts
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 i An HTTP 503 error code **should** be treated as a recoverable error (i.e. **should not** terminate any reliable mes retries). Codes in the 3xx and 4xx ranges **must** be interpreted as errors.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.11.3 Profile Requirement Item: HTTP Access Control §

[EBXML-MSG] Appendix B.2.6 Access Control Header elements	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	MIME parts
Which HTTP access control mechanism(s) are required or allowed? [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.	Access control is based on client certificate i only. HTTP Basic or Digest authentication ar **supported**.
Alignment	Appears as AccessAuthentication elements i
Test References	(empty)
Notes	(empty)

5.11.4 Profile Requirement Item: HTTP Confidentiality and Security §

[EBXML-MSG] Appendix B.2.7 Confidentiality and Transport Protocol Level Security	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	MIME parts
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 is based on HTTPS and TLS. The currently allowed protocol versions for T described in the [Digikoppeling Beveiligingsdocument] Note: TLS implementations **mu** support SSL v3 backwards compatiblity mode.
What encryption algorithm(s) and minimum key lengths are required?	The currently allowed protocol versions for TLS are described in the [Digikoppeling Beveiligingsdocument]
What Certificate Authorities are acceptable for server certificate authentication?	PKI overheid maintains a list of approved trusted service providers [PKI CA].
Are direct-trust (self-signed) server certificates allowed?	Self-signed certificates are only allowed in test cases.
Is client-side certificate-based authentication allowed or required?	Client-side authentication is required.
What client Certificate Authorities are acceptable?	PKI overheid maintains a list of approved trusted service providers [PKI CA].
What certificate verification policies and procedures must be followed?	PKI overheid procedures are described in [PKI Policy]. The use of certificate revocatio (CRL) from the trusted CA's is required.
Alignment	(empty)
Test References	(empty)
Notes	For more information see [Digikoppeling Beveiligingsdocument]

5.12 SMTP Binding §

5.12.1 Profile Requirement Item: MIME Headers §

[EBXML-MSG] Appendix B.3.2 Sending ebXML Messages over SMTP	All profiles: Best effort, Reliable Messaging, End-to-End Security
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 s the HTTP transport protocol.
If other than "ebXML" what must the SOAPAction SMTP header field contain?	**Not applicable**. This specification only s the HTTP transport protocol.
What additional MIME headers must be included amongst the SMTP headers?	**Not applicable**. This specification only s the HTTP transport protocol.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

5.13 Profile Requirement Item: SMTP Confidentiality and Security §

[EBXML-MSG] Appendix B.3.4, B.3.5	All profiles: Best effort, Reliable Messaging, End-to-End Security
Header elements	MIME parts
What SMTP access control mechanisms are required? [Refer to item 4.1.4.8 in Security section.]	**Not applicable**. This specification only supports transport protocol.
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 transport protocol.
Alignment	(empty)
Test References	(empty)
Notes	(empty)

6. 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.

6.1 Deployment and Processing requirements for CPAs §

	All profiles: 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 "CPA Register" facility. A web-based program is available by which CPA's are creat stored. See https://cparegister.minvenj.nl/logius See http://www.logius.nl/digikoppeling/documentatie for information abou Creation facility (document is written in Dutch). In addition to this there is a **Best Practices** document with information abo 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 us and) the same default channel for sending acknowledgements. This default channel can only support **one specific profil** CPA (for instance either osb-rm-s or osb-rm, not both within one CPA). As a result, when there are actions which are bas different profiles (for instance osb-rm-s and osb-be) and the profiles for the acknowledgements are different as well (for in osb-rm-s and osb-be), multiple CPA's must be created.

6.2 Security Profile §

	All profiles: 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 negotiate a secure channel to transmit data" **must be** applied. The HTTPS conne encryption to provide in transit confidentiality regarding the complete ebXML mes performs **both** certificate-based Client and Server authentication during the TLS h
(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	(empty)

6.3 Reliability Profile §

	All p Best Relia Mes End- Secu
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 app**
Which Reliable Messaging feature combinations are required? [Refer to Section 6.6 of Message Service Specification.]	
Others	

6.4 Error Handling Profile §

[EBXML-MSG] Section 4.2.4.2	All pr Best e Reliab Messa End-t Secur
(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 recon 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?	Pend
(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?]	Pend
Others	

6.5 Message Payload and Flow Profile §

	All profiles: 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 payloa than a (single digit) megabyte in size. Some partners may need to bridge incoming ebXI Message flows to other (enterprise) messaging protocols which have message size limit 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 may contain one or more payload containers
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?	Each payload container will get a MIME type reflecting the type of the 'content' it contair
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	

6.6 Additional Messaging Features beyond ebMS Specification §

	All profil Best effo Reliable End-to-E
Are there additional features out of specification scope, whichare part of this messaging profile, as an extension to the ebMS profiling?	No.

6.7 Additional Deployment or Operational Requirements §

	All profiles: Best effort, Reliable Messa End-to-End Sec
Operational or deployment aspects which are object to further requirements or recommendations.	Pending.

7. Conformiteit §

Naast onderdelen die als niet normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet normatief. Verder is alles in dit document normatief.

8. Lijst met figuren §

A. Referenties §

A.1 Normatieve referenties §

[Digikoppeling Architectuur]
Digikoppeling Architectuur. Logius Centrum voor standaarden. Logius. december 2020. URL: https://centrumvoorstandaarden.github.io/Architectuur2.0-metRestfulAPI/static.html

[Digikoppeling Beveiligingsdocument]
Digikoppeling Beveiligingsstandaarden en voorschriften. Logius. 2020. URL: https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.3.pdf

[EBXML-MSG]
OASIS ebXML Message Service Specification. Ian Jones; Brian Gibb; David Fischer. 1 April 2002. URL: https://www.oasis-open.org/committees/download.php/272/ebMS_v2_0.pdf

[PKI CA]
Toegetreden vertrouwensdienstverleners. Logius. URL: https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/toegetreden-vertrouwensdienstverleners

[PKI Policy]
Programma van Eisen (PKIoverheid). Logius. URL: https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen

[rfc2392]
Content-ID and Message-ID Uniform Resource Locators. E. Levinson. IETF. August 1998. Proposed Standard. URL: https://tools.ietf.org/html/rfc2392

[rfc5322]
Internet Message Format. P. Resnick, Ed.. IETF. October 2008. Draft Standard. URL: https://tools.ietf.org/html/rfc5322

[SOAP]
SOAP Specifications. W3C. 8 May 2000. W3C Note. URL: https://www.w3.org/TR/SOAP/

[xml-exc-c14n]
Exclusive XML Canonicalization Version 1.0. John Boyer; Donald Eastlake; Joseph Reagle. W3C. 18 July 2002. W3C Recommendation. URL: https://www.w3.org/TR/xml-exc-c14n/

[xmldsig-core-20020212]
XML-Signature Syntax and Processing. Donald Eastlake; Joseph Reagle; David Solo et al. W3C. 12 February 2002. W3C Recommendation. URL: https://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[xmlenc-core]
XML Encryption Syntax and Processing. Donald Eastlake; Joseph Reagle. W3C. 10 December 2002. W3C Recommendation. URL: https://www.w3.org/TR/xmlenc-core/

A.2 Informatieve referenties §

[Deployment Guide 1.1]
Deployment Profile Template For OASIS ebXML Message Service 2.0 Pete Wenzel; Jacques Durand. OASIS. June 2005. URL: http://www.oasis-open.org/apps/org/workgroup/ebxml-iic-deployment-profile-template-intro-100406.doc

[ebMS3]
Collaboration-Protocol Profile and Agreement Specification Version 2.0. Ian Jones; Pete Wenzel. Oasis. October 2007. URL: https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.html

[UMMR10]
UMM Revision 10. . UN/CEFACT. 2001. URL: https://unece.org/DAM/cefact/umm/UMM_Revision_10_2001.zip

[UMMUG]
UN/CEFACT Modeling Methodology (UMM) User Guide. . UN/CEFACT. 2003. URL: www.unece.org/fileadmin/DAM/cefact/umm/UMM_userguide_220606.pdf