FS-20071003.05Ce

OSB Versie 1
OSB Koppelvlak Standaard ebMS

Datum: **5 september 2007**
DocumentVersie: **0.91**

OVERHEIDSSERVICEBUS

Documentbeheer

Documenthistorie

datum	versie	auteur	opmerking
11-02-2007	WD1	P. van der Eijk	Working draft 1 of version 1.0 of OSB profiles for ebXML Messaging 2.0.
13-02-2007	WD2	A. Kappe	Minor edits
5-03-2007	WD3	P. van der Eijk	Comments Paul Schlotter; formatting.
19-03-2007	WD4	P. van der Eijk	PartyId section adapted based on comments Freddy Keij
25-3-2007	WD5	P. van der Eijk	Review 21/3/2007 comments.
28 Juni 2007	0.91	E.J. van Nigtevecht	Aangepast aan OSB template
25 Juli 2007	0.91	E.J. van Nigtevecht	Opmerkingen Paul verwerkt

Goedkeuring

datum	versie	goedgekeurd door	opmerking

OVERHEIDSSERVICEBUS

Inhoudsopgave

1 Inleiding

1.1 Doel en Doelgroep

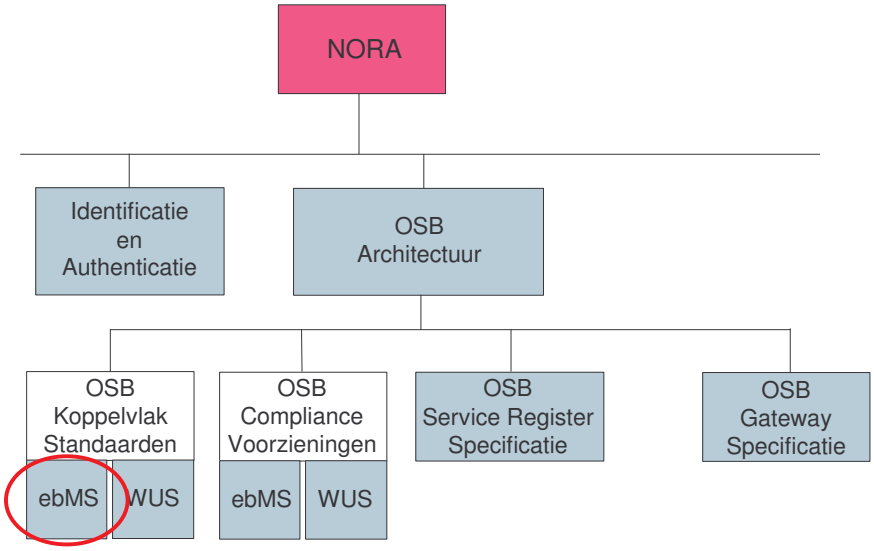
Dit document beschrijft de functionele specificaties voor de OSB ebMS Deployment Profile, onderdeel van OSB 1.0.

Het document is bestemd voor

- Architecten en ontwikkelaars die op basis van ebMS gegeven willen uitwisselen via de OSB.

1.2 Opbouw OSB documentatie

De OSB is beschreven in een set van documenten. Deze set is als volgt opgebouwd.



Dit document beschrijft de ebMS Koppelvlak Standaard.

OVERHEIDSSERVICEBUS

1.3 De OverheidsServiceBus OSB

Deze paragraaf bevat zeer beknopt een aantal hoofdpunten uit de overige documentatie.

Doel en scope van de OSB
De Overheidsservicebus biedt de mogelijkheid om op een sterk gestandaardiseerde wijze berichten uit te wisselen tussen serviceaanbieders (Service Providers) en serviceafnemers (Service Requesters of Consumers).

De uitwisseling tussen Service providers en Requesters 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, waardebereiken etc.
De OSB houdt zich niet met de inhoud bezig, “geen boodschap aan de boodschap”.

Logistiek: Op deze laag bevinden zich de afspraken en voorzieningen van de OSB.

Transport: deze laag verzorgt het daadwerkelijke transport van het bericht.

De OSB afspraken op de logistieke laag betreffen transportprotocollen (HTTP), messaging (SOAP), beveiliging en betrouwbaarheid. Deze afspraken landen in de koppelvlakstandaarden. De architectuur van de Gateway is beschreven in het document “Architectuur OSB”.

Leidend principe (requirement)
De koppelvlakstandaarden dienen te leiden tot een maximum aan interoperabiliteit met een minimum aan benodigde ontwikkelinspanning.
Daarom wordt gekozen voor bewezen interoperabele internationale standaarden.

De OSB maakt berichtenuitwisseling mogelijk op basis van de ebXML/ebMS en WUS families van standaarden incl. de daarbij behorende verwante standaarden.

Aan te sluiten overheidsorganisaties hebben aangegeven op een uniforme manier (één stekker) te willen aansluiten aan de OSB. Organisaties die beschikken over eigen middleware (ESB, broker) kunnen de aansluiting aan de OSB, de adapters, in het algemeen realiseren via voorzieningen in die middleware. Voor andere organisaties is afgesproken dat de OSB Gateway beschikbaar komt, die “intern”, d.w.z. naar de organisatie toe, die ene stekker biedt, gebaseerd op de protocollen WUS-lite en JMS, en extern, d.w.z. naar de OSB toe communiceren op basis van de OSB koppelvlakstandaarden.

1.4 Opbouw van dit document

Hoofdstuk 2 beschrijft de achtergrond en het gebruik van de ebMS Deployment Profile. Hoofdstuk 3 tot en met 5 beschrijft de parameters van het ebMS profiel zoals dat gekozen is voor de OSB.

OVERHEIDSSERVICEBUS

2 Inleiding

Dit document specificeert de Koppelvlakstandaard ebMS voor berichtenuitwisseling over de Overheids Service Bus (OSB) als een toepassing van de ISO 15000-2 standaard, de ebXML Message Service Specification versie 2.0 **[ISO 15000-2]**. De OSB is bedoeld als generieke infrastructuur voor een grote varieteit 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 de OSB. 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 van 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]**, al hebben sommige onderdelen van een deployment specificatie gevolgen voor de specifieke invulling van CPA elementen.

2.1 Doel van dit document

Het doel van dit document is om organisaties die gebruik willen maken van de OSB een formele basis te geven om ebXML Messaging software te configureren zodat berichten uitgewisseld kunnen worden.

Als op een bepaald onderdeel geen specifieke richtlijn is gegeven, is een van de volgende waarden aangegeven:

- **Not Applicable**. Dit is voor onderdelen die niet relevant zijn voor de OSB, 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 zoals beschreven in **[RFC2119]**.

2.2 Ondersteunde varianten

De ebXML Messaging 2.0 standaard waarop deze specificatie is gebaseerd biedt een hogere mate van configureerbaarheid dan in de praktijk wenselijk is. Om redenen van interoperabiliteit, eenvoud en overzichtelijkheid onderscheidt deze specificatie een tweetal 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 de OSB versie 1 zal moeten voldoen aan één van deze OSB 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 ontvangstbevestigingen en duplicaateliminatie door de ontvangende message handler. Dit profiel is onder meer geschikt voor alle berichtenstromen die leiden tot updates van gegevensverzamelingen.

In beide profielen wordt vertrouwelijkheid en authenticatie van zender en ontvanger gerealiseerd op transportniveau. Beide profielen maken gebruiken van HTTPS als transport kanaal, en beide profielen zijn asynchroon.

2.3 Bericht uitwisselpatronen

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 bedrijfstransactiepatronen). In het geval van tweewegsverkeer leggen de ebXML headervelden (*MessageId, RefToMessageId* 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 tweewegs uitwisseling) het teruggaande bericht kunnen naar keuze gebruik maken van het Best Effort profiel of het Reliable Messaging profiel.

2.4 Gerelateerd werk

Dit document bouwt voort op eerdere toepassingen van ebXML Messaging in de strafrechtketen, de keten openbare orde en veiligheid en de vreemdelingenketen en is verwant aan de Justitiestandaard Asynchroon Berichtenverkeer **[JAB 2.0]**.

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. Doordat in de loop der tijd kwetsbaarheden kunnen worden ontdekt in de cryptografische algorithmen 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

In this section, users will only specify which modules of the source specification are used in this profile (i.e. modules that business partners need to use or support in order to comply with the profile and communicate with others who do comply). For each used module, users also specify whether the module has been profiled or not. If yes, some profiling details should be given for this module in section 3 or 4.

3.1 Core Modules

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	Core Extension Elements (section 3)		
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			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	Security Module (section 4.1)		
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	The Security Module is **never used** in these profiles.	
Notes		Security profile 3: "*Sending MSH* authenticates and both MSHs negotiate a secure channel to transmit data" **must be** used. The HTTPS connection uses encryption to provide *in transit* confidentiality of the complete ebXML message and performs certificate-based Client and Server authentication during the TLS handshake.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	SyncReply Module (section 4.3)		
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 asychronously.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	Reliable Messaging Module (section 6)		
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*.

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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 MessageId. Any intermediate *NextMSH* ebXML-aware nodes (see caveat in section on multi-hop module) 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.

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	Message Status Service (section 7)		
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	**Optional**. Message Status Service is not required in these profiles.	
Notes			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	Ping Service (section 8)		
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	**Optional**. Ping Service is not required in these profiles.	
Notes			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	Message Order (section 9)		
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Message Order is **never used** in these profiles.	
Notes		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.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Module Name and Reference	Multi-Hop (section 10)		
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	**Never used** in this profile.	
Notes		These profiles use asynchronous communication for business messages, acknowledgments and error messages. This protocol is therefore compatible with asychronous, transparent, store-and-forward ebXML Messaging (or other SOAP-based) intermediaries. However, this document only specifies functionality of ebXML message endpoints.	

3.3 Communication Protocol Bindings

3.3.1 Profile Requirement Item: Transport Protocol

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements:		
Specification Reference	ebMS 2, Appendix B		
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.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	In message Header: /SOAP:Header/eb:MessageHeader/eb:From/eb:PartyId /SOAP:Header/eb:MessageHeader/eb:To/eb:PartyId Is a specific standard used for party identification? Provide details.		
Specification Reference	ebMS 2, section 3.1.1.1 PartyId Element		
Profiling (a)	Is a specific standard used for party identification? Provide details. Example - EAN•UCC Global Location Number. Ref.: ISO6523 - ICD0088.	Partners **should** use an identification based on the *FI* number of the Netherlands Business Registry (*Nieuw Handelsregister;* http://www.kvk.nl/nhr) concatenated with a location number (*vestigingsnummer*). The combination of these values is unique and allows identification of partners that are not themselves legal entities but departments or units of larger organizations.	
Profiling (b)	Should multiple PartyId elements be present in From and To elements?		

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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 *urn:oasis:names:tc:ebxml-cppa:partyid-type:iso6523:0106*. Example: <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:iso6523:0106">1234567890</eb:PartyId> Op dit moment staat nog niet volledig vast welk type van identificatie gebruikt zal worden.	
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:From/eb:Role /SOAP:Header/eb:MessageHeader/eb:To/eb : Role		
Specification Reference	ebMS 2, section 3.1.1.2 “Role Element”		
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>	No recommendation made. Business process is out of scope for (this version of the) OSB.	
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:CPAId		
Specification Reference	ebMS 2, section 3.1.2		
Profiling	What identification scheme is used for the CPAId, and what form should it take? If 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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:ConversationId		
Specification Reference	ebMS 2, section 3.1.3		
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.* Furthermore, values **should** be re-used in situations where this facilitates message tracking or business activity monitoring. In the case of the base registries (*basisregistraties*), the identification code of the registered entity **may** be used to allow monitoring of all communication about this entity.	
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 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 instead to a business collaboration?	No recommendation made. Business process is out of scope for OSB.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Test References			
Notes		ConversationId is a required ebXML message header element.	

4.1.5 Profile Requirement Item: MessageId

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:MessageId		
Specification Reference	ebMS 2, section 3.1.6.1		
Profiling (a)	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 if the ID is generated?	No recommendation made. The value of *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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Service /SOAP:Header/eb:MessageHeader/eb:Service/@type		
Specification Reference	ebMS 2, section 3.1.4		
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 whitespace.	
Alignment	Appears as Service element in CPA Appears as Service/@type in CPA		
Test References			
Notes			

4.1.7 Profile Requirement Item: Action

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Action	The text content of the *Action* element **must not** contain whitespace.	
Specification Reference	ebMS 2, section 3.1.5		
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			

4.1.8 Profile Requirement Item: Timestamp

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:Timestamp /SOAP:Header/eb:MessageHeader/ eb:Acknowledgment/eb:Timestamp		
Specification Reference	ebMS 2, section 3.1.6.2, 6.3.2.2, 6.4.5, 7.3.2		
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Description		
Specification Reference	ebMS 2, section 3.1.8		
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.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Alignment			
Test References			
Notes			

4.1.10 Profile Requirement Item: Manifest

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Body/eb:Manifest		
Specification Reference	ebMS 2, section 3.2.2		
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. While **[ISO 15000-2]** allows for references to external message payloads (for instance, using HTTP URIs), that are logically part of the message, but not as a physical entity in the MIME envelope. This option is **not supported** in these profiles.	
Profiling (b)	Must a URI that cannot 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			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Notes		XML or other business documents can have references to other resources that are not part of the ebXML message. It is up to the receiving application to interpret any such references. Any such mechanism is out of scope for OSB.	

4.1.11 Profile Requirement Item: Reference

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference	Only the *Content Id* reference mechanism **[RFC 2392]** is allowed.	
Specification Reference	ebMS 2, section 3.2.1		
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			

4.1.12 Profile Requirement Item: Reference/Schema

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Schema		
Specification Reference	ebMS 2, section 3.2.1.1		
Profiling	Are there any Schema elements required? If so, what are their location and version attributes?	Schema elements are not required. The OSB does not perform XML schema validation.	
Alignment			
Test References			
Notes			

4.1.13 Profile Requirement Item: Reference/Description

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Description		
Specification Reference	ebMS 2, section 3.2.1.2		
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			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Test References			
Notes			

4.2 Module: Security

4.2.1 Profile Requirement Item: Signature generation

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/Signature		
Specification Reference	ebMS 2, section 4.1.4.1		
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.	
Profiling (b)	Are additional Signature elements required, by whom, and what should they reference?	Not applicable	
Profiling (c)	What canonicalization method(s) must be applied to the data to be signed? [Recommended method is "http://www.w3.org/TR/2001/REC-xml-c14n-20010315".]	Not applicable	
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	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Profiling (f)	What Certificate Authorities (issuers) are allowed or required for signing certificates?	Not applicable	
Profiling (g)	Are direct-trusted (or self-signed) signing certificates allowed?	Not applicable	
Profiling (h)	What certificate verification policies and procedures must be followed?	The requirements as stated by the PKIOverheid **[PKI-Policy]**.have to be used.	
Alignment	(a) Appears as BusinessTransactionCharacteristics/@isAuthenticated=persistent and BusinessTransactionCharacteristics/@isTamperProof=persistent in CPA		
Test References			
Notes		Applications submitting data to, or receiving data from, OSB 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 these cases, the OSB is not aware of the presence of signatures and does not perform signature verification.	

4.2.2 Profile Requirement Item: Persistent Signed Receipt

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.2		

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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	
Profiling (b)	If so, what is the Acknowledgment or Receipt schema?	Not applicable	
Alignment	Appears as BusinessTransactionCharacteristics/@isNonRepudiationReceiptRequired=persistent in CPA.		
Test References			
Notes			

4.2.3 Profile Requirement Item: Non Persistent Authentication

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.3		
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** be able to operate in SSL v3 backward compatibility mode.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthenticated=transient in CPA.]		
Test References			
Notes			

4.2.4 Profile Requirement Item: Non Persistent Integrity

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.4.		
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.5		
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.	
Alignment	(b) [Appears as BusinessTransactionCharacteristics/@isConfidential=persistent in CPA.]		
Test References			
Notes		Applications submitting data to, or receiving data from, OSB 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 the OSB.	

4.2.6 Profile Requirement Item: Non Persistent Confidentiality

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.6		
Profiling	Are communication channel confidentiality methods required? [Yes, for Security Services Profiles 3, 6, 8, 11, 12.] Which methods are allowed or required?	HTTPS using TLS 1.0 **[RFC 2246]** Message service handlers **should** support SSL v3 compatibility mode.	
Alignment	[Appears as BusinessTransactionCharacteristics/@isConfidential=transient in CPA.]		
Test References			
Notes			

4.2.7 Profile Requirement Item: Persistent Authorization

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.7		
Profiling	Are persistent authorization methods required? [Yes, for Security Services Profiles 18-21.] Which methods are allowed or required?	Not applicable	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequired=persistent in CPA.]		
Test References			
Notes			

4.2.8 Profile Requirement Item: Non Persistent Authorization

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.8		
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 **must** be applied 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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:Signature		
Specification Reference	ebMS 2, section 4.1.4.9		
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, OSB 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 OSB 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:

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:ErrorList/eb:Error /SOAP:Header/eb:ErrorList/ eb:Error/@codeContext /SOAP:Header/eb:ErrorList/ eb:Error/@errorCode		
Specification Reference	ebMS 2, section 4.2.3.2.		
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 notification be performed (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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:SyncReply/		
Specification Reference	ebMS 2, section 4.3		
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 *MessageId* and *RefToMessageId* header elements encode correlation of request and response messages.	

4.5 Module : Reliable Messaging

4.5.1 Profile Requirement Item: SOAP Actor attribute

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/		
Specification Reference	ebMS 2, section 6.3.1.1		
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	The final recipient MSH returns a receipt acknowledgment message.
Test References			
Notes			

4.5.2 Profile Requirement Item: Signed attribute

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/		
Specification Reference	ebMS 2, section 6.3.1.2		
Profiling	Must MSH Acknowledgments be (requested to be) signed ?	Not applicable	
Alignment	[Appears as MessagingCharacteristics/ @ackSignatureRequested in CPA.]		
Test References			
Notes			

4.5.3 Profile Requirement Item: DuplicateElimination

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/		
Specification Reference	ebMS 2, section 6.4.1		
Profiling (a)	Is elimination of duplicate messages required? [Yes, for RM Combinations 1-4. .]	Not applicable	Duplicate Elimination is required.

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Profiling (b)	What is the expected scope in time of duplicate elimination? In other words, how long should messages or message Ids be kept in persistent storage for this purpose?		Message IDs **should** minimally be kept in persistent storage to prevent duplicate delivery during the time interval during 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 Ids in ebXML are based on **[RFC 2822]**, and must therefore be globally unique, which in theory prevents accidental re-use of IDs 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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/		
Specification Reference	ebMS 2, section 6.4.3, 6.4.4		

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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 OSB 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.
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			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 such that any such transport retries have completed first.

4.5.5 Profile Requirement Item: PersistDuration

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements:		
Specification Reference	ebMS 2, section 6.4.6		
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.
Alignment	[Appears as ReliableMessaging/PersistDuration in CPA.]		
Test References			
Notes			

4.5.6 Profile Requirement Item: Reliability Protocol

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements:		
Specification Reference	ebMS 2, section 6.5.3, 6.5.7		The Reliable Messaging Protocol in **[ISO 15000-2] must** be used.
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.

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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 parties are 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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: Eb:MessageHeader/eb:StatusRequest		
Specification Reference	ebMS 2, section 7.1.1		
Profiling (a)	If used, must Message Status Request Messages be digitally signed?	Not applicable. Digital signing is **not supported**.	
Profiling (b)	Must unauthorized Message Status Request messages be ignored, rather than responded to, due to security concerns?	No recommendation made.	
Alignment			
Test References			
Notes			

4.6.2 Profile Requirement Item: Status Response message

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: Eb:MessageHeader/eb:StatusResponse		
Specification Reference	ebMS 2, section 7.1.2		
Profiling	If used, must Message Status Response Messages be digitally signed?	Not applicable. Digital signing is **not supported**.	
Alignment			
Test References			
Notes			

4.7 Module : Ping Service

4.7.1 Profile Requirement Item: Ping-Pong Security

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: Eb:MessageHeader/eb:Service Eb:MessageHeader/eb:Action		
Specification Reference	ebMS 2, section 8.1, 8.2		
Profiling (a)	If used, must Ping Messages be digitally signed?	If Ping-Pong is used, Ping messages **must not** be digitally signed	
Profiling (b)	If used, must Pong Messages be digitally signed?	If Ping-Pong is used, Pong services **must not** be digitally signed	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements:		
Specification Reference	ebMS 2, section 10		
Profiling (a)	Are any store-and-forward intermediary MSH nodes present in the message path?	Endpoints connecting to the OSB **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.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Profiling (b)	What are the values of Retry and RetryInterval between intermediate MSH nodes?		Not applicable. Any OSB-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 OSB-level ebXML intermediaries **should** attempt to forward end-to-end receipts and errors.
Alignment			
Test References			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Notes		Any OSB-level ebXML intermediary may support transport retries, for instance to handle temporary TCP or HTTP transport level errors. This is not required.	This profile uses end-to-end reliable messaging. This allows the OSB to recover from any temporary processing failures at the level of intermediaries. Upcoming versions of the OSB **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 this 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.

4.8.2 Profile Requirement Item: Acknowledgements

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements: Eb:MessageHeader/		
Specification Reference	ebMS 2, section 10.1.1, 10.1.3		
Profiling (a)	Must each intermediary request acknowledgment from the next MSH?	Not applicable. There is **no support** for ebXML *next MSH* acknowledgments.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements:		
Specification Reference	ebMS 2, section 2.3.6, 2.3.7, 2.3.8		
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.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Profiling (b)	**(Section 2.3.7)** Is a unique “id” attribute required for each (or any) ebXML SOAP extension elements, 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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	MIME Header elements: Content-Type		
Specification Reference	ebMS 2, section 2.1.3.2		
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			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Test References			
Notes			

4.11 HTTP Binding

4.11.1 Profile Requirement Item: HTTP Headers

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements, MIME parts		
Specification Reference	ebMS 2, Appendix B.2.2.		
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements, MIME parts		
Specification Reference	ebMS 2, Appendix B.2.3.		
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

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements, MIME parts		
Specification Reference	ebMS 2, Appendix B.2.6.		
Profiling	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 information only. HTTP Basic or Digest authentication are **not supported**.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Alignment	Appears as AccessAuthentication elements in CPA.		
Test References			
Notes			

4.11.4 Profile Requirement Item: HTTP Confidentiality and Security

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements, MIME parts		
Specification Reference	ebMS 2, Appendix B.2.7.		
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** 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?	No	
Profiling (e)	Is client-side certificate-based authentication allowed or required?	Client-side authentication is **required**.	

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Profiling (f)	What client Certificate Authorities are acceptable?	PKI overheid maintains a list of approved certificate service providers **[PKI-CA]**.	
Profiling (g)	What certificate verification policies and procedures must be followed?	PKI overheid procedures are described in **[PKI-Policy]**.	
Alignment			
Test References			
Notes			

4.12 SMTP Binding

4.12.1 Profile Requirement Item: MIME Headers

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements, MIME parts		
Specification Reference	ebMS 2, Appendix B.3.2.	Not Applicable. This specification only supports the HTTP transport protocol.	
Profiling (a)	Is any specific content-transfer-encoding required, for MIME body parts that must conform to a 7-bit data path? [Base64 or quoted-printable, for example.]	Not Applicable.	
Profiling (b)	If other than "ebXML" what must the SOAPAction SMTP header field contain?	Not Applicable.	
Profiling (c)	What additional MIME headers must be included among the SMTP headers?	Not Applicable.	
Alignment			

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Test References			
Notes			

4.12.2 Profile Requirement Item: SMTP Confidentiality and Security

		OSB profiles for ebXML Messaging 2.0	
		Best effort	Reliable messaging
Specification Feature	Header elements, MIME parts		
Specification Reference	ebMS 2, Appendix B.3.4, B.3.5		
Profiling (a)	What SMTP access control mechanisms are required? [Refer to item 4.1.4.8 in Security section.]	Not Applicable.	
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.	
Alignment			
Test References			
Notes			

5 Operational Profile

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

5.1 Deployment and Processing requirements for CPAs

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
Is a specific registry for storing CPAs required? If so, provide details.	Pending	
Is there a set of predefined CPA templates that can be used to create given Parties' CPAs?	CPA templates are available for the two profiles defined in this specification.	
Is there a particular format for file names of CPAs, in case that file name is different from CPAId value?	Pending	
Others		

5.2 Security Profile

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
Which security profile(s) 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, isTamperproof, isAuthenticated definitions.]	Security profile 3: "*Sending MSH authenticates and both MSHs negotiate a secure channel to transmit data*" **must be** applied.	
(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.	

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
Are any specific third-party security packages approved or required?	No recommendation made	
What security and management policies and practices are recommended?	Pending	
Any particular procedure for doing HTTP authentication, e.g. if exchanging name and password, how?	Not applicable.	
Others		

5.3 Reliability Profile

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
If reliable messaging is required, by which 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.
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

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
(Section 4.2.4.2) Should errors be reported to a URI that is different from that identified within the From element? What are the requirements for the error reporting URI and the policy for defining it?	No recommendation made	

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
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		

5.5 Message Payload and Flow Profile

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
What are typical and maximum message payload sizes that 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 that have 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?		
(Section 2.1.4) How many Payload Containers must be present?	Messages other than standalone receipt acknowledgement messages and error messages **must** contain exactly one payload container. This limit is imposed to facilitate bridging to other protocols at the enterprise level that may not support multiple payloads natively.	

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
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 payload **must** be of type "*application/xml*". I.e. this version of the OSB is limited to payloads consisting of a single XML business document.	
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		

5.6 Additional Messaging Features beyond ebMS Specification

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
Are there additional features out of specification scope, that are part of this messaging profile, as an extension to the ebMS profiling?	No	No

5.7 Additional Deployment or Operational Requirements

	OSB profiles for ebXML Messaging 2.0	
	Best effort	Reliable messaging
Operational or deployment aspects that 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/voor-certificaatverleners/toegetreden-certificaatverleners/

[PKI-Policy] PKI Overheid Programma van Eisen Deel 2. Toetreden en Toezicht.
URL http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2005/pve-deel-2/

[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/

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/download.php/13750/ebxml-iic-ebms2_deploy_template-spec-cd-11-final.doc

[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

[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

[JAB 2.0] Justitiestandaard Asynchroon Berichtenverkeer 2.0. Technische Specificatie ebXML Configuratiegids.

[NIST-Keys] NIST Key Management Guideline. . URL http://csrc.nist.gov/CryptoToolkit/kms/key-management-guideline-(workshop).pdf

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

[UMMR10] UMM Revision 10. URL http://www.untmg.org/index.php?option=com_docman&task=docclick&Itemid=137&bid=21&limitstart=0&limit=5.

[UMMUG] UMM User Guide URL http://www.untmg.org/index.php?option=com_docman&Itemid=137&task=docclick&bid=20&limitstart=0&limit=5