

Multiple Messaging Services (MMS) Profile for ebMS 3.0

ドキュメント情報	
名前	Multiple Messaging Services (MMS) Profile for ebMS 3.0 ebMS 3.0に関するMultiple Messaging Services (MMS)のプロファイル
バージョン	R 12.00.00A
更新日付	2009年10月30日

リリース版 R 12.00.00A

注) この翻訳資料は、英文資料を正式原文とし、あくまで皆様の参考資料として提供するものです。
解釈、表現等で疑問点があれば、必ず原文にてご確認ください。また、翻訳文への疑問点、訂正箇所等お気づき
の場合には、RNJ事務局まで、Mailにてご連絡頂ければ幸いです。
翻訳品質向上に向け、ご協力をお願い致します。

目次

1 始めに (Introduction)	5
1.1 文書の約束事 (Document Conventions).....	5
1.2 一般的な目的と範囲 (General Intent and Scope)	5
1.3 一般的な方法論 (General Methodology)	7
2 ebXML メッセージ概要 (ebXML Messaging Overview)	10
2.1 ebXML フレームワーク (The ebXML Framework).....	10
2.2 ebXML メッセージング (ebXML Messaging).....	11
3 取引先との運用規約 TPA (Trading Partner Agreement)	13
3.1 TPA と 基盤展開パラメータ (TPA and Infrastructure Deployment Parameters)	13
3.2 CPP と CPA プロファイリング (CPP and CPA Profiling)	17
4 メッセージの解説 (Message Description)	18
4.1 ebMS 3.0 プロファイリングに関する一般的な手引き (General approach for ebMS 3.0 profiling)	18
4.2 ebMS V3 ヘッダ・プロファイリング (ebMS V3 Header Profiling).....	20
5 メッセージ処理 (Message Processing)	29
5.1 処理モード (P-Modes) (The Processing Modes (P-Modes)).....	29
5.2 パッケージング (Packaging)	29
5.3 アンパッケージング (Un-packaging)	29
6 サポートされる IT シナリオとメッセージ交換パターン (Supported IT Scenarios and Message Exchange Patterns)	30
6.1 ebMS 3.0 におけるメッセージ交換パターン (MEPs) (Message Exchange Patterns (MEPs) in ebMS 3.0).....	30
6.2 メッセージタイプと用語 (Message Types and Terminology)	32
6.3 受領の意味:単純否認防止と検証後に否認防止 (Receipt Semantics: Simple and Validating Non-Repudiation).....	35
6.4 ITシナリオ:サーバーからサーバーへの一方向PIP (IT Scenario: One-Action PIP from Server to Server)...	38
6.5 ITシナリオ:ピュア・クライアントからサーバーへの一方向PIP (IT Scenario: One-Action PIP from Pure Client to Server)	44
6.6 IT シナリオ:サーバーから純粋クライアントへの一方向PIP (IT Scenario: One-Action PIP from Server to Pure Client).....	47
7 QoS 方針 (Quality of Service Policies)	51
7.1 一般的なセキュリティ方針 (General Security Policies).....	51
7.2 受領の取り扱い (Handling of Receipts).....	53
7.3 一般的な信頼性方針 (General Reliability Policies).....	54
8 展開構成と MSH の要求事項 (Deployment Configurations and MSH Requirements)	55
8.1 Web サービスへの接続 (Connecting to Web Services)	55
9 付録 A:CPA プロファイリングと例題 (Appendix A: CPA Profiling and Sample)	56
9.1 CPA プロファイリング形式 (CPA Profiling Forms)	56
9.2 CPA 関連書類名と参照のプロファイリング (Profiling the CPA Artifact Names and References).....	56

9.3	当事者情報のプロファイリング (Profiling the Party Info)	58
9.4	コラボレーションの際の役割のプロファイリング (Profiling the Collaboration Roles).....	59
9.5	配信チャネルのプロファイリング (Profiling the Delivery Channels).....	61
9.6	文書交換のためのプロファイリング (Profiling the Document Exchanges)	62
9.7	トランスポート層のプロファイリング (Profiling the Transport Protocol).....	63
9.8	PIP 定義における表の利用実例 (Examples of Tables Used in PIP Definitions).....	64
10	付録 (Appendix) B: 用語集 (Glossary)	65
11	参照 (References)	66

免責事項 (Legal Disclaimer)

RosettaNet™ 及びそのメンバー、職員、管理者、従業員、又は代理人は、本書や本書で提示する仕様及び関連するガイドラインやスキーマの使用によって発生した、あるいはそれらに関連した金銭的またはその他の損害、損失、障害に対して一切の責任を負うものではない。前述の仕様の使用をもって、本弁明への承諾の表明とみなされる。

著作権 (Copyright)

©2009 RosettaNet. All Rights Reserved. 本書の一部あるいは全部について、出版元からの文書による許諾を得ずに、電子的、機械的、写真複写、録音、あるいはその他いかなる形式または方法においても、再版、検索システムへの保存、あるいは移送を行うことを禁ずる。

商標 (Trademarks)

RosettaNet、Partner Interface Process、PIP及びRosettaNetロゴは、非営利組織「RosettaNet」の商標または登録商標である。その他の製品名及び企業のロゴは、それらの所有者の商標である。本書では、商標または登録商標として認知された表記について言及する場合、その表記が最初に登場した箇所のできる限り適切な確認を行うようにした。

ドキュメントのバージョン履歴 (Document Version History)

バージョン	日付	コメント
リリース版 R12.00.00A	2009年10月30日	リリース版として公開

謝辞 (Acknowledgments)

本書は、RosettaNet (<http://www.rosettanet.org/>) により準備されたものであり、基盤・プログラムにおいて集められた RosettaNet メソッドロジへの適合要件に基づくものである。この PIP の設計及び開発に携わった法人は次の通りである。

MMS ebMS チーム

<u>Members</u>	<u>Company</u>
Durand, Jacques	OASIS
Moberg, Dale	Axway
Stojanovic, Nikola	RosettaNet
Chew, Jasmine	RosettaNet
Hussam El-Leithy	RosettaNet

1 始めに (Introduction)

1.1 文書の約束事 (Document Conventions)

このドキュメントの中で、大文字で表示される "MUST", "REQUIRED", "SHALL", "SHOULD", "RECOMMENDED", "MAY", "OPTIONAL", "MUST NOT", "NOT REQUIRED", "SHALL NOT" と "SHOULD NOT" が、が本文書に現われる場合、このプロファイル仕様の特別な意味を持って使われる。これらは、[RFC2119]で記述される様に、解釈される。

1.2 一般的な目的と範囲 (General Intent and Scope)

1.2.1 目的 (Intent)

RosettaNet implementations currently require users to buy a messaging system capable of running the RosettaNet Implementation Framework (RNIF). Although such RNIF systems are robust and widely adopted for XML payloads in the high-tech industry, this solution has the following drawbacks:

現在、RosettaNetの実装には、RosettaNet実装フレームワーク (RNIF) を実装できるシステムを購入する必要がある。こうしたシステムは安定しており、ハイテク業界においてXML本文の交換に広く採用されているが、しかしながら、このようなRNIFメッセージングシステムは、以下の様な問題点がある。

- Such RNIF messaging systems are not commonly used by other vertical markets. As a result, companies who support both the high tech industry and other verticals are forced to support more than one messaging standard for e-business transactions.
このようなRNIFメッセージングシステムは、他の垂直市場では一般に使われていない。その結果、ハイテク産業と他の垂直市場の両方をサポートする企業は、eビジネス取引のために複数のメッセージング標準をサポートすることを強いられている。
- They do not represent a viable solution for small and medium businesses (SMBs).
それは、中小規模企業(SMBs)向けの実行可能なソリューションに対応していない。

To alleviate the problem, RosettaNet created a Multiple Messaging Services (MMS) initiative that included three additional messaging systems, ebMS, AS2 and Profile for Web Services WS.

この問題に対処するために RosettaNet は、ebMS、AS2、WS-I という3つのさらなるメッセージングシステムを含んだマルチ メッセージング サービス (MMS-Multiple Messaging Service) 構想を立ち上げた。

In a first phase of the MMS project, a profile for ebMS V2.0 has been defined. Since then, a new version of the ebMS standard has been completed in OASIS (ebMS V3.0) which has the following advantages compared to ebMS V2.0:

MMS プロジェクトの第一フェーズは、ebMS 2.0のプロファイルに対して定義を行った。その後 OASIS において、ebMS V2.0 に比べ下記の優位性を持った OASIS (ebMS V3.0) が新しい標準として完成した。

- Message pulling feature. This supports partners with limited connectivity (intermittent connectivity, lack of static IP addresses) who can only behave as pure clients, pushing messages to a server, and pulling messages from this server.
メッセージ取り込み機能。 この機能は、メッセージをサーバーに送り出し、このサーバーからメッセージを取り込むピュア・クライアントとしてのみ利用することができる、接続性に制限(断続的な接続性、静的IPアドレスの欠如)のあるパートナーをサポートします。

- Integration with back-end Web Services. The format of ebMS V3 messages is fully compatible with protocol-level Web services standards. As a result, integration with back-end Web services is facilitated, while still ensuring B2B decoupling between partners: WSDL definitions and their subsequent upgrades only need to be known from the ebMS gateway or the Enterprise Service Bus, while the messaging middleware – connecting message handlers over the Internet – supports all QoS and connectivity modes.

バックエンドWebサービスとの統合。 ebMSV3メッセージ形式は、プロトコルレベルのWebサービス標準と完全互換である。結果として、パートナー間のB2Bデカップリングを確保しつつ、バックエンドWebサービスとの統合が促進される。WSDL定義とそれ以降のアップグレードはebMSゲートウェイ、又はエンタープライズ・サービスバスから伝えられ、一方、メッセージング・ミドルウェアはインターネット上で、メッセージ・ハンドラーを接続し、全てのQoS及び接続モードをサポートする。

- Native support for advanced security features, such as non-repudiation of receipts and service-level authorization.

受領の否認防止及びサービスレベルの承認といった高度なセキュリティ機能がもともとサポートされている。

The purpose of this document is to recommend to users and developers how best to use an ebMS messaging V3 handling system to transport RosettaNet PIP business messages between trading partners. Including ebMS V3 in this way will add another messaging option for trading partners transporting RosettaNet business payloads and may lower the infrastructure investments required to exchange RosettaNet payloads across trading networks that employ ebMS V3.

本書の目的は、取引企業間でRosettaNetビジネス・メッセージを送るために、ebMSメッセージ V3処理システムを最も有効に使う方法をユーザーや開発者に推奨することである。ebMS V3をこのように組み入れると、RosettaNetビジネス情報を送る取引相手にとってメッセージングのオプションが増え、ebMS V3 を採用した取引ネットワークに亘ってRosettaNet PIPを交換するのに必要なインフラ投資を削減することが出来るかもしれない。

1.2.2 このプロファイルの範囲 (In-Scope of this Profile)

This document is concerned with the profiling and the configuration of an ebXML framework, for carrying RosettaNet PIPs according to the requirements identified in the MMS - Abstract Message Definition (AMD) document.

本書は、MMS で指定されている要求事項 (即ちメッセージ定義の要約書(AMD-Abstract Message Definition)) に従った RosettaNet PIP を実装するための ebXML フレームワークのプロファイリング及び構成について述べている。

The approach we have taken is to focus on ebMS 3.0, include part of the CPA and limit choreography to the lowest level covering one action PIPs.

我々の取ったアプローチは、ebMS 3.0に焦点を当てたもので、メッセージ交換プロトコル合意(CPA-Collaboration Protocol Agreement) の一部及び 1アクションPIPのみに対応する制限付のコレオグラフィが含まれる。

- ebXML version: V 3.0. The ebXML context for this profiling document includes ebBP2.0 (in RN PIPs: BPSS 1.01, though a customized version – validate against 1.01 at least. Some references will be made to ebBP 2.0 when appropriate). Profiling of CPPA 2.0 / CPPA 2.1. is added in appendix, although it is expected that CPPA V3 should be used instead when complete.

ebXML バージョン (ebXML version) : V3.0 このプロファイル文書用のebXMLコンテキストは、ebBP2.0を含む (RN PIPsに対しては、BPSS 1.01はカスタマイズされたバージョンであっても最低限 1.01に対して検証される。リファレンスのいくつかは、適切であればebBP 2.0に対して行われる)。CPPA 3.0が利用可能になれば使いたいが、CPPA 2.0 / CPPA 2.1を添付として追加した。(CPPA- Collaboration Protocol Profile and Agreements :メッセージ交換プロトコル・プロファイル及び合意)

- **Choreography:** The approach is here to cover simple choreographies, involving one or two business messages (action messages in RosettaNet), augmented with ebMS signals message (e.g. Receipts, Errors, PullRequest) when QoS requirements demand it.

コレオグラフィ (Choreography): このアプローチは、QoS要件が要求する際に、ebMS信号メッセージ (受領、エラー、引き込みリクエストなど) で拡張された、1通または2通のビジネス・メッセージ (RosettaNetのアクション・メッセージ) に含まれるシンプルなコレオグラフィをカバーするものである。

- **Subset of Agreements:** Although ebMS is the target, the intent of this profiling goes beyond just wire interoperability and addresses some agreement aspects (CPA). Defining CPA templates or guidelines is the best way to represent the out-of-band agreement required for a practical deployment of PIPs. Only the part of the CPA that relates to messaging and maps to PIP definition data, will be profiled.

合意の部分集合 (Subset of Agreements): ebMSがターゲットではあるが、このプロファイリングの意図は、単なるワイヤ相互運用性の範囲を超え、いくつかの合意問題 (CPA:メッセージ交換プロトコル合意) を取り扱うことである。CPAテンプレート又はガイドラインを定義することは、PIPの実際の展開に必要な私的な合意 (out-of-band agreement) を示すもっともよい方法である。メッセージング及びPIP定義データへのマップに関連したCPAの部分についてのみプロファイルする。

1.2.3 このプロファイルの範囲外について (Out-Of-Scope of this Profile)

- **Multi-hop.** Part 2 of ebMS V3 is still in the design process at the time this V3 profile is written. This includes routing functions in multi-hop environments.

マルチホップ (Multi-hop): このV3 プロファイルを作成中では、ebMS V3のパート 2は、未だ設計段階であった。これには、マルチホップ環境のルーティング機能も含まれる。

1.3 一般的な方法論 (General Methodology)

- The Trading Partner Profiles (TPP) and resulting Abstract Trading Partner Agreement (ATPA) is a good starting point for users. Although the core of the ebXML profiling described here is defined solely based on mapping RNIF features into ebXML features (via the MMS-AMD [AMD] requirements), the ATPA represents parameters that need to be defined in order to complete a user-specific profiling of ebXML for a PIP deployment.

取引先プロファイル (TPP- Trading Partner Profiles) 及びその結果の取引先との取引契約要約 (ATPA- Abstract Trading Partner Agreement) はユーザーにとっていい出発点である。ここで示す ebXMLプロファイリングの中核部分は、(MMS-AMD [AMD] 要件によって) RNIF機能を ebXML機能にマッピングすることによって単独で定義されるが、取引先との運用規約要約 (ATPA) は、PIPの展開のための ebXMLのユーザー固有プロファイリングを完成させるために定義する必要があるパラメータを示す。

- From the TPP info, a CPP (Collaboration Protocol Profile) template can be filled for each partner, and a resulting agreement (TPA) can be mapped to a subset of the CPA. However, the suggested approach is for a business entity to directly define a partially-filled CPA with its capabilities and communication requirements (a “CPA template”), then share this CPA template with its business partner(s) who will complete it. The resulting document is a CPA instance.

TPP情報から、取引先プロファイル (CPP- Collaboration Protocol Profile) テンプレートに各取引先について記入され、その結果得られる取引先との運用規約 (TPA) をCPAのサブセットにマップすることができる。しかし、提唱されている方法は、企業体が能力及び通信要件が部分的に記入されたCPA (“CPA テンプレート”) を直接定義し、このCPAテンプレートを完成させる取引相手と共有するためのものである。結果として出てくる文書は、CPAインスタンスである。

- This CPA instance will be somehow orthogonal to PIPs: the deployment of several PIPs may share the same CPA instance. Conversely, several instances of the same PIP may use different CPAs, based on requirements that are specific to the nature of the document contents and other business considerations. Tools exist for producing the Collaboration Role part of a CPP or CPA directly from a 2.0 ebBP Business Collaboration specification.

このCPAインスタンスは、どういうわけかPIPとは異なる:複数のPIPを展開することは、同じCPAインスタンスを共有することになるかもしれない。逆に、同じPIPの複数のインスタンスは、ドキュメント内容やその他のビジネス上の留意事項の性質に固有の要件に基づいた異なるCPAを使っているかもしれない。2.0 ebBPビジネス・コラボレーション仕様からCPPまたはCPAのコラボレーション役割部分を直接生成するためのツールは、存在する。

- This document describes profiling rules for ebMS V3 and for CPA 2.1. These rules, when applied to data that is specific to business partners (TPA) and specific to targeted PIPs, will define specific messaging profiles.

この文書は、ebMS V3 及びCPA 2.1の**プロファイリング・ルール**を記述する。これらのルールは、取引先(TP)及び目的のPIPに特有のデータに適用される場合、特定の**メッセージ・プロファイル**を定義する。

- ebMS can be used with ebBP2.0 (and former BPSS versions as well) or CPPA, and so both ebBP2.0 and CPPA can also be used when ebMS is used for RosettaNet. No attempt will be made to produce a complete profile for CPPA or ebBP2.0 for RosettaNet in this document. However, it will occasionally be explained what CPPA or ebBP2.0 features would need to be in a CPPA or ebBP2.0 that governed ebMS messaging when used for RosettaNet. These features can be understood as configuration input for the ebXML MSH mode of operation, as they may affect the MSH behavior without necessarily affecting the message header. For example, for GS1 EDIINT there exists a standard ebBP set of templates that comply with GS1 recommended configurations.

ebMSは、ebBP2.0(前のBPSSバージョンも同様)とCPPAのいずれかが使用できるので、RosettaNetにebMSが使われている場合、ebBP 2.0とCPPAの両方を使用することもできる。本文書ではRosettaNetのためのCPPA、又はebBP2.0の完全なプロファイルを提示することは試みていない。

しかしながらRosettaNetに使用される場合、ebMSメッセージングにより支配されるCPPA、又は、BPSSの中に、どのCPPA、又はebBP 2.0機能が必要であるか説明される場合もある。これらの機能は、メッセージ・ヘッダに影響するとは限らないもののMSH(Message Service Handler)の行動に影響するかもしれないので、ebXML MSHオペレーション・モードのための設定入力として理解される。例えば、GS1 EDIINT(EDI over Internet)には、GS1推奨構成に準拠するebBP標準テンプレートのセットがある。

Some general rules of ebMS profiling:

ebMS プロファイリングのいくつかの一般的なルール:

- The proposed profiling in this document does not make use of customization points in the ebMS3 header – in particular MessageProperties – so that a broader set of MSH implementations can be used.

本文書で提案されているプロファイリングは、より広範なMSH実装を使用できるように、特にメッセージプロパティにおけるebMS3ヘッダのカスタマイズ・ポイントを使用しない。

- The ebMS header will fulfill the functions of the RNIF Delivery header, although it does not contain all the information present in the Delivery header. Some elements of the ebMS header will also map to elements from the Service header.

ebMSヘッダには、デリバリー・ヘッダにある全ての情報が含まれているわけではないが、RNIFデリバリー・ヘッダの機能を果たす。ebMSヘッダのいくつかの要素は、サービス・ヘッダの要素にマッピングする。

- Clearly there is more data in Standard Business Document Header (SBDH) and/or RNIF Service Header than can be represented in ebMS headers (without using extensions). In case the SBDH needs be preserved as is – e.g. for reuse of legacy back-end integration -, then the entire SBDH header can be added as a distinct payload part (referenced by a separate eb:PartInfo element in the header). It is RECOMMENDED to add it in the SOAP Body instead of as an attachment.

標準ビジネス文書ヘッダ(SBDH)および/またはRNIFサービス・ヘッダの方が、(拡張なしの)ebMSヘッダよりも明らかにデータが多い。SBDHをそのまま保存する必要がある場合(例:レガシーバックエンド統合の再利用のため)は、SBDHを異なるペイロード部として使用することができる(ヘッダの個別のeb:PartInfo要素が参照して利用)。添付ではなくSOAP本体に追加することが推奨される。

2 ebXML メッセージ概要 (ebXML Messaging Overview)

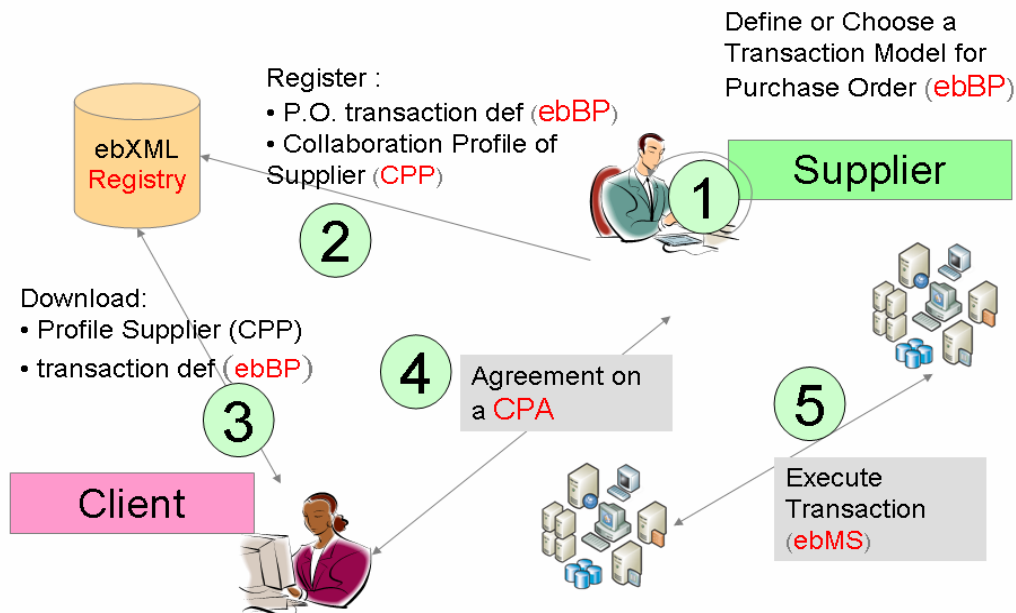
2.1 ebXML フレームワーク (The ebXML Framework)

The ebXML specifications support the exchange of business messages required to conduct electronic trading relationships between business partners. These capabilities logically separate but allow coordinated use of five key technologies important for eBusiness:

ebXML仕様は、ビジネス・パートナー間で電子商取引を行う場合に要求されるビジネス・メッセージの交換を支援する。これらの機能は理論的には別々であるが、eBusinessにとって重要な5つの主要な技術の相互活用を可能にする。

- Communicating data in common terms using a defined methodology (Core Components)
規定された手段(コアコンポーネント)を使った一般的な用語でのデータのやりとり。
- Defining business processes and assembling business transactions (ebXML Business Process Specification Schema, ebBP)
ビジネス・プロセスを定義し、商取引(ebXMLビジネス・プロセス仕様スキーマ、ebBP)を纏める。
- Providing secure and reliable transport (ebXML Messaging Service [ebMS])
安心かつ信頼できるトランスポート層の提供。(ebXMLメッセージング・サービス[ebMS])。
- Registering and making available key eBusiness artifacts and services (ebXML Registry Services [ebRS] and Registry Information Model [ebRIM])
重要なeBusinessの作成物やサービス(ebXML登録サービス(ebXML Registry Services [ebRS])及び登録情報モデル(Registry Information Model [ebRIM])を登録し、利用可能にする。
- Providing a technical configuration contract between business partners (Collaboration Protocol Profile and Agreements [CPP/CPA])
ビジネス・パートナー間の技術的設定契約を提供する。(取引先 プロファイル及びメッセージ交換プロトコル合意 [CPP/CPA])

An ebXML Scenario



The business case and requirements that prompted the development of the set of ebXML specifications were to:

一連の ebXML 仕様の開発を促したビジネス事例及び要求事項は次の様なものであった。

- Provide a migration path for and leveraging of EDI-compatible technologies.
EDI互換性技術の活用及び移行方法を提供すること。
- Develop openly accessible technologies for Small-Medium Enterprises whether in a managed or non-managed environment.
管理、無管理環境に関係なくオープンにアクセスできるSMEのためのテクノロジーを開発すること。
- Enable all supply-chain partners using XML technologies.
XML技術を用いて、全てのサプライチェーン・パートナーとの連携を可能にすること。
- Provide an integrated eBusiness approach focused on interoperability needs, while maintaining loosed-coupling to backend systems.
バックエンド・システムとの疎結合を維持しながら、相互運用性ニーズを重視した統合的eBusinessアプローチを提供すること。

The heterogeneous nature of eBusiness transactions require a flexible infrastructure and architectural framework that can support service calls (catalog status requests) and more complex document exchange (offers and acceptance).

eBusinessのやりとりが色々な種類のものである性質上、サービス・コール(カタログ状況要求)や、より複雑なドキュメントの交換(提案及び受諾)をサポートできる柔軟なインフラやアーキテクチャの枠組みが必要である。

The business document processing was decoupled from the messaging layer. The consumer of these documents may be a service, a business process instance, or middleware or business application interested in the business document contents. Such documents cannot be directly associated with an application service in a predefined way. The coupling between the messaging system and the consumers of these messages must be supported in an adaptable way.

ビジネス文書処理は、メッセージ層から分離させた。これらの文書の使われる先は、サービス、ビジネスプロセスインスタンス、またはビジネス文書の内容に関心があるミドルウェアまたはビジネス・アプリケーションなどが考えられる。そのような文書は、所定の方法でアプリケーション・サービスに直接的に関連している可能性はない。メッセージング・システムとこれらのメッセージの消費者の間の結合は、柔軟な方法でサポートしなければならない。

2.2 ebXML メッセージング (ebXML Messaging)

メッセージング概観 (Messaging Overview)

The ebMS protocol runs over several transport protocols, and provides bindings for HTTP and SMTP. It supports several message exchange patterns including push and pull that map to different types of business transactions. ebMS V3 improves on ebMS V2 on several aspects such as message pulling, non-repudiation of receipt, and full compliance with Web service protocols such as WS-ReliableMessaging and WS-Security. V3 is also compliant with related WS-I Basic Profiles [WS-I].

ebMS プロトコルは、複数のトランスポート・プロトコル上で動作し、HTTP と SMTP のための結合を提供する。ebMS プロトコルは、異なるタイプのビジネス取引とマッピングし、送出及び引取を含む複数のメッセージ交換パターンをサポートする。ebMS V3 はメッセージの取り出し、受領の否認防止、及び WS-ReliableMessaging や WS-Security などの Web サービス・プロトコルへの全面順守といった複数の側面において ebMS V2 より優れている。又、V3 は関連 WS-I 基本プロファイル[WS-I]にも順守している。

ebXML メッセージ標準の状況 (Status of ebXML Messaging Standards)

- The ebMS V2 was approved in 2002, and, in May 2004, submitted and accepted an ISO standard, ISO/TS 15000-2.

ebMS V2 は、2002年の8月に承認され、又、2004年5月に提案され、ISO標準のISO/TS 15000-2として承認された。

- The ebMS v3.0 OASIS Standard was approved in September 2007 [ebMS3]. An adjunct document on “Conformance Profiles for ebMS V3” [ebMS3-CP] has been defined. A second part to ebMS V3 is scheduled for end of 2009, which defines multi-hop and routing support as well as message bundling rules.

ebMS v3.0 OASIS標準は2007年9月に承認された[ebMS3]。"ebMSV3の適合性プロファイル" [ebMS3-CP] に関する付属文書が定義された。ebMSV3の第二部は2009年末に予定されており、そこにはメッセージ・バンドリング・ルールの外に、マルチホップ及びルーティング・サポートも定義される。

3 取引先との運用規約 TPA (Trading Partner Agreement)

3.1 TPA と基盤展開パラメータ (TPA and Infrastructure Deployment Parameters)

This table shows the relationships between TPA and ebXML components. It shows how elements of a TPA relate to the ebXML components. A dependency in the table indicates that some features of the ebXML component are concerned by the TPA item, or even further, that the feature must comply with the profiling described in this document.

この表は、TPA と ebXML 構成要素の関係を表したものである。TPA の各要素が如何に ebXML の構成要素と関係しているかが良くわかる。ebXML コンポーネントの一部の機能が TPA 項目と関係がある、あるいは、更にその機能は本文書に記載のプロファイリングに適合しなければならないことを、表における従属関係は示している。

The elements of a TPA that do not directly affect the standardized features of an ebXML component may still concern this component, but its impact will be at implementation, administration or deployment level, i.e. will affect the operational aspect, which is outside the scope of this profiling guideline.

直接的に ebXML コンポーネントの標準化された機能に影響していない TPA の要素が、それでもこのコンポーネントと関係する可能性はあるが、その影響は、実装、管理、又は展開レベル等の運用面に見られ、このプロファイル基準の対象外である。

- An “F” means that the answer to the question will affect features that are specified in the related standard (ebMS, CPPA or ebBP2.0). In other words, a compliant implementation to these standards explicitly supports answers to this question.

“F”は、質問に対する回答が関連規格(ebMS, CPPA または ebBP2.0)で規定される機能に影響することを意味する。言い換えると、これらの基準に適合した実装は、この質問への回答を明白に支持する。

- An “X” means that depending on the user answer to the question, the usage of this ebXML component will be affected in a way that must comply with the profiling defined in this document. In other words, you need to be aware of this profiling in order to implement the answer in a compliant way

“X”は、質問に対するユーザーの回答によっては、この ebXML コンポーネントの使用法は、本文書に記載のプロファイリングに適合しなければならないという形で影響を受けることを意味する。言い換えると、適合する方法で回答を実施するためには、このプロファイリングを知る必要がある。

- No mark means no direct effect or dependency on features that are specified in the related standard. The answer to the question becomes more a product implementation or deployment issue (how well this is handled depends more on additional product features than on conformance to the standard.)

マークがないのは、関連規格で規定される機能への直接的な作用または従属が一切ないことを意味する。質問に対する回答は、むしろ製品実装または展開上の問題となる(いかにうまくこれに対処するかは、基準への適合性よりも製品のその他の機能に依存する)。

TPA Item	ebMS V3	CPPA (<i>partial profiling here</i>)	BPSS (no rofiling defined here)
General Operation Parameters 一般的な運用に関するパラメータ			
Specify the standard you will use to identify trading partners. (DUNS, GLN, other authority name) あなたが取引相手を特定するために使う標準を指定してください。 (DUNS, GLN, 他の標準機関名)	FX	FX	

What is the maximum volume of messages you expect to exchange with any specific trading partner? What is the average? 貴社が特定の取引相手と交換しようとしているメッセージの最大量は、どの位ですか？又、平均は、どの位と想定していますか？			
What is your peak time interval? 貴社のピーク時間帯は、どの位ですか？			
What is the average size of the message during the peak time interval? ピーク時間帯におけるメッセージの平均サイズは、どの位ですか？			
How many messages do you receive and send during the peak time interval? ピーク時間帯にどの位のメッセージを送受信しますか？			
Will you use peer-to-peer routing or will you be using a messaging service (MS) (temporary message store)? 1対1ルーティングを利用されますか？又は、メッセージング・サービス (MS: 一時的メッセージ保管)を利用されますか？			
Will you operate via a message Hub, or directly point-to-point? メッセージハブを通して通信されますか？それとも直接1対1で、通信されますか？	FX	F	
If using a Hub, which message data will be used for doing routing? ハブを使うならば、どのメッセージ・データを、ルーティングとして使用しますか？			
Which of these Message Exchange Patterns will you be using? One-Way, Request-Response, Notification, Solicit-Response メッセージ交換方式としてどのような方式が使われますか？ 一方通行、要求-応答、通知、請求-応答	FX	FX	F
Will you need to correlate messages from a single PIP instance, or will you need to correlate messages from several PIP instances, as belonging to a same long-lasting conversation (e.g. for monitoring purpose) 同じ継続する会話として、一つのPIPインスタンスからのメッセージを関連づけますか？又はいくつかのPIPインスタンスからのメッセージを関連づけますか？(例: モニターする目的のために)	FX	FX	F
Will you be using a specific registry? If Yes, please specify 特定のレジストリーが使われますか？Yesならば、明示して下さい			
Will you be defining specific roles for each party of each business process? 各ビジネス・プロセスで、各々の関係者の明確な役割を定められていますか？	FX	FX	F
Indicate the level of Management Services you will require for your messaging system メッセージシステムのために必要とするマネージメント・サービスのレベルを示して下さい	F		
Do you need to track messages based on their participation in complex business processes? 複雑なビジネス・プロセスにおいて、彼らの参加に関するメッセージの追跡	FX (maybe)		

が必要ですか？			
Do you need status services? 状況サービスは必要ですか？	F (maybe)		
Do you need remote management? 遠隔管理は必要ですか？			
Do you need monitoring? 監視機能は必要ですか？	FX (maybe)		
Do you need BI support? BIサポート機能は必要ですか？			
Do you require disaster recovery? 災害復旧機能は必要ですか？			
Do you require Debugging capabilities? デバッグ機能は必要ですか？			
Indicate the level of Connectivity you will have with the Internet インターネットで必要な接続性のレベルを示して下さい			
Are you occasionally connected (dialup with modem?) 時折接続ですか(モデムによるダイヤルアップ)？	FX	F	
Are you permanently connected with a permanent IP address (T1, DSL)? 静的IPアドレスを使用して、常時接続を行いますか(T1, DSL)？	FX	F	
Are you permanently connected without a permanent IP address (Cable)? 静的IPアドレスを使用しないで、常時接続を行いますか(ケーブル)？	FX	F	
Indicate the Security Services you will require for your messaging system メッセージシステムにおけるセキュリティサービスの要望について示してください			
Do you need the headers to be encrypted? ヘッダの暗号化は必要ですか？	FX	FX	
Do you need the payload to be encrypted? Using which method? (S/MIME, XML Encryption) ペイロードの暗号化は、必要ですか？ どの方法を用いて？(S/MIME、XML暗号化)	FX	FX	
Do you need non-repudiation of origin? 発信元の否認防止を必要としますか？	F	F	
Do you need non-repudiation of receipt? 受領の否認防止を必要としますか？	FX	FX	
If need non-repudiation of receipt, is it required to have a digest of the acknowledged message in the acknowledgement, or is a simple reference to Message ID sufficient? 受領の否認防止が必要な場合、応答メッセージの中に応答確認の要約を必要としますか？又は、メッセージ IDへの単純な参照で充分ですか？	FX		

Do you need to digitally sign your messages (i.e.: X.509)? 電子署名(例:X.509) が必要ですか？	FX	FX	
Do you want to transport level encryption? (i.e.: TLS/SSL)? トランスポート層での暗号化が必要ですか？(例: TLS/SSL)	F	F	
Do you require timestamp of your messages? メッセージに対するタイムスタンプは必要ですか？	F		
Do you subscribe to authority domains? (i.e.: DUNS/GLN/EANUCC/ DUNS+ 4/Vertical) 標準機関と契約されていますか？ (例:DUNS/GLN/EANUCC/ DUNS+4/Vertical)	FX	F	
Indicate the Reliability you will require for your messaging system メッセージシステムにおける信頼性の要望について、示してください			
Do you need guaranteed message delivery? (include ACK signals) 保障されたメッセージの到達が必要ですか？(受領確認信号を含めて)	FX	FX	
Do you need de-duping? 重複削除が必要ですか？	FX	FX	
Do you require Ordered Delivery? 順序だてた配信が必要ですか？			
Do you require a Manifest? 目録が必要ですか？	F		
Do you require expiration control? 期限管理が必要ですか？	F		
Indicate what you will need to compress in your messages メッセージにおける圧縮の必要性について、示してください			
Do you need to compress headers? ヘッダの圧縮は必要ですか？	F		
Do you need to compress payload? 本文の圧縮は必要ですか？			
Do you need to compress attachments? 添付の圧縮は必要ですか？			
Indicate the Error Handling you will require for your messaging system メッセージシステムにおけるエラー処理の要望について示してください			
Do you need Message Service error handling (too many retries, etc.)? メッセージサービスにおけるエラー処理は必要ですか(再送制限等)	F	F	
Do you need Message Content error handling (invalid message, etc.)? メッセージ内容のエラー処理は必要ですか(無効メッセージ等)			
Do you need out of band error notification? 規定外データ(OOB) エラー処理は必要ですか？			

Indicate the Payload Capabilities you will require for your messaging system メッセージシステムにおける本文能力に対する要望について、示して下さい			
Do you need Globalization/I18? グローバリゼーション/I18が必要ですか？	F		
Do you need attachments? 添付は必要ですか？	F		
Do you need payload validation? 本文(Payload)の検証は必要ですか？			
What type of payload will you be exchanging, ASCII, Binary or both? どのような本文の交換を考えていますか？アスキー-ASCII, バイナリー 又は両方どの様なPayloadの交換を考えていますか？ASCII, Binary 又は両方？			
Will you need to support different versions of PIPs? 異なったバージョンのPIPのサポートが必要ですか？			
Indicate the requirements imposed by integration with existing software 既存ソフトウェアとの統合に関する必要条件について、示して下さい			
Do you need to preserve (some) previous message header structures (not native to ebMS) as is, so that you can reuse back-end binding technology? バックエンドの関連付け技術を再利用するために、前のメッセージ・ヘッダ内容を(ebMS固有でない)そのまま保存する必要がありますか？	FX		
Do you need to move message header data into your back-end? バックエンド・システムにメッセージ・ヘッダのデータを移動させる必要はありますか？	FX		

3.2 CPP と CPA プロファイリング (CPP and CPA Profiling)

Only CPPA V2.1 has been profiled here (Appendix 9). Use of CPP V3.0 once completed, is RECOMMENDED. Many profiling aspects of CPPA V2.1 defined here, can be transposed to subsequent CPPA versions.

ここでは、CPPA V2.1 のみが記述されている(付録9)。CPP V3.0 が完成した場合、利用することを推奨する。本書に規定される CPPA V2.1 のプロファイリングの多くは、今後出てくる CPPA バージョンに置き換えることができる。

4 メッセージの解説 (Message Description)

4.1 ebMS 3.0 プロファイリングに関する一般的な手引き (General approach for ebMS 3.0 profiling)

4.1.1 ebMS メッセージ・ヘッダと RosettaNet メッセージ・ヘッダ (ebMS message headers and RosettaNet message headers)

RNIFヘッダ: RNIF Headers:

The existing RNIF headers are dealt with in the following way:
既存のRNIFヘッダは、以下の方法で対応する:

- The RNIF Preamble header is not supposed to appear anymore in the ebMS message. RNIF 前文ヘッダは、もはや ebMS メッセージに表示されない。
- The RNIF Preamble header is not supposed to appear anymore in the ebMS message. It is replaced by the ebMS header. Although not all the information encoded in the Delivery header will be translated into the ebMS header, this header is not relevant anymore in the ebXML context.

RNIF前文ヘッダは、もはやebMSメッセージに表示されない。それはebMSヘッダに置き換わる。デリバリー・ヘッダに符号化される全ての情報がebMSヘッダに翻訳されるわけではないけれども、このヘッダは、もはや ebXMLコンテキストに適しない。

- The RNIF Service header may still be present in the ebMS message, in case it is needed for binding a message to existing PIP software that needs to be reused with ebXML. Some but not all of its elements map to the ebMS header. The Service header may be preserved as a separate attachment in the ebMS payload. However, in case of conflict between data in Service header and analogous data in ebMS header, the ebMS header will prevail as long as the messaging transfer is still in progress

RNIFサービス・ヘッダは、ebXMLで再利用する必要がある既存のPIPソフトウェアにメッセージを結合するために必要とされる場合、依然としてebMSメッセージに存在するであろう。その要素の全てではないが、一部はebMSヘッダに組み込まれる。サービス・ヘッダは、ebMSペイロードに別の添付ファイルとして保存される可能性がある。しかし、サービス・ヘッダのデータとebMSヘッダの類似データの間には矛盾が生じる場合は、メッセージの転送が進行中である限り、ebMSヘッダが優先する。

標準[ビジネス]文書ヘッダ(SBDH): Standard [Business] Document Headers (SBDH):

Not all information in the SBDH will map to ebMS headers. In case where an SBDH structure is present and used in the binding of the message with backend processes, it is recommended to keep the SBDH in the payload. However, in case of conflict between data in SBDH and analogous data in ebMS header, the ebMS header will prevail as long as the messaging transfer is still in progress (this includes routing in multi-hop environments). There are two options to consider:

SBDHの全ての情報がebMSヘッダに対応するわけではない。SBDH構造が存在し、情報のバックエンドプロセスとの結合に使用される場合、SBDHをペイロードに保つことが推奨される。しかし、サービス・ヘッダのデータとebMSヘッダの類似データの間には矛盾が生じる場合は、メッセージの転送が進行中である限り(これはマルチホップ環境でのルーティングを含む)、ebMSヘッダが優先する。二つのオプションについて考える。

- 1) The PIP document is defined using XML schema. In this case the SBDH is bound to the PIP document, and both are represented in the SOAP Body. The ebMS3 message has then only one MIME part: the SOAP envelope in which the eb:Messaging SOAP header contains the ebMS2 header, and the SOAP Body contains the payload (SBDH + PIP).

PIP文書は、XMLスキーマを使用し定義される。この場合、SBDHはPIP文書に結合され、両方ともSOAP本体の中に含まれる。ebMS 3メッセージは、1つのMIMEパートを持つ: eb:Messaging SOAP ヘッダにあるSOAPエンベロープには、ebMS 2ヘッダが含まれ、SOAP本体には、ペイロード(SBDH + PIP)が含まれる。

- 2) The PIP document is defined using DTD. In general, no SBDH instance is defined. Additional meta-data that may be needed and that is not in ebMS headers, is supposed to be found in the Service header -, and in FromRole + ToRole elements of PIPs. The Service Header can be preserved as a distinct payload part in the ebMS payload if needed. In case the SBDH is defined for this PIP and added to the message, it should also be sent as a distinct payload part in the ebMS payload. In both cases, it is RECOMMENDED to add it in the SOAP Body instead of as an attachment.

PIP文書は、DTDを使用し定義される。一般的に、SBDHインスタンスは必要とされない。ebMSヘッダではなく、サービスヘッダ及びPIPのFromRole+ToRole要素内に追加のメタデータが必要とされる可能性がある。サービスHeaderは、必要ならばebMS本文内で別個の本文として保たれることができる。SBDHがこのPIPのために定められてメッセージに加えられる場合、それはebMS本文と別個の本文としても送られなければならない。両方のケース共、添付としてではなく、SOAP本体に付加することを推奨する。

ebMS ヘッダの拡張 (ebMS header extensions)

For better interoperability between users, a deployment that conforms to this messaging profile MUST NOT use such extensions on any element under the eb:Messaging element. It is NOT RECOMMENDED to use the eb:MessageProperties child element of eb:Messaging.

ユーザー間の相互運用性を向上するため、このメッセージ・プロファイルに適合させる配置では、eb:Messaging 要素の元で、いかなる要素に対しても、そのような拡張を使用してはならない。eb:Messaging の子要素である eb:Message Properties を使用することは推奨しない。

既存のインフラストラクチャーとの統合 (Integrating with existing infrastructures:)

In order to preserve the ability to reconstruct the former RNIF structure (minus preamble and delivery headers), in case some users consider this a good integration approach with existing systems, the Service header MAY be included as a separate MIME part in the ebMS3 message, i.e. as an additional SOAP attachment element of the ebMS payload.

旧来のRNIF構造(前文ヘッダ及びデリバリーヘッダを差し引いたもの)を再構築する能力を維持するために、一部のユーザーがこれを既存のシステムとの優れた統合方法と考える場合、サービスヘッダはebMS2メッセージのMIME個別パートとして、即ち、ebMSペイロードのSOAP添付要素として含まれる可能性がある。

4.1.2 メッセージ・バンドリングとバッチング(Message Bundling and Batching)

- Payloads Bundling is the grouping of several payloads inside the same ebMS User Message unit (the eb:UserMessage element will refer to everyone of these payloads) . There is a single set of ebMS V3 "business headers", i.e. a single eb:Messaging SOAP header block.

本文を束ねるとは、同一のebMS User Messageユニット内に複数のペイロードをグループ化することである (eb:UserMessage要素はこれらのペイロードの1つ1つを参照する)。一組のebMSV3 "ビジネスヘッダ"、つまり単一のeb:Messaging SOAPヘッダ・ブロックがある。

- User Message Bundling is the grouping of several ebMS User Message units (eb:UserMessage elements) inside the same eb:Messaging SOAP header block. There is still a single SOAP envelope, but several ebMS business headers. This practice simply consists of packaging several ebMS messages in the same SOAP envelope (and leaving all additional payloads as separate attachments of the same MIME envelope). Except for security and reliability that will be processed once per SOAP envelope, the receiver MSH will process each User Message unit individually as if it had been received separately. The difference with payload bundling is that a set of well-formed ebMS messages is bundled, not just their payloads.

ユーザー・メッセージを束ねるとは、eb:Messaging SOAPヘッダ・ブロック内に複数のebMSユーザー・メッセージ単位 (eb:UserMessage要素) をグループ化することである。SOAPエンベロープは依然として1つであるが、ebMSビジネス・ヘッダは複数存在する。この規範は、単に同一のSOAPエンベロープ内に複数のebMSメッセージをパッケージングするというものである (又、全ての追加ペイロードを同一のMIMEエンベロープに個別の添付ファイルとして保存する)。各SOAPエンベロープに処理される保証及び信頼性を除き、受信側MSHは各ユーザー・メッセージ単位を個別に受信したかのように処理する。本文の束ねとの差は、単に本文だけでなく、XML規則に従ったebMSメッセージ式が束ねられるということである。

- Message batching is the ability to nest several SOAP ebMS messages (each one with its own SOAP envelope and individual headers) within the same MIME message. This option is not considered here.

メッセージ・パッチングとは、同一のMIMEメッセージ内に複数のSOAP ebMS (各々が自らのSOAPエンベロープと個別ヘッダを有する) を存在させる能力である。このオプションはここでは検討しない。

4.2 ebMS V3 ヘッダ・プロファイリング (ebMS V3 Header Profiling)

The tables below are borrowed from the Deployment Profile Template 1.1 for ebMS 2.0, [DPT-ebMS2] a document guide for deploying ebMS that has been developed by the ebXML Implementation, Interoperability and Conformance OASIS TC.

以下の表は、ebXML実装、相互運用性及び適合性OASIS TCによって開発されたebMS展開用の文書ガイドであるebMS 2.0 [DPT-ebMS2] のための展開用プロファイル・テンプレート 1.1 からの引用である。

4.2.1 プロファイル要求事項 eb:PartyId (Profile Requirement Item eb:PartyId)

Specification Header elements:
Feature

eb: UserMessage/eb: PartyInfo/eb: From/eb: PartyId
 eb: UserMessage/eb: PartyInfo/eb: From/eb: PartyId/@type
 eb: UserMessage/eb: PartyInfo/eb: To/eb: PartyId
 eb: UserMessage/eb: PartyInfo/eb: To/eb: PartyId/@type

Specification ebMS 3 [ebMS3], section 5.2.2.2
Reference

Profiling One instance of PartyId (in case several exist) must have as value either a DUNS (or DUNS+4) or Global Location Number (GLN). Both should not be found at the same time under the same From or To element.
 PartyId の 1 つのインスタンス (複数存在する場合) の値は、DUNS (又は DUNS+4)、又は GLN (Global Location Number) のどちらかであってはならない。どちらも、同一の From 要素、又は To 要素下で同時には見つからないものとする。

When several PartyId are present, the one above should be the first PartyId element. It is allowed to have additional PartyId elements in eb:From or in eb:To (they just need to have different @type values)
 複数の PartyId が存在する場合、上記のものが最初の PartyId 要素となる。eb:From 又は eb:To に追加の PartyId 要素があることは、許される。(但し、異なった @type 値を持つ必要がある)

- PartyID values MUST comply with ISO 6523 values, when applicable. That includes DUNS and GLN identifiers.
 適用できる場合、PartyIDの値はISO 6523の値に準拠しなくてはならない。DUNS及びGLN IDを含む。
- PartyID type attribute MUST be used to represent the Domain name and ICD (International Code Designator) according to section 24 "PartyID" of the CPPA V2.1 specification, found in:
<http://www.oasis-open.org/committees/ebxml-cppa/documents/ebCPP-2>

[_1.pdf](#) (April 2005)

PartyIDのタイプ属性は、CPPA V2.1仕様の24項“PartyID”に準拠し、ドメイン名及びICD: International Code Designator (国際コード指定子)を表すために使用されなければならない。 http://www.oasis-open.org/committees/ebxmlcppa/documents/ebCPP-2_1.pdf (April 2005)を参照。

More generally: もっと一般的に:

- the type value of the type attribute MUST be a URN. If the type attribute is present, then it provides a scope or namespace for the content of the PartyId element.
タイプ属性のタイプ値はURNでなければならない。タイプ属性が存在する場合、それはPartyId要素の中味の範囲、又は名前空間を提供する。
- if the type attribute is not present, the content of the PartyId element MUST be a URI that conforms to [RFC2396].
タイプ属性が存在しない場合、PartyId要素は[RFC2396]に準拠するURIでなければならない。

If an abbreviated name is described in the item titled “Name of Coding System” within the ICD list, it should be used, followed by the ICD value.
ICDリスト内の“コーディングシステム名”というタイトルのアイテムに略称が記述されている場合は、それを使用し、続いてICD値を使用するのがよい。

Example:

```
<tp:PartyId
  tp:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:D-U-N-SNumber:0060">123456789</tp:PartyId>
```

Where “0060” is the ICD value of D-U-N-S Number.

A GLN value can be used instead (see at the end of this section) e.g.:

```
tp:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:EANLocationCode:0088"> ... </tp:PartyId>
```

Alignment

- MUST map to (RNIF, Delivery Header) element: PartnerIdentification / GlobalBusinessIdentifier.
- MUST map to (Standard Bus. Doc Header - SBDH) element: PartnerIdentification (choice of Duns, Duns+ 4 or GLN), when applicable.
- MUST map to ebXML CPPA 2.0 or 2.1 element: PartyInfo/PartyId, when used.
- Value and type MUST conform to ISO 6523 when applicable, and the type attribute to section 24 “PartyID” of the ebXML CPPA V2.1 specification.
適用する場合、値ならびにタイプはISO 6523、タイプ属性はebXML CPPA V2.1仕様の24項 “PartyID” に準拠しなければならない。

Test

References

An implementation SHOULD provide support, and be able to accommodate, the usage of the type values standardized herein:

実装では、本書で規格が定められたタイプ値の使用法のサポートを提供するべきであり、又適合させることができることとする。

- If an abbreviated name is described in the item titled “Name of Coding System” within the ICD list (see [ISO 6523](#)), a type attribute can be constructed by prepending: “urn:oasis:names:tc:ebxml-cppa:partyid-type:” to the abbreviated name and appending a colon “:” followed by the ICD value. For example, using the abbreviated name D-U-N-S Number:

略称が、ICD リスト(ISO 6523 参照)中の表題 “コーディングシステム名”の項目に記述されている場合は、略称の先頭に “urn:oasis:names:tc:ebxml-cppa:partyid-type:”を付加し、その後でコロン“:”を付け、ICD 値を続けることによって、タイプ属性を構成できる。例えば、略称 D-U-N-S Number を用いて:

Abbreviated Name: “D-U-N-S Number

Upper-camel-case resultant string: “D-U-N-SNumber”

tp: type= " urn:oasis:names:tc:ebxml-cppa:partyid-type:D-U-N-SNumber:0060"

Note: “0060” is the ICD value of D-U-N-S Number.

To be consistent with v2 CPP/A, the value that follows remains a valid type attribute value or content for the PartyId element: “urn:oasis:names:tc:ebxml-cppa:partyid-type:duns”.

v2 CPP/A と矛盾しないように、後続値は PartyId 要素:

“urn:oasis:names:tc:ebxml-cppa:partyid-type:duns”に対して、有効なタイプ属性値または内容を維持する。

- Because an abbreviated name may be omitted from the ICD list, the type attribute can always contain the string derived from “Name of Coding System” expressed in upper-camel-case. A value can always be constructed by pre-pending “urn:oasis:names:tc:ebxml-cppa:partyid-type:” to the upper-camel-case name and appending a colon “:” followed by the ICD value. For example, using the formal name of the Name of Coding System: “Data Universal Numbering System”:
Transformed Camel-case: “DataUniversalNumberingSystem”

tp: type= " urn:oasis:names:tc:ebxml-cppa:partyid-type:DataUniversalNumberingSystem:0060"

略称が ICD リストから除外される可能性があるため、タイプ属性には常に先頭語が大文字 (UpperCamelCase) で表される“コーディングシステム名”から派生する文字列を含むことができる。

値はいつでも先頭語が大文字 (UpperCamelCase) の名称の先頭に

“urn:oasis:names:tc:ebxml-cppa:partyid-type:”を付加することによって構成できる。その後でコロン“:”を付け、ICD 値を続けることによって、タイプ属性を構成できる。例えば、“コーディングシステム名”から正しい名前を用いた“Data Universal Numbering System”は、変換された Camel-case 名は、“DataUniversalNumberingSystem”となる。

- Punctuation marks in these formal names (such as, “/”, “-“ or “””) should be included unless they are not allowed in URNs [RFC2141]. If the punctuation characters are not allowed in URNs, then the hexadecimal escaping convention explained in [RFC2141] should be followed for characters

これらの正式名称(例: “/”, “-“ 又は “”)における句読点は、URN[RFC2141]で許されないものを除いて、含まれるのが望ましい。句読点文字が URN で許されない場合は、文字の代わりに[RFC2141]中で説明される規則に抵触しない 16 進数で記述しなければならない。

Given the directives in [ISO 6523](#) related to Global Location Numbers (GLN) (ICD: 0088, Name of coding : EAN Location Code system, the above example yields a GLN type value of:urn:oasis:names:tc:ebxml-cppa:partyid-type: EANLocationCode:0088.

国際標準の事業所コード(GLN;Global Location Numbers)に関しては、ISO 6523 として通達されている。(ICD:0088,)

Name of coding : EAN の事業所コードシステム。上記の例では GLN タイプ値として、urn:oasis:names:tc:ebxml-cppa:partyid-type: EANLocationCode:0088 が生み出た。

4.2.2 プロファイル要求事項 eb:Role (Profile Requirement Item eb:Role)

Specification Feature	Header elements: eb: UserMessage/eb: PartyInfo/eb: From/eb: Role eb: UserMessage/eb: PartyInfo/eb: To/eb: Role
Specification Reference	ebMS 3, section 5.2.2.3, 5.2.2.5
Profiling	Role Name of the partner in this business transaction (in Partner Role Description of the PIP) <u>Example:</u> < eb: To > < eb: PartyId eb: type= " urn: oasis: names: tc: ebxml-cppa: partyid-type: D-U-N-SNumber: 0060" > myDUN S < /PartyId > < eb: Role > Seller < /eb: Role > < /eb: To >
Alignment	<ul style="list-style-type: none"> • MUST map to (RNIF, Service Header) element: from{ to} Role/GlobalPartnerRoleClassificationCode • MUST map to ebXML ebBP2.0: the role value maps to the corresponding BinaryCollaboration/Role/@name in ebBP2.0 (or BPSS 1.*) definition, when used. • MUST map to ebXML CPPA 2.0 or 2.1 element: CollaborationRole/Role/@name, when used.
Test References	

4.2.3 プロファイル要求事項 eb:Service (Profile Requirement Item eb:Service)

Specification Feature	Header element: eb: UserMessage/eb: CollaborationInfo/eb: Service
Specification Reference	ebMS 3, Section 5.2.2.8
Profiling	<p>This value MUST be the same as the one used in the ebBP2.0 instance (or BPSS) for the PIP (*). Its format must be:</p> <p>この値はPIPのebBP2.0インスタンス(又はBPSS)で使用される値と同一でなければならない。そのフォーマットは以下の通りでなければならない。</p> <p>“urn: rosettanet: specification: interchange: PIP” + < alphanumeric name of PIP > + “: xml: ebbp: ” + < PIP Version Identifier > .</p> <p>The Service element MUST have same value for all messages involved in a single PIP or TPIR-PIP (whether it is an Action, Confirmation or Signal message).</p> <p>サービス要素は、単一PIP、又はTPIR-PIPに含まれる全てのメッセージと同じ値を持たなければならない。(アクション、確認、又はシグナルメッセージのいずれであっても)</p>

Example:

If in ebBP2.0:

nameID="urn:rosettanet:specification:interchange:PIP7C7:xml:ebbp:v11_00" version="V11.00"

In ebMS header:

<eb:Service>

urn:rosettanet:specification:interchange:PIP7C7:xml:ebbp:v11_00</eb:Service>

Alignment

- MUST map to ebXML ebBP 2.0 or BPSS 1.* element when used: ProcessSpecification/@uuid or if not present, ProcessSpecification/@NameId
- MUST map to ebXML CPPA 2.0 or 2.1 element, when used: Service/@name

Test

References

(*) XSD (Modular) PIPs have BPSS documents defined while DTD (Monolithic) PIPs do not.

4.2.4 プロファイル要求事項 eb:Action (Profile Requirement Item eb:Action)Specification
Feature

Header element:

eb:UserMessage/eb:CollaborationInfo/eb:Action

Specification
Reference

ebMS 3, section 5.2.2.9

Profiling

In case of an Action message, the value MUST be consistent with Global Business Action Code (camel case version of this value).

アクション・メッセージの場合には、値はグローバルビジネス・アクション・コード(この値のキャメルケースバージョン:単語の先頭が大文字)と一致しなければならない。

eb:Action value needs to correspond to

ServiceHeader/ProcessControl/ActivityControl/MessageControl/Manifest/

ServiceContentControl/ActionIdentity/GlobalBusinessActionCode

In case of a RosettaNet signal, the value MUST be consistent with the following:

RosettaNet シグナルの場合は、値は以下と一致していなければならない:

If Signal is positive (ReceiptAcknowledgment):

もし、信号がポジティブ(ReceiptAcknowledgment)である場合:

Value= "ReceiptAcknowledgment"

If Signal is negative (Exception):

信号がネガティブである場合:

Value= "Exception"

Examples:

<eb:Action>Purchase Order Request</eb:Action>

<eb:Action>Purchase Order Change</eb:Action>

<eb:Action>Shipment Receipt Notification</eb:Action>

Alignment	<ul style="list-style-type: none"> MUST map to ebXML ebBP2.0 or BPSS 1.* element when used: RequestingBusinessActivity/@nameId, RespondingBusinessActivity/@nameId Map to ebXML ebBP2.0 element when used: BinaryCollaboration//@name or BusinessCollaboration/@name, Or, more precisely, the no-space version of these values.
Test	
References	

4.2.5 プロファイル要求事項 eb:Conversation Id (Profile Requirement Item eb:ConversationId)

Specification Feature	Header element: eb:UserMessage/eb:CollaborationInfo/eb:ConversationId
Specification Reference	ebMS 3, section 5.2.2.10
Profiling	<p>It is RECOMMENDED that ConversationId represents the PIP instance ID value, i.e. has same value for all messages related to the same PIP instance.</p> <p>ConversationId が PIP インスタンス ID 値を表す (つまり、同一の PIP インスタンスに関連する全てのメッセージに対し同一の値を有する) が推奨される。</p> <p>In other words, messages from the same PIP instance MUST have same ConversationID, and it is recommended that this ConversationID be unique to this PIP instance (not shared with other PIP instances).</p> <p>つまり、同一 PIP からのメッセージの ConversationID は同じでなければならないということであり、ConversationID はこの PIP インスタンスに対して一意 (他の PIP インスタンスと共有しない) であることが推奨される。</p>
Alignment	<ul style="list-style-type: none"> MUST map to Standard Business Doc Header (SBDH) element when applicable: RequestingDocumentInformation / BusinessProcessInstanceIdentifier MUST map to (in RNIF Service header) element: ServiceHeader/ProcessControl/pipInstanceId/InstanceIdentifier
Test	
References	

4.2.6 プロファイル要求事項 eb:RefToMessageId (Profile Requirement Item eb:RefToMessageId)

Specification Feature	Header element: eb:UserMessage/eb:MessageInfo/eb:RefToMessageId
Specification Reference	ebMS 3, section 5.2.2.1

Profiling	<p>As a reminder, it MUST be used only for:</p> <ol style="list-style-type: none"> (1) relating business signals messages to action messages, by referencing the ebMS ID. (2) Relating a business response to a business request. <p>確認として、ConversationID は以下の目的のみに使用されなければならない。</p> <ol style="list-style-type: none"> (1) ebMS ID を参照して、ビジネス信号メッセージをアクション・メッセージに関連づける。 (2) ビジネス応答をビジネス要求に関連づける。 <p>Every message involved in a PIP instance MUST refer to another previous message of this instance (except for the initial message of the instance, which MUST NOT have a RefToMessageId element.)</p> <p>PIPインスタンスに含まれる全てのメッセージ(RefToMessageId要素を有してはならないインスタンスの最初のメッセージを除く)は、このインスタンスの前のメッセージを参照しなければならない。</p> <p>If several PIP instances must be correlated, this MUST NOT be achieved by this value (the first message of a PIP instance MUST NOT refer to another PIP).</p> <p>複数のPIPインスタンスを関連づけなければならない場合は、この値でそれを達成してはならない (PIP インスタンスの最初のメッセージは別の PIP を参照してはならない)。</p>
Alignment	<ul style="list-style-type: none"> • MUST map to RNIF Service header element, in the sense it plays a similar role: 同様の役割を担うという意味で、RNIFサービス・ヘッダ要素にマッピングしなければならない: ServiceHeader/ProcessControl/ActivityControl/MessageControl/inReplyTo/messageTrackingID
Test References	

4.2.7 プロファイル要求事項 eb:MessageId (Profile Requirement Item eb:MessageId)

Specification Feature	<p>Header element:</p> <p>eb:UserMessage/eb:MessageInfo/eb:MessageId</p>
Specification Reference	<p>ebMS 3, section 5.2.2.1</p>
Profiling	<p>Used for uniquely (globally) identifying a message (either signal or action). Normally, this identifier is automatically generated by an MSH, and out of control from applications. (However, an MSH provides visibility to applications on this value, so that an application can use it for referencing (see eb:RefToMessageId).</p> <p>メッセージ(信号またはアクション)を一意(グローバルで)に識別するために使用する。通常、この識別子は自動的に MSH によって生成され、アプリケーションからは制御できない。(しかし、MSH はアプリケーションに対しこの値を見えるようにするので、アプリケーションが参照使用できるようになる (eb:RefToMessageId を参照)。</p>
Alignment	<ul style="list-style-type: none"> • MUST map to RNIF Delivery header, in the sense it plays a similar role: DeliveryHeader/messageTrackingID.InstanceIdentifier.
Test References	

4.2.8 プロファイル要求事項 eb:AgreementRef (Profile Requirement Item eb:AgreementRef)

Specification	Header element:
Feature	eb:UserMessage/eb:CollaborationInfo/eb:AgreementRef (NOTE: in ebMS V2, this corresponds to the element eb:MessageHeader/eb:CPAId)
Specification Reference	ebMS 3, section 5.2.2.7
Profiling	See Section “CPA Profiling and Sample” in Appendix A, for recommended profiling.
Alignment	
Test References	

4.2.9 プロファイル要求事項 eb:PayloadInfo (Profile Requirement Item eb:PayloadInfo)

Specification Feature	Header element: eb:UserMessage/eb:PayloadInfo/eb:PartInfo eb:UserMessage/eb:PayloadInfo/eb:PartInfo/eb:Schema
Specification Reference	ebMS 3, section 5.2.2.12, 5.2.2.13
Profiling	<p>Element eb:PartInfo: SHOULD include an eb:Schema element when the eb:PartInfo element is referring to the service content part (main XML document) of a PIP payload, or is referring to an XML RosettaNet signal. When present it MUST use an URN identifying the schema or DTD that applies to the part. The schema URN identifier MUST comply with [RN-NameSpaces].</p> <p>eb:PartInfo 要素は、eb:PartInfo 要素が PIP 本文のサービス内容部 (主な XML 文書) を指している、あるいは、XML RosettaNet 信号を指している場合、eb:Schema 要素を含まなければならない。存在する場合、その部分に適用されるスキーマ又は、DTD を識別する URN を用いなければならない。スキーマの URN 識別子は、[RN-NameSpaces] に準拠していなければならない。</p> <p>Example for a PIP service content with XML schema:</p> <pre>urn:rosettanet:specification:interchange:PIP3A4PurchaseOrderRequest:xsd:schema:1.0</pre> <p>When a legacy RNIF header (such as Service header) is included in the message, it must be added as a single attachment. The eb:Reference element SHOULD contain an eb:Schema element to identify it, which conforms to [RN-NameSpaces].</p> <p>レガシーな RNIF ヘッダ (サービスヘッダなど) がメッセージに含まれている場合、単独の添付として追加しなければならない。eb:Reference 要素には、それを識別する eb:Schema 要素を持つべきであり、それは [RN-NameSpaces] に準拠する。</p>

Example for a Service header:

```
urn:rosettanet:specification:system:ServiceHeader:dtd:schema:2.0
```

NOTE: The use of an XLINK processor should not be required.

Alignment

Test

References

5 メッセージ処理 (Message Processing)

5.1 処理モード(P-Modes) (The Processing Modes (P-Modes))

A P-Mode (Processing Mode) can be seen as configuration data that controls the way each message of a kind is processed by the Message Handler, when sent or received.

P-Mode (処理モード) は、送信時または受信時にメッセージ・ハンドラーが同じ種類の各メッセージを処理する方法を制御するコンフィギュレーション・データと見なすことができる。

Because different messages may be subject to different types of processing, an MSH generally supports several P-Modes.

メッセージが異なると、異なる種類の処理をする可能性があるため、一般的に MSH は複数の P-Mode に対応している。

On a Sending MSH, together with the information provided by the application layer for each submitted message, the P-Mode fully determines the content of the message header. For example, the "security" part of the P-Mode will specify certificates and keys, as well as which messages will be subject to these. This in turn will determine the content of the Security header.

送信側 MSH では、アプリケーション層によって各送信メッセージに対して提供された情報と共に、P-Mode が全てのメッセージ・ヘッダの内容を決定する。例えば、P-Mode の"セキュリティ"部分が証明書及びキーを指定し、どのメッセージをこれらの証明書とキーの対象とするかを定める。これにより、セキュリティ・ヘッダの内容が決定される。

The association of a P-Mode with a message may be based on various criteria, usually dependent on header data (e.g. Service/Action, Conversation ID, or other message properties). Which security and/or which reliability protocol and parameters, as well as which Message Exchange Pattern (MEP) is being used when sending a message, is determined by the P-Mode associated with this message.

P-Mode とメッセージとの関連付けは、様々な基準に基づく可能性があり、通常はヘッダ・データ(例: サービス/アクション、Conversation ID、あるいはその他のメッセージ・プロパティなど)に基づく。メッセージの送信時にどのセキュリティ・プロトコルおよび/またはどの信頼性プロトコル、並びにどのメッセージ交換パターン(MEP)が使用されるかはこのメッセージに関連した P-Mode によって決定される。

5.2 パッケージング (Ppackaging)

The packaging of the message headers and payloads, including security headers, follows the ebMS 3.0 specification. It is automatically implemented by conforming ebMS V3 MSH implementations. The content of ebMS header elements is largely controlled by PMode parameters. These parameters in turn reflect profiling decisions made in section 4 (for business headers) and in section 6 (for the MEP).

セキュリティ・ヘッダを含むメッセージ・ヘッダ及びペイロードのパッケージングは、ebMS 3.0 仕様に準拠する。それは、ebMS MSH 3.0 の実装に準拠して、自動的に実行される。ebMS ヘッダ要素の内容は、主に PMode パラメータによって制御される。これらのパラメータは、同様にセクション 4(ビジネスヘッダ用)及びセクション 6(MEP 用)でおこなったプロファイルの決定を反映する。

5.3 アンパッケージング (Un-packaging)

The un-packaging of the message headers and payloads, including security headers, follows the ebMS 2.0 specification. It is automatically implemented by conforming ebMS MSH implementations.

セキュリティ・ヘッダを含むメッセージ・ヘッダ及びペイロードのアンパッケージングは、ebMS 2.0仕様に準拠する。それは、ebMS MSH実装に準拠して、自動的に実行される。

6 サポートされるITシナリオとメッセージ交換パターン (Supported IT Scenarios and Message Exchange Patterns)

Partners implementing a RosettaNet PIP may not always have advanced infrastructure or persistent Internet connection. This Profile supports two kinds of business partners:

RosettaNet PIP を実装しているパートナーが必ずしも高度なインフラやインターネットの常時接続を備えているとは限らない。このプロファイルでは、以下の2種類のビジネス・パートナーをサポートする。

- A pure-client business partner does not run a messaging server (e.g. does not run an HTTP server), does not have a static IP address, and cannot receive incoming request messages (e.g. HTTP requests). It can have varying QoS capabilities (reliability, security).

ピュアクライアント・ビジネス・パートナーは、通信サーバーを持たず(例:HTTPサーバーを持たない)、静的IPアドレスも持たず、到着する要求メッセージ(例:HTTP要求)を受信できない。ピュアクライアント・ビジネス・パートナーは様々なQoS能力(信頼性、セキュリティ)を有することができる。

- A server-enabled business partner is running a messaging server, is an addressable endpoint to which messages can be sent directly (e.g. HTTP requests). It can have varying QoS capabilities (reliability, security), generally more complete than a pure-client partner.

サーバー機能を有するビジネス・パートナーは、通信サーバーを起動し、メッセージ(例:HTTP要求)が直接送信されるアドレスを持つエンドポイントである。サーバー機能を有するビジネス・パートナーは様々なQoS能力(信頼性、セキュリティ)を有することができ、一般的にピュア・クライアント・パートナーよりも完備している。

Accordingly, PIP interactions are supported in two basic IT scenarios:
従って、以下の2つの基本的なITシナリオにおけるPIPのやり取りをサポートする。

- Server to server: Interactions between two server-enabled business partners
サーバーとサーバー:2つのサーバー機能を有するビジネス・パートナー間のやり取り。
- Pure-client to server: Interactions between a pure-client business partner and a server-enabled business partner.
ピュア・クライアントとサーバー:ピュア・クライアント・ビジネス・パートナーとサーバー機能を有するビジネス・パートナー間のやり取り。

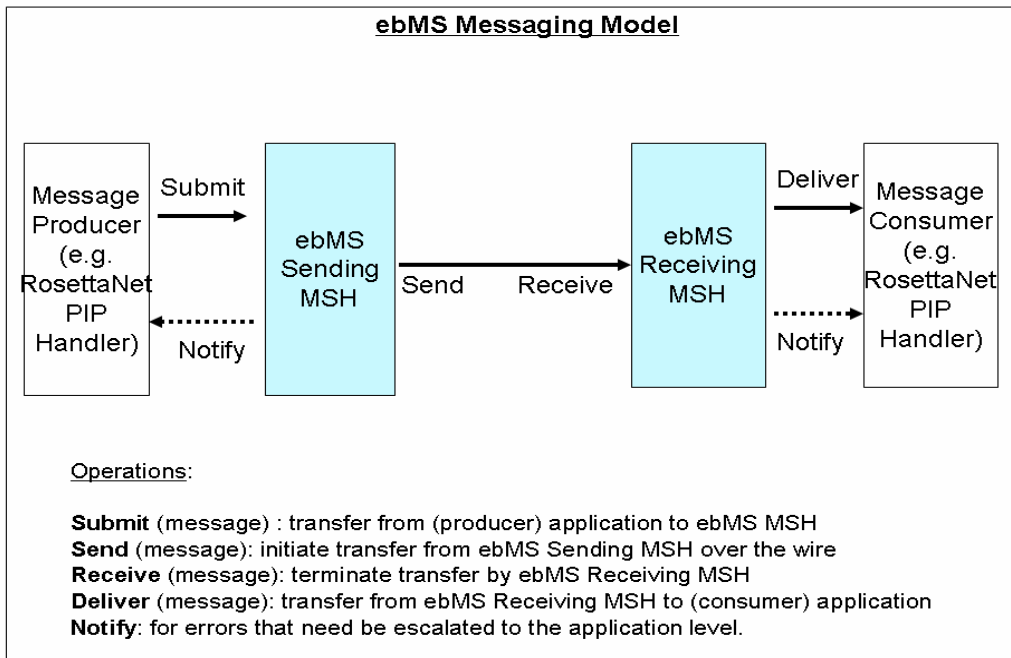
6.1 ebMS 3.0 におけるメッセージ交換パターン (MEPs) (Message Exchange Patterns (MEPs) in ebMS 3.0)

This section describes how ebMS MEPs map to PIPs involving action message(s), and potentially some RosettaNet signal message(s).

このセクションでは、ebMS MEPsがアクション・メッセージを含むPIP、及びできればいくつかのRosettaNet信号メッセージにどのようにマップするかを説明する。

The general messaging model in ebMS V3 is illustrated in the following figure. The model of integration with RosettaNet “PIP handler” is of a layering: PIP handling code is acting as the “application layer” for an ebMS Message Service Handler, communicating with the ebMS MSH via abstract operations (Submit, Deliver). An MSH will act in either one or both of the following roles: Sending and Receiving.

ebMSV3の一般的な通信モデルを以下の図に示す。RosettaNet“PIPハンドラー”との統合モデルは以下の様な階層化モデルである:PIP処理コードは、ebMS メッセージ・サービス・ハンドラー(MSH)の“アプリケーション層”として機能し、抽象的操作(Submit, Deliver)を経由してebMS MSHと通信する。MSHは以下の役割のうちのどちらか一方または両方として機能する:送信および受信。

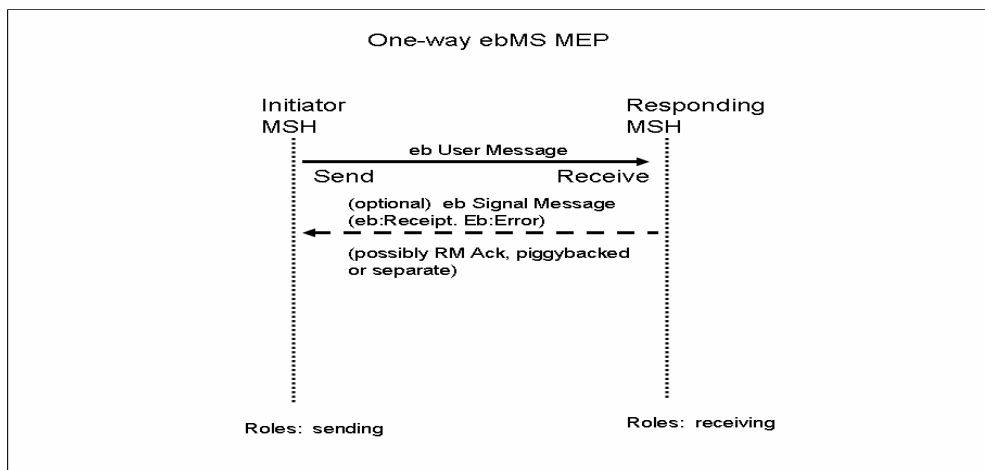


NOTE: The ebMS operation “Notify” is not bound to a business action, like Notifications often are in RosettaNet. Instead, they fulfill a QoS contract between the messaging layer and the application layer, about the reporting of errors.

注: ebMS 操作の“通知(Notify)”は、RosettaNet での通知(Notifications)が通常はビジネスアクションに結び付いているのとは異なり、ビジネスアクションには結び付いていない。そのかわり、メッセージレイヤとアプリケーションレイヤの間で、エラーの報告についての QoS 契約を履行する。

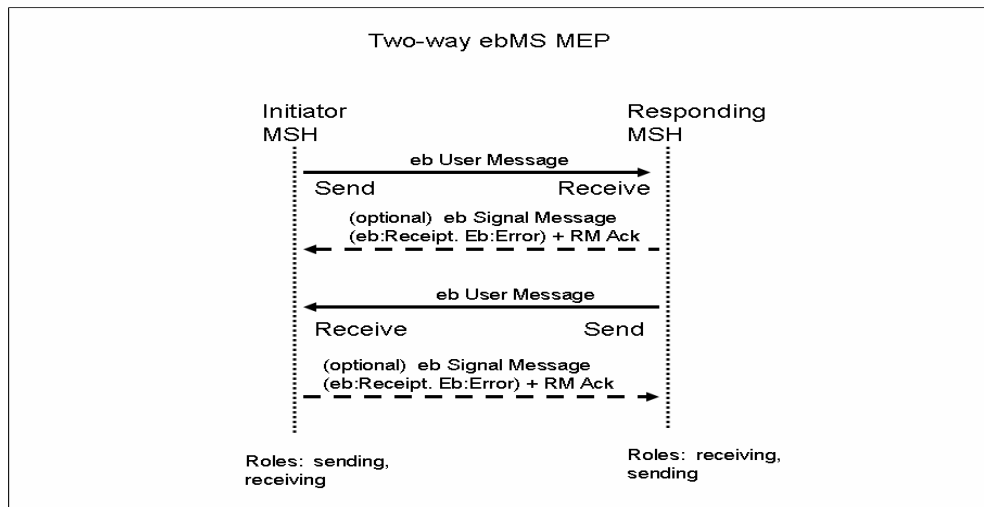
Two basic MEPs are supported in ebMS 3.0.: 2 つの基本的 MEP が ebMS3.0 ではサポートされる。

- **One-way MEP:** involves the transfer of a single business message (or action message), followed by some optional message(s) flowing in the other direction, that provide some status about the initial message.
一方向MEP: 一方向のビジネスメッセージ(又はアクション・メッセージ)の転送と、それに続く最初のメッセージに関する何らかのステータスを提供する、反対方向に流れるオプションのメッセージからなる。



- Two-way MEP: involves the transfer of a business (or action) message in one direction, followed by the transfer of another business message in the opposite direction (the “response”). Each one of these business messages may be followed by some optional message(s) flowing in the other direction, that provide some status about it. The following figure shows an asynchronous Two-way MEP (synchronous cases are shown in later sections).

双方向MEP: 一方向のビジネス(またはアクション)メッセージの転送と、それに続く逆方向の別のビジネスメッセージ(“返信”)の転送からなる。こうした各ビジネスメッセージには、メッセージについてのステータスを提供する逆方向に流れる何らかのオプションのメッセージが続くことがある。次の図は、非同期双方向MEPを示す(同期の例は後のセクションで示す)。



6.2 メッセージタイプと用語 (Message Types and Terminology)

6.2.1 ebMS メッセージの異なったタイプ (Different Types of ebMS Messages)

In the following, a distinction is made between ebMS signal messages and RosettaNet signal messages.

以下で、ebMS 信号メッセージと RosettaNet 信号メッセージが区別されている。

- ebMS User message: Such a message has a business payload, and direct significance for the application layer. It is subject to the “submit” and “deliver” operations mentioned in the messaging model, section 6.1. It is subject to ebMS Receipts.

ebMSユーザ・メッセージ: このようなメッセージは、ビジネス・ペイロードを有し、アプリケーション・レイヤにとって直接的な重要性を持つ。通信モデル6.1項に記載の“送信”及び“配信”操作の対象となる。ebMS受領の対象である。

- ebMS Signal message: Such a message has no direct significance for the application layer: instead, it is a message that facilitates the exchange or informs on the status of other ebMS messages. Such signals can be “piggy-backed” on other messages as they are in form of SOAP header elements. The following message types are in this category:

ebMS信号メッセージ: このようなメッセージは、アプリケーション層に対して直接的な重要性を持たない。むしろ、メッセージの交換を円滑に進め、他のebMSメッセージの状況について知らせるメッセージである。そのような信号は、SOAPヘッダ要素の形なので、他のメッセージに“上乘せられて”いることもある。次のようなメッセージ・タイプが、このカテゴリーに入る。

- ebMS Error message
- ebMS Pull message
- ebMS Receipt messages (eb:Receipt) are also considered as ebMS signals: Although they do have application relevance, they usually are not intended to be delivered directly to applications the same way a User message is.

ebMS 受領メッセージ(eb:Receipt)も、ebMS信号とみなされる:アプリケーション的な関連はあるが、通常は、ユーザー・メッセージの様にはアプリケーションに直接送られるようにはなっていない。

- Accessory signals: These are SOAP messages that do not have an ebMS header, but assist in some way the transfer of ebMS messages, e.g. from a QoS point of view. Such messages may be supported by external specifications accessory to ebMS, such as Reliable Messaging. Such signals can often be “piggy-backed” on other messages as some of them are in form of SOAP headers (e.g. RM Acks). It is not intended to be visible beyond the ebMS messaging layer (although it may generate some form of notification to the upper layer; e.g. an error notification). The following message types are in this category:

アクセサリ信号:これらはebMSヘッダを持たないが、何らかの方法でebMSメッセージの転送を援助する(例、QoS の観点から)SOAPメッセージである。このようなメッセージは、信頼性通信など、ebMSに付属する外部仕様によってサポートされている場合がある。そのような信号の中には、SOAPヘッダ要素の形のものもあるため、他のメッセージに”上乗せされて”いることもある(例、RM Acks)。(エラー通知など、何らかの形の通知を上部のレイヤ上に発生させることがあるが)ebMSメッセージ層を超えて見えるようにはなっていない。次のようなメッセージ・タイプが、このカテゴリーに入る。

- Mapping Reliable Messaging protocol messages (management of RM sequences, etc)
信頼性通信プロトコル・メッセージのマッピング (高信頼性通信シーケンスの管理など)。
- Reliable Messaging acknowledgements. That is for the exclusive usage of the ebMS protocol. It would generally be at lower level than message choreographies defined by RosettaNet PIPs.
信頼性通信の確認。それはebMSプロトコル専用である。RosettaNet PIPで定義されたメッセージ・コレオグラフィよりも下位のレベルにあることが多い。
- SOAP Faults or HTTP errors (with error status codes)
SOAPフォルト又は、HTTPエラー(エラー・ステータス・コードを伴う)。

6.2.2 RosettaNet メッセージを ebMS メッセージへのマッピングについて (Mapping of RosettaNet messages to ebMS Messages)

The following rules define how RosettaNet messages map to ebMS Messages:

以下のルールは、どのように RosettaNet メッセージが、ebMS メッセージにマップするかを定義する。

- A RosettaNet Action message is always mapped to an ebMS User message: These are the messages to be consumed by applications, with a rich ebMS “business header” (in eb: Messaging element) the profiling of which is defined in section 4.

RosettaNet のアクション・メッセージは、常に ebMS ユーザー・メッセージにマップされる:これらは情報量豊かな ebMS “ビジネス・ヘッダ”(eb:通信要素)を持ち、アプリケーションにより使用されるメッセージで、そのプロファイルはセクション 4 に定義されている。

- A RosettaNet signal message (receipt, exception) is, from an ebMS perspective, closer to application than to ebMS signaling. It maps to an ebMS User message too. ebMS V2 does not handle these any differently from action messages. The signal content is treated in ebMS V2 as any other application payload.

RosettaNet信号メッセージ(受領、例外)は、ebMSの観点から見ると、ebMS信号よりもアプリケーションに近い。それはebMSユーザー・メッセージにもマップする。ebMS V2ではこれらをアクション・メッセージと異なった処理をしない。ebMS V2では、信号内容は、他のアプリケーション・ペイロードと同様に扱われる。

- NOTE: In some cases where non-repudiation is not required or does not involve payload validation (see 6.3), the ebMS V3 Receipt - which is an ebMS Signal message (as opposed to an ebMS User message) - will be used instead of the RosettaNet Receipt. In other cases when Reliable Messaging is used, RM Acks will play a similar role.

注: 否認防止が必要ない場合、又はペイロードの検証をしない場合(6.3項参照)、ebMS V3の受領 - それは、ebMS信号メッセージであるが (ebMSユーザー・メッセージとは反対に)、- は、RosettaNetの受領の代わりに使われる。高信頼性通信が使われる他のケースでは、高信頼性通信のAcksが、似たような役割を果たす。

- It is possible to piggyback ebMS signal messages or accessory message (acknowledgements, errors, Receipt) on ebMS User messages, merging into one message what could have been considered as two separate messages.

ebMS信号メッセージまたはアクセサリ・メッセージ(確認、エラー、受領)をebMS ユーザー・メッセージに上乗せされ、2つの別々のメッセージと見なされるようなメッセージを1つのメッセージにまとめることが可能である。

The following figure shows how RosettaNet message types map to ebMS V3. They all map to ebMS User Messages, except in some cases the RosettaNet Receipt Acknowledgement is substituted by the ebSMS Receipt signal (eb:Receipt).

次の図は、RosettaNet メッセージ・タイプが、どの様に ebMS V3 上にマップするかを示している。RosettaNet 受領確認が ebSMS 受領信号 (eb: Receipt) に置き換わっている一部のケース以外は、いずれも ebMS ユーザー・メッセージにマップする。

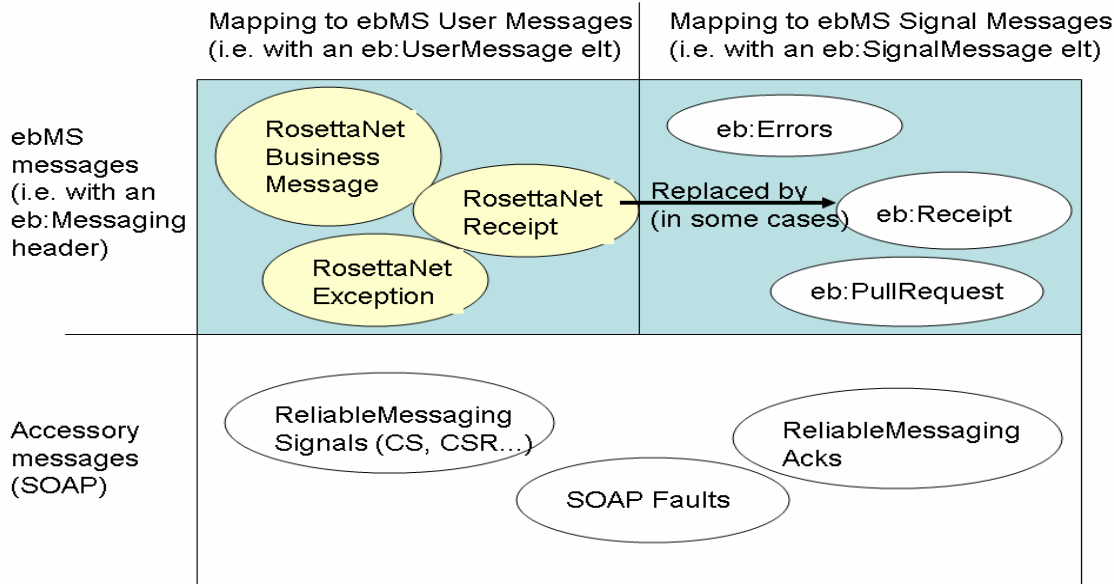
- White-colored ovals show all types of messages involved in ebMS exchanges, that do not have RosettaNet (RNIF) counterparts but assist the exchange in various functions.

白い楕円は、RosettaNet (RNIF) に相当するものがないが、様々な機能でメッセージ交換を支援する、ebMS メッセージ交換に関わる全てのタイプのメッセージを示す。

- Peach-colored ovals show RosettaNet messages and how they are categorized in terms of ebMS messages.

桃色の楕円は、RosettaNet のメッセージ及びそれらが ebMS メッセージの観点からどのように分類されているかを示している。

RosettaNet Messages and ebMS Messages



6.3 受領の意味: 単純否認防止と検証後に否認防止。 (Receipt Semantics: Simple and Validating Non-Repudiation)

We consider here the basic message sequence of sending an Action message, and getting back a Receipt Acknowledgement or an Exception. As ebMS V3 provides both (a) a Reliable Messaging (RM) feature, and (b) a Receipt signal message, it appears that in most cases these ebMS features make the RosettaNet Receipt Acknowledgement redundant:

我々はここで、アクション・メッセージを送信し、受領確認または例外を受信することからなる基本的なメッセージ・シーケンスについて検討する。ebMS V3 は、(a)高信頼性メッセージング機能と(b)受領信号メッセージの両方を用意するので、大半の場合、この ebMS 機能によって RosettaNet 受領確認が不必要なものに見える。

- A retry mechanism is specified in RN, triggered by not receiving a Receipt Acknowledgement in time. It is controlled with a RetryCount parameter, and Time to Acknowledge.

ある再試行メカニズムがRN (RosettaNet) の仕様であり、時間内に受領確認を受け取らなかった時に起動される。これは再試行回数パラメータ及び確認までの時間によって制御される。

- ebMS 3.0 has a similar mechanism of retries, until an ebMS acknowledgement (Reliable Messaging - or RM - Ack) is received. A maximum number of retries as well as a retry interval, are specified.

ebMS 3.0は、ebMS確認(高信頼性通信又はRM 確認)を受信するまで続く類似の再試行メカニズムを持っている。再試行最大数ならびに再試行間隔は指定される。

The mapping of the parameters of RM features to RosettaNet equivalent has been described in Appendix A.

RM(高信頼性通信)機能のパラメータをRosettaNetの同等機能へのマッピングは、付録Aで説明している。

The RN Retry and Acknowledgement mechanisms can be largely supported by ebMS 3.0 Reliable Messaging mechanism, except for two aspects:

RN再試行及び確認のメカニズムは、2つの側面を除いて、ebMS 3.0の高信頼性通信機能によってほとんどがサポート可能である。

- Document Validation: The meaning of an RN Receipt Acknowledgement usually goes beyond message reception, to include document validation (grammar level). The ebMS acknowledgement does not have this semantics.

ドキュメントの検証: RosettaNetの受領確認とは、通常のメッセージの受信を超え、ドキュメントの検証(文法レベル)をも含む。ebMSの受領確認にはこの意味はない。

- Non-repudiation of Receipt. Receipt Acknowledgements are used for non-repudiation of receipt. ebMS RM acknowledgements cannot be used for this purpose.

受領の否認防止: ロゼッタネットの受領確認は受領否認防止に用いられる。ebMSの高信頼性通信確認は、この目的には使えない。

On these same functions, the ebMS Receipt signal compares as follows with the RN Receipt Acknowledgement:

これらの同じ機能について、ebMS受領信号とRN受領確認応答との比較は、以下の通りである:

- Document Validation: The ebMS Receipt signal is generally sent back by the MSH before payload validation occurs. It cannot be counted on to implement this semantics.

ドキュメントの検証: 通常本文の検証の前にebMS受領信号は、MSHによって送り返される。この意味で実装することができない。

- Non-repudiation of Receipt. The (signed) ebMS Receipt signal can be used for this purpose and replace here the RN Receipt Acknowledgement.

受領の否認防止: (署名された)ebMS受領信号はこの目的のために使うことができ、RNの受領確認と代わることができる。

In case non-repudiation of receipt is required, the signed ebMS Receipt signal (eb:Receipt) MUST be used – whether or not RM is also used. This ebMS Receipt signal must include a digest of the original message. It MUST include the ebbpsig:NonRepudiationInformation child element, as defined in the ebBP Signal Schema [ebBP-SIG].

受領の否認防止が求められる場合、高信頼性通信が使用されていなくても、署名されたebMS受領信号 (eb:Receipt)を使用しなければならない。このebMS受領信号は、元のメッセージのダイジェスト値を含まなければならない。それは、ebBP情報スキーマ[ebBP-SIG]に記載のebbpsig:NonRepudiationInformation子要素を持たなければならない。

Two variants of non-repudiation of receipts are supported in this profile:

受領の否認防止の2つの変形が、このプロファイルではサポートされる:

- Simple non-repudiation: In this variant, the signed eb:Receipt is sent back before document validation occurs. The eb:Receipt only means that the message has been well received and that the receiving endpoint is taking responsibility for further processing (including payload validation).

単純な否認防止: この変形では、文書の検証が行われる前に、署名されたeb:Receiptは送り返される。eb:Receiptの意味は、単にメッセージは正常に受信され、受信した所が更なる処理(本文の検証を含む)のために責任を持っていることである。

- Validating non-repudiation: In this variant, the signed eb:Receipt is sent back only after the document validation occurs. The eb:Receipt means that the message has been well received and that it is considered as valid for further business processing.

検証後に否認防止: この変形では、文章の検証が終了した後、署名されたeb:Receiptは送り返される。eb:Receiptの意味は、メッセージが正常に受信され、更なる業務処理のために有効であると考えられることを意味する。

The recommended profiling is as follows: 推奨されるプロファイルは、以下の通り:

When non-repudiation of receipt is not required

Do NOT use the RosettaNet Receipt Acknowledgement (positive) signals.
RosettaNet 受領確認(肯定)信号は使用禁止。

Instead, use the ebMS3 Receipt signal message. In that case, the ebbsig:NonRepudiationInformation MAY be absent. No other element than ebbsig:NonRepudiationInformation is allowed by this profile as child of eb:Receipt. If this element is not used, then eb:Receipt MUST be empty.

代わりに、ebMS3 受領信号メッセージを使用する。その場合、ebbsig:NonRepudiationInformation が脱落する可能性がある。当プロファイルでは、ebbsig:NonRepudiationInformation 以外の要素は、eb:Receipt の子要素として許可されない。この要素を使用しない場合、eb:Receipt は空でなければならない。

NOTE: In case Reliable Messaging is used (generating RM Acks and automatic resends), the use of ebMS3 Receipt signal is optional, as the RM Ack will provide reception awareness.

高信頼性通信が使用される(RM Ack 及び自動再送が生成される)場合、RM Ack が受領確認を提供するので、ebMS3 受領信号の使用はオプションとなる。

In case of invalid payload: only then would an RosettaNet exception message (type:Receipt Acknowledgement Exception) be sent back, as the result of a validation check occurring at higher level than the messaging layer. The sending of this exception SHOULD use Reliable Messaging supported by ebMS3. It MUST be sent as a regular ebMS User Message. The absence of such a signal tells the sender that the payload was valid. Note: a OA1 PIP could be used too.

無効ペイロードの場合: 通信層より高いレベルで行われている検証の結果として、その時だけ、RosettaNet 例外メッセージ(type:Receipt Acknowledgement Exception) が送り返される。この例外の送信は、ebMS3 でサポートされる高信頼性通信を使用すべきである。それは、正規の ebMS ユーザー・メッセージとして送信しなければならない。該当信号がなければ、送信者はペイロードが有効であったとってしまう。注: PIP OA1 も利用可能。

When non-repudiation of receipt is required

Often there are several steps in a non-repudiation mechanism (or layers). Validation of the payload may not belong to the initial step. Also, it appears that different users give different meaning to non-repudiation, e.g. regarding the degree of payload validation. For these reasons, two options are available to users, depending on the precise semantics of non-repudiation that is required.

否認防止の機構(あるいは層)には、いくつかのステップがあることが多い。ペイロードの検証は、最初のステップには属さない可能性がある。又、例えば、ペイロード検証の程度など、ユーザーが異なれば否認防止に異なる意味を与えるように見える。このような理由でユーザーは、求められる否認防止の厳密な意味に応じて2つのオプションを使用できる。

Option 1: Simple non-repudiation: Payload validation is NOT a recondition to sending the receipt. In that case, an ebMS Receipt signal is sent back (eb:SignalMessage/eb:Receipt header element), including a digest of the received payload. The value of eb:MessageInfo/eb:RefToMessageId MUST refer to the message for which this signal is a receipt. Reliable Messaging may or may not be used.

オプション1:単純否認防止:ペイロードの検証は、受領を送ることの前提条件ではない。その場合、受信したペイロードのダイジェスト値を含めて ebMS 受領信号 (eb:SignalMessage/eb:Receipt header element) が送り返される。 eb:MessageInfo/eb:RefToMessageId の値は、この信号がその受領を示す対象のメッセージを指さなければならない。高信頼性通信は使用される場合もされない場合もある。

Option 2: Validating non-repudiation: Payload validation is a precondition to sending the receipt. In that case, an RN Receipt Acknowledgement will be sent back as a regular ebMS User Message, bundled with the eb:SignalMessage/eb:Receipt header element that includes a digest of the received valid payload. The value of eb:MessageInfo/eb:RefToMessageId MUST refer to the message for which this signal is a receipt. Reliable Messaging may or may not be used.

オプション 2:検証後に否認防止:ペイロード検証は、受領を送ることの前提条件である。その場合RN受領確認は、受信した有効ペイロードのダイジェスト値を含む eb:SignalMessage/eb:Receiptヘッダ要素と束にされて、正規のebMSユーザー・メッセージとして送り返されることになる。 eb:MessageInfo/eb:RefToMessageIdの値は、この信号がその受信を示す対象のメッセージを指さなければならない。高信頼性通信は使用される場合もされない場合もある。

6.4 ITシナリオ:サーバーからサーバーへの一方向PIP (IT Scenario: One-Action PIP from Server to Server)

The business requirement is for one business partner to send another a RosettaNet Business Message, and in return it receives a confirmation of receipt (RN Receipt Acknowledgement or other signal, depending on non-repudiation requirements) or an RN Exception for it. Both partners have “Server” capability, i.e. are able to receive incoming requests.

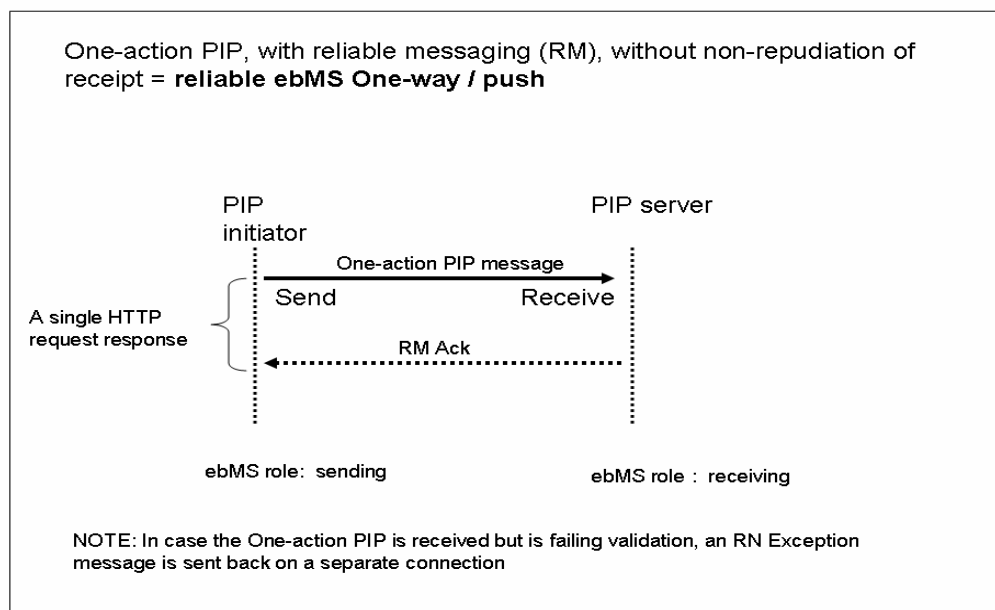
ビジネス要件は、商取引する人が取引先に RosettaNet ビジネス・メッセージを送るためのものであり、逆にそれに対する受領の確認 (否認防止要件に応じ、RN 受領確認乃至は他の信号)、又は RN 例外を受け取る。両者は “サーバー” を有する、即ち、入ってくる要求を受け取ることができる。

The choreography variants are: コレオグラフィの変形は:

6.4.1 受領の否認防止なしの一方 PIP (One-action PIP without Non-Repudiation of Receipt)

In this variant, Reliable Messaging is used and no receipt message (RosettaNet format or ebMS format) is expected. The Reliable Messaging acknowledgement is expected on the same HTTP connection (back-channel).

この変形では、高信頼性通信が使用され、受領メッセージ(RosettaNet形式またはebMS形式)は、届けられない。高信頼性通信の確認は、同一HTTP接続(バック・チャンネル)上で届けられる。



The PMode parameters that control this variant are (in addition to other PMode parameters common to all One-action PIP variants and not specific to this variant):

この変形を制御するPModeパラメータは以下の通りである(他のPModeパラメータに加えて、全ての一方 PIPの変形に共通で、この変形に固有ではない):

General PMode parameters:

- **PMode.MEP:** <http://www.oasis-open.org/committees/ebxml-msg/one-way>
- **PMode.MEPbinding:** <http://www.oasis-open.org/committees/ebxml-msg/push>

PMode[1].ErrorHandling:

- **PMode[1].ErrorHandling.Report.AsResponse:** true.
- **PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer:** true

PMode[1].Reliability:

- **PMode[1].Reliability.AtLeastOnce.Contract:** true
- **PMode[1].Reliability.AtLeastOnce.ReplyPattern:** Response

PMode[1].Security:

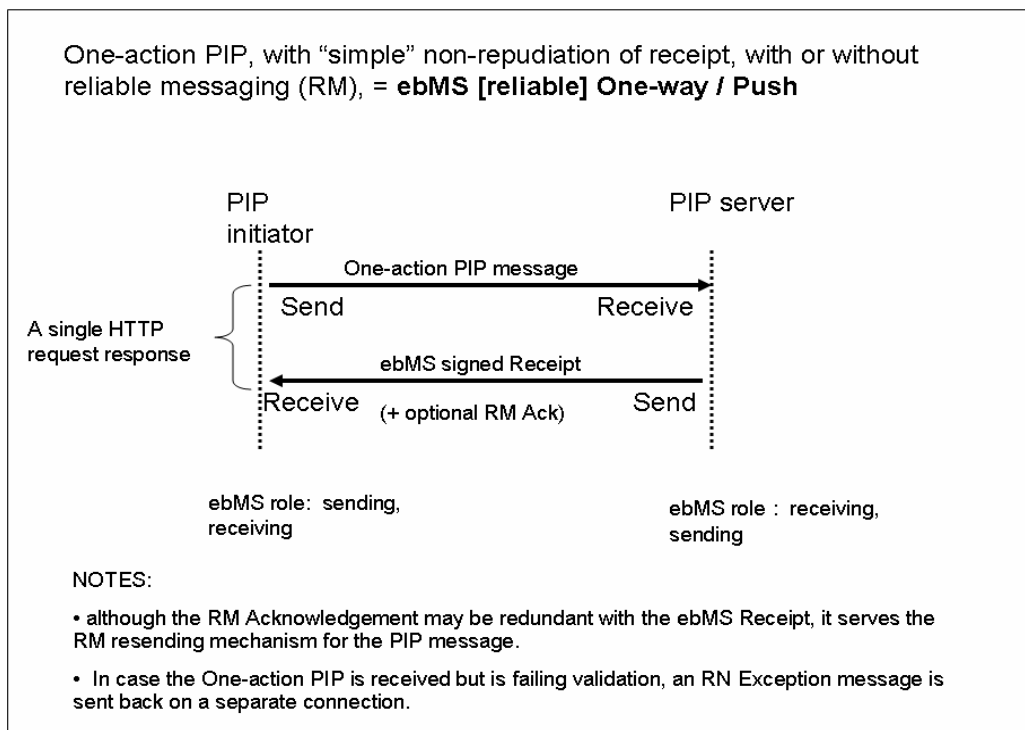
- **PMode[1].Security.SendReceipt:** false

6.4.2 受領の単純否認防止付の一方方向 PIP

One-action PIP, with Simple Non-Repudiation of Receipt)

In this variant, a signed ebMS receipt message (but no RosettaNet Receipt Acknowledgement) is expected. Non-repudiation is required, with “simple” semantics (sent before the message payload is validated). Reliable Messaging is optional, mostly for providing automatic message resending capability.

この変形では、署名付の受領メッセージ(RosettaNet受領確認ではない)がある。“単純”な意味 (メッセージ本文が検証される前に送られる)を持った、否認防止が求められる。高信頼性通信は任意であり、主に自動メッセージ再送信機能を提供するためである。



The PMode parameters that control this variant are (in addition to other PMode parameters common to all One-action PIP variants and not specific to this variant):

この変形を制御するPModeパラメータは以下の通りである(他のPModeパラメータに加えて、全ての一方方向PIPの変形に共通で、この変形に固有ではない):

General PMode parameters:

- **PMode.MEP:** <http://www.oasis-open.org/committees/ebxml-msg/one-way>
- **PMode.MEPbinding:** <http://www.oasis-open.org/committees/ebxml-msg/push>

PMode[1].ErrorHandlerling:

- **PMode[1].ErrorHandlerling.Report.AsResponse:** true.
- **PMode[1].ErrorHandlerling.Report.DeliveryFailuresNotifyProducer:** true. (in case RM is used)

PMode[1].Reliability: (if used)

- `PMode[1].Reliability.AtLeastOnce.Contract`: true
- `PMode[1].Reliability.AtLeastOnce.ReplyPattern`: Response

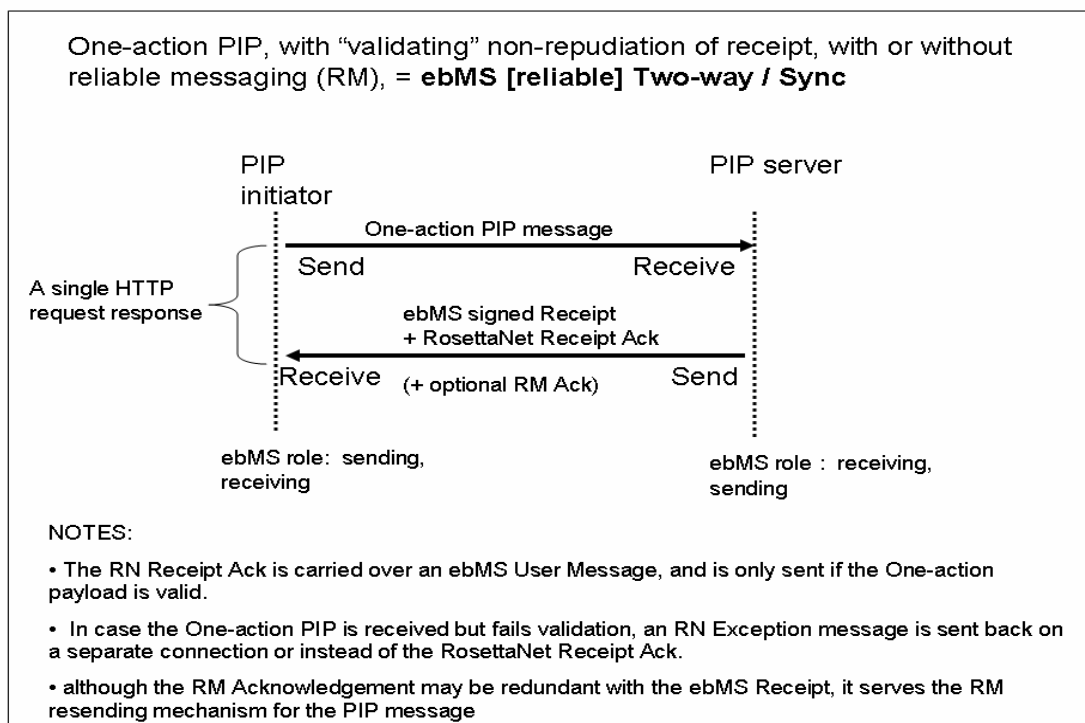
`PMode[1].Security`:

- `PMode[1].Security.SendReceipt`: true
- `PMode[1].Security.SendReceipt.ReplyPattern`: response

6.4.3 検証後に受領の否認防止付の一方 PIP (One-action PIP, with Validating Non-Repudiation of Receipt)

In this variant, both a signed ebMS receipt message and a RosettaNet Receipt Acknowledgement are expected. Non-repudiation is required, with “validating” semantics (sent after the message payload is validated). The MSH on the PIP Server side is waiting for submission of the RN Receipt Acknowledgement to be submitted before sending back the ebMS Receipt header, both piggy-backed on the HTTP response. Reliable Messaging is optional, mostly for providing automatic message resending capability.

この変形では、署名付ebMS受領メッセージとRosettaNet受領確認の両方がある。“検証”したという意味（メッセージ本文が検証された後に送られる）を持った否認防止が求められる。PIPサーバー側にあるMSHは、ebMS受領ヘッダを送り返す前に送信されるはずのRN受領確認の送信を待っており、両方共HTTP応答に上乘せされる。高信頼性メッセージングは任意であり、主に自動メッセージ再送信機能を提供するためである。



The PMode parameters that control this variant are (in addition to other PMode parameters common to all One-action PIP variants and not specific to this variant):

この変形を制御するPModeパラメータは以下の通りである(他のPModeパラメータに加えて、全ての一方 PIPの変形に共通で、この変形に固有ではない):

General PMode parameters:

- PMode.MEP: <http://www.oasis-open.org/committees/ebxml-msg/two-way>
- PMode.MEPbinding:
<http://www.oasis-open.org/committees/ebxml-msg/sync>

PMode[1].ErrorHandling:

- PMode[1].ErrorHandling.Report.AsResponse: true.
- PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer: true. (in case RM is used)

PMode[1].Reliability: (if used)

- PMode[1].Reliability.AtLeastOnce.Contract: true
- PMode[1].Reliability.AtLeastOnce.ReplyPattern: Response

PMode[1].Security:

- PMode[1].Security.SendReceipt: true
- Pmode[1].Security.SendReceipt.ReplyPattern: response

6.4.4 否認防止のためのコールバックによる受領付の一方向 PIP (One-action PIP, with Callback Receipt for Non-Repudiation)

In this variant, the signed ebMS receipt message (and optionally a RosettaNet Receipt Acknowledgement in case of deep non-repudiation) is sent back as a “callback” on a separate connection. The MSH on the PIP Server side is waiting for submission of the RN Receipt Acknowledgement before sending back the ebMS Receipt header, both piggy-backed on the HTTP request. Reliable Messaging is optional, mostly for providing automatic message resending capability.

この変形では、署名付ebMS受領メッセージ(そして、強度な否認防止の場合は任意選択でRosettaNe受領確認)が、別個の接続で“コールバック”として送り返される。PIPサーバー側にあるMSHIは、ebMS受領ヘッダを送り返す前に、RN受領確認の送信を待っており、両方共HTTP応答に上乘せされる。高信頼性通信は任意であり、主に自動メッセージ再送信機能を提供するためである。

6.5 ITシナリオ:ピュア・クライアントからサーバーへの一方向PIP (IT Scenario: One-Action PIP from Pure Client to Server)

The business requirement is same as in 6.4 (Server to Server). But the PIP Initiator cannot act as a Server, i.e. cannot receive incoming requests. It is a “Pure Client”, meaning it either does not have a static IP address, or has connectivity restrictions preventing others to connect to it.

ビジネス要件は、6.4項(サーバーからサーバー)と同じである。しかしPIPイニシエータはサーバーとして機能できない、即ち、入ってくる要求を受けることができない。それは「純粹クライアント“Pure Client”」であり、静的IPアドレスを持たないか、あるいは他クライアントの自分への接続を妨げる接続性制約があることを意味する。

The choreography variants are: コレオグラフィの変形は:

6.5.1 受領の否認防止なしの一方向 PIP (One-action PIP without Non-Repudiation of Receipt)

In this variant, Reliable Messaging is used and no receipt message (RosettaNet format or ebMS format) is expected. The Reliable Messaging acknowledgement is expected on the same HTTP connection (back-channel).

この変形では、高信頼性通信が使用され、受領メッセージ(RosettaNet形式またはebMS形式)はない。高信頼性通信の確認は、同一HTTP接続(バックチャネル)上で届けられる。

The choreography is same as defined in section 6.4.1.

コレオグラフィは、6.4.1 項で定義された通りである。

6.5.2 受領の単純否認防止付の一方向 PIP (One-action PIP, with Simple Non-Repudiation of Receipt)

In this variant, a signed ebMS receipt message (but no RosettaNet Receipt Acknowledgement) is expected. Non-repudiation is required, with “simple” semantics (sent before the message payload is validated). Reliable Messaging is optional, mostly for providing automatic message resending capability.

この変形では、署名付の受領メッセージ(RosettaNet受領確認ではない)がある。“単純”な意味(メッセージの本文が検証される前に送られる)を持つ否認防止が求められる。高信頼性通信は任意であり、主に自動メッセージ再送信機能を提供するためである。

The choreography is same as defined in section 6.4.2.

コレオグラフィは、6.4.2 項で定義された通りである。

6.5.3 確認付受領の否認防止の一方向PIP (One-action PIP, with Validating Non-Repudiation of Receipt)

In this variant, both a signed ebMS receipt message and a RosettaNet Receipt Acknowledgement are expected. Non-repudiation is required, with “validating” semantics (sent after the message payload is validated). The MSH on the PIP Server side is waiting for submission of the RN Receipt Acknowledgement to be submitted before sending back the ebMS Receipt header, both piggy-backed on the HTTP response. Reliable Messaging is optional, mostly for providing automatic message resending capability.

この変形では、署名付ebMS受領メッセージとRosettaNet受領確認の両方が届けられる。“検証”したという意味(メッセージの本文が検証された後に送られる)を持つ否認防止が求められる。PIPサーバー側にあるMSHは、ebMS受領ヘッダを送り返す前に、送信されるはずのRN受領確認の送信を待っており、両方共HTTP応答に上乘せられる。高信頼性通信は任意であり、主に自動メッセージ再送信機能を提供するためである。

The signed ebMS receipt message (and optionally a RosettaNet Receipt Acknowledgement in case of deep non-repudiation) is sent back as a “callback” on a separate connection.

署名付ebMS受領メッセージ(そして、強度な否認防止の場合は任意選択でRosettaNet受領確認)が、別個の接続で“コールバック”として送り返される。高信頼性通信は任意であり、主に自動メッセージ再送信機能を提供するためである。

The choreography is same as defined in section 6.4.3.

コレオグラフィは、6.4.3 項で定義された通りである。

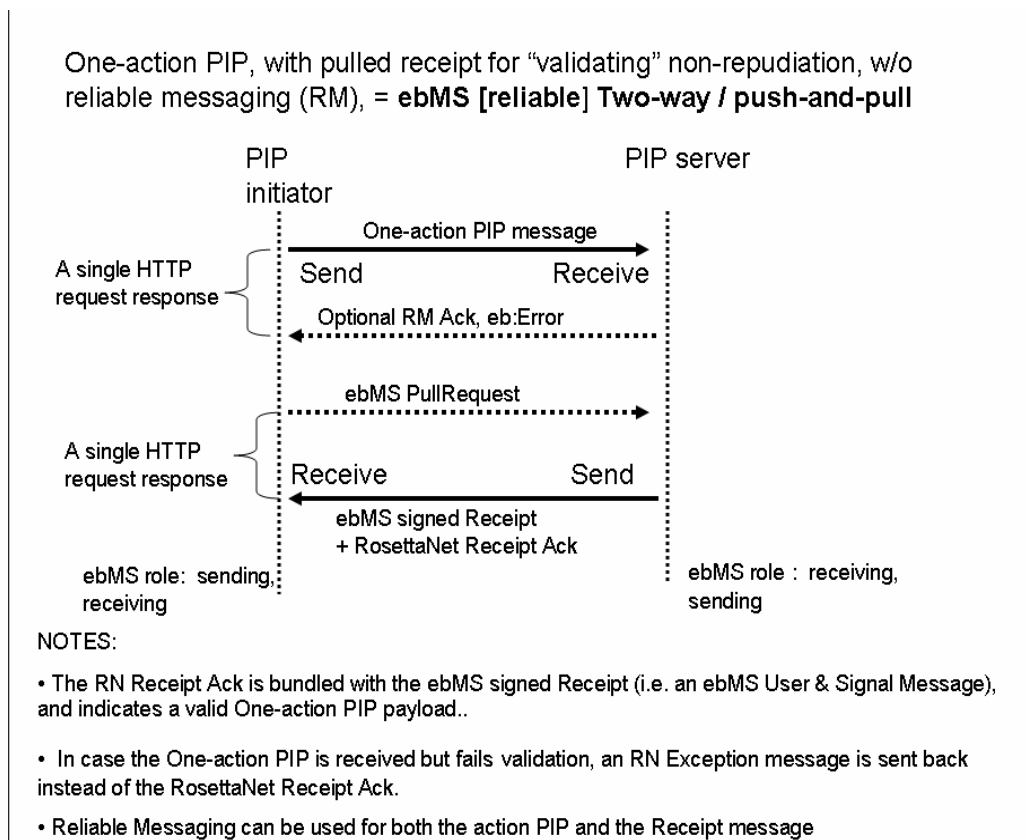
6.5.4 検証後に否認防止のための取り込んだ受領付一方向 PIP (One-action PIP, with Pulled Receipt for Validating Non-Repudiation)

This case typically applies when the validation time for the payload document prohibits a synchronous response as in 6.5.3.

このケースは、6.5.3 項にあるように、本文文書についての検証時間が同期応答を妨げる場合に一般的に適用される。

The MSH on the Pure Client side is sending PullRequest signals until the PIP Server side sends back the RN Receipt Acknowledgement along with the ebMS Receipt header, both piggy-backed on the HTTP response. Reliable Messaging is optional, mostly for providing automatic message resending capability

純粋クライアント(Pure Client)側にある MSH は、PIP サーバー側が ebMS 受領ヘッダと一緒に RN 受領確認を返信するまで、PullRequest 信号を送信しており、両方共 HTTP 応答に乗せられる。高信頼性通信は任意であり、主に自動メッセージ再送信機能を提供するためである。



The PMode parameters that control this variant are (in addition to other PMode parameters common to all One-action PIP variants and not specific to this variant):

この変形を制御するPModeパラメータは以下の通りである(全ての一方方向PIPの変形に共通で、この変形に固有ではない他のPModeパラメータに加えて):

General PMode parameters:

- **PMode.MEP:** <http://www.oasis-open.org/committees/ebxml-msg/two-way>
- **PMode.MEPbinding:**
<http://www.oasis-open.org/committees/ebxml-msg/push-and-pull>

PMode[2].BusinessInfo:

- **PMode[2].BusinessInfo.MPC:** this parameter must specify a Message Partition Channel where Receipts will be assigned for pulling.
このパラメータは、受領が取り込み用に割り当てられることになる場合、メッセージ区分チャンネル(MPH)を指定しなければならない。

PMode[1].ErrorHandling:

- **PMode[1].ErrorHandling.Report.AsResponse:** true.
- **PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer:** true. (in case RM is used)

PMode[1].Reliability: (if used)

- **PMode[1].Reliability.AtLeastOnce.Contract:** true
- **PMode[1].Reliability.AtLeastOnce.ReplyPattern:** Response

PMode[1].Security:

- **PMode[1].Security.SendReceipt:** true
- **PMode[1].Security.SendReceipt.ReplyPattern:** pulled

6.6 IT シナリオ: サーバーから純粋クライアントへの一方向PIP (IT Scenario: One-Action PIP from Server to Pure Client)

The business requirement is same as in 6.4 (Server to Server) and 6.5 (Client to Server). But the sender of the One-action PIP cannot initiate the transfer because its partner is a Pure Client. In that case, the action PIP receiver (Pure Client) is the PIP Initiator.

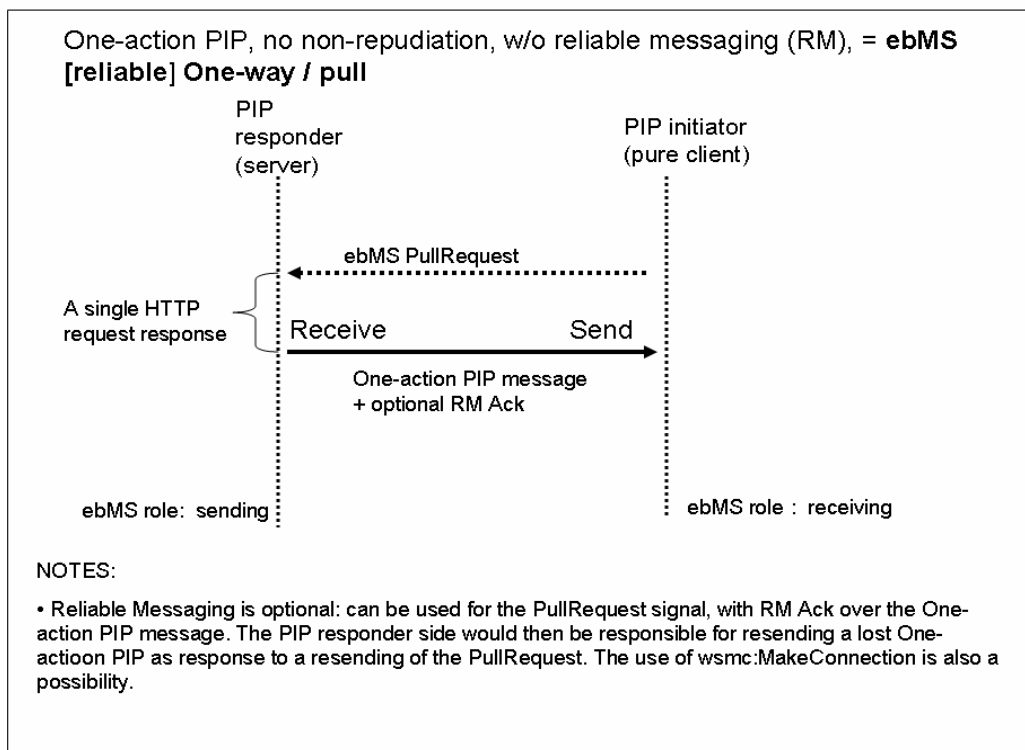
ビジネス要件は、6.4 項(サーバーからサーバー)と 6.5 項 (クライアントからサーバー)と同じである。しかし一方向 PIP の送信者は、その相手が純粋クライアントであるため、転送を開始できない。その場合、PIP 受信者(純粋クライアント)が PIP 開始者である。

The choreography variants are: コレオグラフィ(振り付け)変形は次の通り:

6.6.1 受領の否認防止なしの一方向PIP (One-action PIP without Non-Repudiation of Receipt)

In this variant, no receipt message (RosettaNet format or ebMS format) is expected. Reliable Messaging is used for the PullRequest signal, with acknowledgement expected on the same HTTP connection (back-channel). Optionally an RM Ack is sent for the Action PIP, on a separate connection (e.g. bundled with the next PullRequest).

この変形では、受領メッセージ(RosettaNetフォーマットまたはebMSフォーマット)はない。高信頼性通信は、同一 HTTP接続(バックチャネル)上で届けられる確認を持った、PullRequest信号のために使用される。任意として、RM Ackは別の接続上でAction PIPのために送信される(例えば、次のPullRequestに含まれる)。



The PMode parameters that control this variant are (in addition to other PMode parameters common to all One-action PIP variants and not specific to this variant).

この変形を制御するPModeパラメータは以下の通りである(他のPModeパラメータに加えて、全ての一方向PIPの変形に共通で、この変形に固有ではない):

General PMode parameters:

- **PMode.MEP:** <http://www.oasis-open.org/committees/ebxml-msg/one-way>
- **PMode.MEPbinding:** <http://www.oasis-open.org/committees/ebxml-msg/pull>

PMode[1].BusinessInfo:

- **PMode[1].BusinessInfo.MPC:** this parameter must specify a Message Partition Channel where the Action PIP message will be assigned for pulling.
このパラメータは、Action PIPメッセージが取り込み用に割り当てられる場合、メッセージ区分チャンネルを指定しなければならない。

PMode[1].ErrorHandling:

- **PMode[1].ErrorHandling.Report.AsResponse:** false. (errors regarding the Action PIP must be sent as callback)
(Action PIPに関するエラーは、コールバックとして送られなければならない。)

PMode[1].Reliability: (if used. This applies to the PullRequest signal as well)
(もし使用される場合、PullRequest 信号にも同様に適用される。)

- **PMode[1].Reliability.AtLeastOnce.Contract:** true
- **PMode[1].Reliability.AtLeastOnce.ReplyPattern:** Response (this concerns the PullRequest message, N/A for the pulled Action PIP message.)
(PullRequest メッセージに関わるもので、取り込まれたAction PIPメッセージに対しては、使用“不可”である。)
- **PMode[1].Reliability.AtLeastOnce.Contract.AckResponse:** False (in case no RM Ack is expected for the Action PIP sent over the HTTP Response).
(HTTP応答上で送られたAction PIPに対して、RM Ackが届けられない場合。)

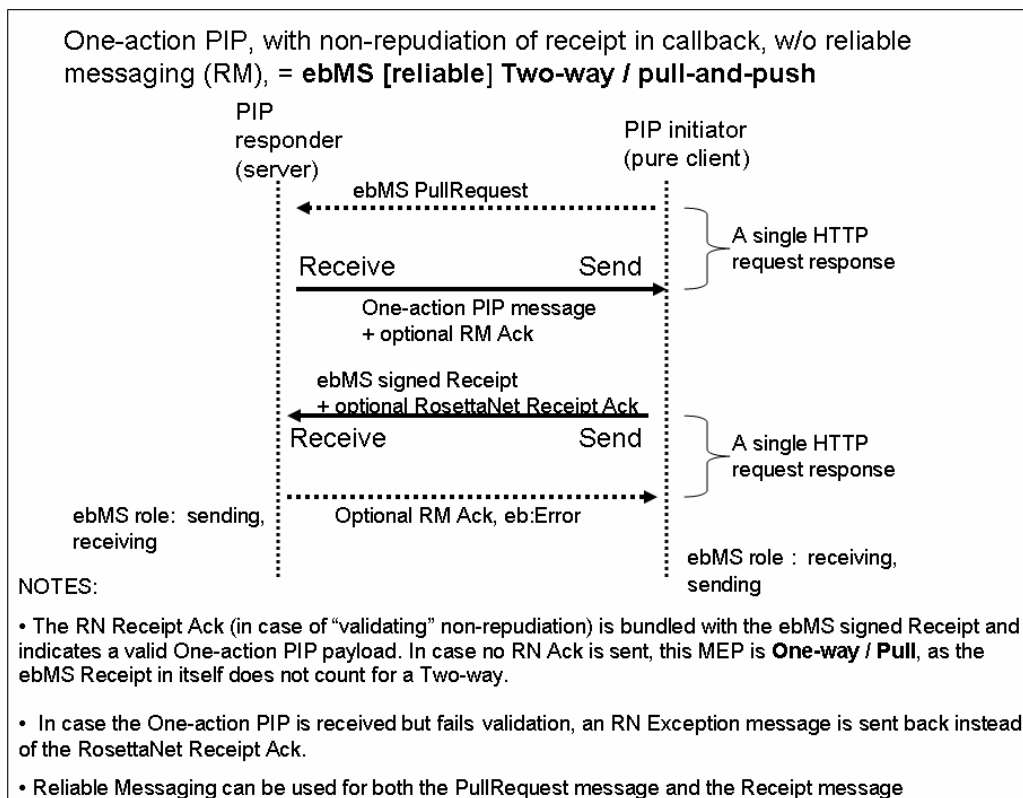
PMode[1].Security:

- **PMode[1].Security.SendReceipt:** false

6.6.2 受領の否認防止付一方向 PIP (One-action PIP, with Non-Repudiation of Receipt)

In this variant, non-repudiation is required. A signed ebMS receipt message is sent in callback mode, with an optional RosettaNet Receipt Acknowledgement (in case of “validating” non-repudiation). Reliable Messaging is optional, mostly for providing automatic message resending capability.

この変形では、否認防止が要求される。署名付ebMS受領メッセージがコールバックモードで、任意のRosettaNet受領確認と一緒に送信される(“検証”後に否認防止の場合)。高信頼性通信は任意であり、主に自動メッセージ再送信機能を提供するためである。



The PMode parameters that control this variant are (in addition to other PMode parameters common to all One-action PIP variants and not specific to this variant).

この変形を制御するPModeパラメータは以下の通りである(全ての一方向PIPの変形に共通で、他のPModeパラメータに加えて、この変形に固有ではない):

General PMode parameters:

- **PMode.MEP:** <http://www.oasis-open.org/committees/ebxml-msg/two-way>. (in case an RN Ack Receipt is expected. Otherwise this MEP would be a One-way/ Pull). (RN Ack受信がある場合、さもないければ、このMEPは一方向/ Pullであろう。)
- **PMode.MEPbinding:** <http://www.oasis-open.org/committees/ebxml-msg/pull-and-push>

PMode[1].BusinessInfo:

- **PMode[1].BusinessInfo.MPC:** this parameter must specify a Message Partition Channel where the Action PIP message will be assigned for pulling.

このパラメータは、Action PIPメッセージが取り込み用に割り当てられる場合、メッセージ区分チャンネルを指定しなければならない。

PMode[1].ErrorHandling:

- PMode[1].ErrorHandling.Report.AsResponse: false.
- PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer: true.
(in case RM is used)

PMode[1].Reliability: (if used. These parameters apply as well to the PullRequest message)

(もし使用されるならば、これらのパラメータは、PullRequest メッセージにも同様に適用される。)

- PMode[1].Reliability.AtLeastOnce.Contract: true
- PMode[1].Reliability.AtLeastOnce.ReplyPattern: Response (this concerns the PullRequest message, N/A for the pulled Action PIP message.)
- PMode[1].Reliability.AtLeastOnce.Contract.AckResponse: False
(in case no RM Ack is expected for the Action PIP sent over the HTTP Response).
(HTTP応答上で送られたAction PIPに対して、RM Ackがない場合。)

PMode[1].Security:

- PMode[1].Security.SendReceipt: true
- PMode[1].Security.SendReceipt.ReplyPattern: callback

7 QoS方針 (Quality of Service Policies)

7.1 一般的なセキュリティ方針 (General Security Policies)

7.1.1 署名と暗号化のルール (Signature and Encryption Rules)

When using digital signatures or encryption, an MSH implementation conforming to this profile is **REQUIRED** to use the Web Services Security X.509 Certificate Token Profile [WSS11-X509].

デジタル署名、又は暗号化を使用する際は、Web サービス・セキュリティ X.509 証明書トークン・プロファイル [WSS11-X509]を使用するために、このプロファイルに準拠する MSH 実装が**求められる**。

This profile **REQUIRES** to use Detached Signatures as defined by the XML Signature Specification [XMLDSIG] when signing ebMS user messages or signal messages. Enveloped Signatures as defined by [XMLDSIG] are not supported by or authorized in this profile.

このプロファイルでは、XML 署名仕様[XMLDSIG]で定義されているように、ebMS ユーザー・メッセージ、又は信号メッセージに署名する際に、メッセージと署名を切り離す分離署名の使用が**求められる**。[XMLDSIG]で定義されているメッセージに署名するエンベロープ署名は、このプロファイルではサポート、又は認可されない。

This profile **REQUIRES** to include the entire eb:Messaging SOAP header block and the SOAP Body in the signature.

このプロファイルでは、eb:Messaging SOAP ヘッダ及び本体全体を署名に含めることが**求められる**。

This profile **REQUIRES** to use the Attachment-Content-Only transform when building application payloads using SOAP with Attachments [SOAPATTACH]. The Attachment-Complete transform is not supported by this profile.

このプロファイルでは、添付ファイル付き SOAP を使用して、アプリケーション・ペイロードを構築する際、添付ファイル[SOAPATTACH]の内容のみの変更が**求められる**。このプロファイルでは、添付ファイル全体の変更はサポートされていない。

This profile **REQUIRES** to include the entire eb:Messaging header block and all MIME body parts of included payloads in the signature.

このプロファイルでは、eb:Messaging ヘッダ・ブロック及び含まれている本文の MIME ボディ部全体を署名に含めることが**求められる**。

An MSH conforming to this profile **SHALL NOT** encrypt the eb:PartyInfo section of the eb:Messaging header. Other child elements of the eb:Messaging header **MAY** be encrypted or left unencrypted as defined by trading partner agreements or collaboration profiles. Messaging header block and all MIME body parts of included payloads in the signature.

このプロファイルに準拠する MSH は、eb:Messaging ヘッダの eb:PartyInfo 部分は暗号化しない。その他の eb:Messaging ヘッダの子要素は、取引当事者間協定書 (TPA) 又は、コラボレーション・プロファイルで規定されるが、暗号化されるか非暗号化のままである可能性がある。

If an user message is to be encrypted and the user-specified payload data is to be packaged in the SOAP Body, MSH implementations are **REQUIRED** to encrypt the SOAP Body.

ユーザー・メッセージが暗号化され、ユーザー指定の本文データが SOAP ボディに内包される場合、SOAP 本体を暗号化するために、MSH の実装が**求められる**。

If an user message is to be encrypted and the user-specified payload data is to be packaged in conformance with the [SOAPATTACH] specification, MSH implementations are REQUIRED to encrypt the MIME Body parts of included payloads.

[SOAPATTACH] 仕様に準拠して、ユーザー・メッセージが暗号化され、ユーザー指定の本文データが内包される場合、包含されている本文の MIME ボディ部を暗号化するために、MSH の実装が**求められる**。

When both signature and encryption are required of the MSH, the message MUST be signed prior to being encrypted, as required in ebMS 3 [ebMS3], section 7.6.

署名と暗号化の両方が MSH に要求される場合、メッセージは ebMS 3 [ebMS3] 7.6 節で求められているように、暗号化の前に署名されなければならない。

7.1.2 取り込みの許可 (Pull Authorization)

Message pulling requires authorization in addition to general authentication security, because pulling is targeted to a Message Partition Channel (MPC). Two different MSHs pulling from the same MSH should only be authorized to pull from their dedicated MPC.

情報の取り込みには、一般的な認証セキュリティに加え、認可が求められる。なぜなら取り込みには、情報区分チャンネル(MPC)をターゲットとしているため、同一の MSH(Message Service Handler)から取り込もうとした 2 つの異なる MSH は、専用の MPC(情報区分チャンネル)からの取り込みのみが認められるべきである。

A Sending MSH conforming to this profile MUST be able to selectively authorize a Receiving MSH that sends a PullRequest in two ways (Options 1 and 2 below), and MAY authorize pulling as Option 3 below:

このプロファイルに準拠する送信 MSH は、2 つの方法(下記のオプション 1 及び オプション 2)で取り込み要求を送信する受信 MSH を選択的に認可できなくてはならない。又、下記のオプション 3 として、取り込みを認可してもよい。

- Authorization Option 1: Use of the WSS security header targeted to the “ebms” actor, as specified in section 7.10 of ebMS V3, with the wsse:UsernameToken profile. This header may either come in addition to the regular wsse security header (XMLDsig for authentication), or may be the sole wsse header, if a transport-level secure protocol such as SSL or TLS is used. An example of message is given in Appendix ...

認可オプション 1: ebMS V3 の 7.10 節に規定される wsse:UsernameToken プロファイル付きの“ebms”を対象として、WSS セキュリティ・ヘッダを使用する。SSL や TLS などの通信レベルの安全なプロトコルが使用される場合、このヘッダは、通常の wsse セキュリティ・ヘッダ(XMLDsig による認可)に加えて使用される、または単に wsse ヘッダとなる可能性がある。

- Authorization Option 2: Use of a regular wsse security header (XMLDsig for authentication, use of X509), and no additional wsse security header targeted to “ebms”. In that case, the MSH must be able to use the credential present in this security header for Pull authorization, i.e. to associate these with a specific Message Partition Channel (MPC).

認可オプション 2: 通常の wsse セキュリティ・ヘッダ(XML デジタル署名による認可、X509 の使用)を使用し、“ebms”を対象とする追加の wsse セキュリティ・ヘッダは使用しない。この場合、MSH はこのセキュリティ・ヘッダにある認証情報を取り込み認可に使用できるようにしなければならない。つまり、これらを特定の情報区分チャンネル(MPC)と関連付けなくてはならない。

- Authorization Option 3: In addition to the two previous authorization options an implementation MAY optionally decide to support a third authorization technique, based on transient security (SSL or TLS). SSL/TLS can provide certificate-based client authentication. Once the identity of the Pulling client is established, the Security module may pass this identity to the ebms module, which can then associate it with the right authorization entry, e.g. the set of MPCs this client is allowed to pull from.

認可オプション 3: 前述の 2 つの認可オプションに加え、実装は一時的なセキュリティ (SSL 又は TLS) に基づき、任意で三番目の認可方法をサポートすることを決定できる。SSL/TLS は、証明書ベースのクライアント認証を提供できる。情報取込みクライアントの識別子が構築されると、セキュリティ・モジュールはこの識別子を ebms モジュールに渡し、次いで、それを正しい認証手続き (例: このクライアントが取込みを許可されている一連の MPC) と関連付けることができる。

This third authorization option – compatible with although not specified in ebMS Core V3 - relies on the ability of the ebms module to obtain the client credentials. This capability represents an (optional) new feature.

ebMS Core V3 に規定されていないが、それに適合するこの 3 番目の認可オプションは、クライアント認証情報を取得する ebms モジュールの能力に依存している。この能力は、(オプション) 新機能を示している。

7.2 受領の取り扱い (Handling of Receipts)

When a Receipt is to be used solely as a reception indicator the sender of the Receipt MAY decide to not insert the ebbpsig:NonRepudiationInformation child element. No other element than ebbpsig:NonRepudiationInformation is allowed as child of eb:Receipt. If this element is not used, then eb:Receipt MUST be empty.

受領が受信インジケータとしてのみ使用される場合、受領の送信者は、ebpsig:NonRepudiationInformation 子要素を挿入しないであろう。ebpsig:NonRepudiationInformation 以外の要素は eb:Receipt の子要素として認可されていない。この要素が使用されない場合は、eb:Receipt は空でなければならない。

Non Repudiation of Receipt (NRR) requires eb:Receipt signals to be signed, and to contain digests of the original message parts for which NRR is required.

受領の否認防止では、eb:Receipt 信号への署名が必要となり、また eb:Receipt 信号に NRR が求められる元のメッセージ部分のダイジェストを含める必要がある。

When signed receipts make use of default conventions, the Sending message handler (i.e. sending messages for which signed receipts are expected) MUST identify message parts using Content-Id values in the MIME headers, and MUST sign the SOAP body and all attachments using the <http://docs.oasis-open.org/wss/oasis-wss-SwAProfile-1.1#Attachment-Content-Signature-Transform> within the SignedInfo References list.

署名された受領が初期設定の規則を利用する際、送信メッセージ・ハンドラー (つまり、署名された受領が求められる送信メッセージ) は、MIME ヘッダの Content-ID 値を使用して、メッセージ部分を識別しなければならない、又、SignedInfo 参照リスト内の <http://docs.oasis-open.org/wss/oasis-wss-SwAProfile-1.1#Attachment-Content-Signature-Transform> を使用して、SOAP 本体及び全ての添付ファイルに署名しなければならない。

As a reminder, the Sending message handler MUST not encrypt any signed content before signing (Section 7.6 in ebMS V3). If using compression in an attachment, the Sending message handler MUST sign the data after compression (see section 3.1). Variations from default conventions can be agreed to bilaterally, but conforming implementations are only required to provide receipts using the default conventions described in this section.

念を押しておく、送信メッセージ・ハンドラーは、署名前にいかなる署名されるべきコンテンツも暗号化してはならない。(ebMS V3 の 7.6 項: 暗号化する前に署名しなければならない)。添付ファイルを圧縮する場合は、送信メッセージ・ハンドラーは圧縮後にデータに署名しなければならない (3.1 節参照)。初期設定の規則の変更は両者間

で合意できるが、このプロファイルに準拠した実装は本節に記載の初期設定の規則を使用して受領を提供することのみ求められる。

In this profile, when sending a receipt for a message that has been digitally signed the eb:Receipt signal MUST itself be digitally signed, and non-repudiation feature MUST be used: the eb:Receipt element MUST contain the information necessary to provide non-repudiation of receipt of the original message.

このプロファイルでは、デジタル署名されたメッセージの受領を送信する場合、eb:Receipt 信号自体にデジタル署名し、否認防止機能を使用しなければならない。eb:Receipt 要素は元のメッセージの受領の否認防止を提供するために必要な情報を含んでいなければならない。

NOTE: The digest(s) to be inserted in the ebbp:MessagePartNRInformation element(s) or the Receipt, related to the original message parts for which a receipt is required, may be obtained from the signature information of the original message (ds:SignedInfo element), as only those parts that have been signed are subject to NRR. This means a Receiving message handler may not have to compute digests outside its security module.

注：受領が求められる元のメッセージ部分に関連した ebbp:MessagePartNRInformation 要素、又は受領に挿入されるダイジェスト値は、署名されたこれらの部分のみが NRR の対象となるため、元のメッセージ(ds:SignedInfo 要素)の署名情報から取得してもよい。これは、受信メッセージ・ハンドラーがそのセキュリティ・モジュール外のダイジェスト値を計算する必要がない可能性を意味する。

7.3 一般的な信頼性方針 (General Reliability Policies)

It is RECOMMENDED to use the WS-RM contract AtMostOnce whenever AtLeastOnce is used, so that duplicates generated by the resending mechanism can be eliminated.

AtLeastOnce (最低一回)を使用する際は必ず、再送信メカニズムによって生成される重複を排除できるように WS-RM contract の AtMostOnce (最大で 1 回)を使用することが推奨される。

8 展開構成とMSHの要求事項 (Deployment Configurations and MSH Requirements)

8.1 Web サービスへの接続 (Connecting to Web Services)

When PIP back-end processing is done by Web services deployed behind the firewall, it is RECOMMENDED to deploy the MSH as a Gateway (e.g. in the DMZ). This gateway will convert back and forth ebMS messages into Web service invocations (or responses). Because of the Web-service compliant nature of ebMS V3 messages it is often sufficient to remove the eb:Messaging header before forwarding the message to the appropriate document-style Web service.

PIPのバックエンド・プロセスが、ファイアウォールの背後に配置されているWebサービスによって行われる場合、ゲートウェイとして(例えばDMZ内に)MSHを配置することが推奨される。このゲートウェイは、Webサービス呼び出し(または応答)にebMSメッセージを往復変換する。eb:ebMSV3メッセージのWebサービス対応性により、メッセージを適切な文書スタイルのWebサービスに転送する前に、eb:Messagingヘッダを除去するの十分であることが多い。

8.1.1 要求されるV3適合プロファイル (Required V3 Conformance Profiles)

The following ebMS V3 Conformance Profiles are RECOMMENDED (see [ebMS3-CP]):

以下のebMS V3適合プロファイルが推奨される。

- (1) Case of a pure-client message endpoint: light-handler (LH-RM) Conformance Profile
ピュア・クライアントメッセージエンドポイントの場合: **ライト・ハンドラー(LH-RM)適合プロファイル**。
<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/lighthandler-rm>
- (2) Case of a server-enabled message endpoint: Gateway RX V3 Conformance Profile.
サーバー対応メッセージエンドポイントの場合: **ゲートウェイRX V3適合プロファイル**。
<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/gateway-rxv3>

9 付録 A: CPA プロファイリングと例題 (Appendix A: CPA Profiling and Sample)

9.1 CPA プロファイリング形式 (CPA Profiling Forms)

The profiling and definition of CPA data (both instance and profile template) can be facilitated using a set of forms, such as those provided by the ebXML Implementation, Interoperability and Conformance (IIC) OASIS Committee. It is recommended for business partners to use the "Deployment Profile Template for CPPA V2.0" published by the OASIS IIC, in order to finalize their collaboration agreements. A subset of these forms is presented here.

CPAデータ(インスタンスとプロファイル・テンプレートの両方)のプロファイリング及び定義は、ebXML実装、相互運用性、および準拠性(IIC)OASIS技術委員会によって提供されるフォームなどの一組のフォームにより促進することができる。ビジネス・パートナーが、提携契約を結ぶために、OASIS IICによって発行された「CPPA V2.0のデプロイメント・プロファイル・テンプレート」を使用することを強く推奨する。これらのフォームのサブセットをここで提示する。

Each element (or entry) in each one of these forms maps to a CPA element. Either the name of the entry is explicit enough to refer to the corresponding CPA element, or the name of the corresponding CPA element is mentioned in clear, usually prefixed with the qualifier "tp:" (e.g. tp:channelID).

これらのそれぞれのフォームにおける各要素(又は、エントリー)がCPA要素にマッピングする。エントリー名が対応するCPA要素を参照するのに十分明示的であっても、または対応するCPA要素名が明確に言及されていても、通常は修飾子「tp:」(例えばtp:channelID)が接頭辞として付けられる。

- When entries in these forms must map to some PIP definition elements, it is indicated in the form entry.
これらのフォームにおけるエントリーが一部の PIP 定義要素にマッピングしなければならない場合、フォーム・エントリーで示される。
- When entries in these forms are left to the user to instantiate as s/he wants to, the entry value is left empty (or just referring to the actual name of the CPA element, e.g. tp:TransportID)
これらのフォームにおけるエントリーがユーザーに任せられ、ユーザーが望むように例示する場合は、エントリー値は空のまま(または CPA 要素の実際の名前、例えば tp:TransportID を参照するのみ)となる。

A sample CPA document is listed in the next sub-section.

サンプルCPA文書は次の補助項にリストされている。

NOTE: These forms and their content are based on CPPA V2.1, which is very close to V2.0 (includes an errata from V2.0 and has additional extensibility points - some element names may be different. Please refer to the Errata for V2.0.) Once CPPA V3 is complete, it is expected that it will become the primary target for this profiling. Profiling CPPA V3 can largely reuse the profiling done for CPPA 2.1.

注記:これらのフォームとそのコンテンツは、V2.0に非常に類似しているCPPA V2.1(V2.0からのバグを含み、追加拡張ポイントを有する。要素名の中には異なるものもある。V2.0の正誤表を参照されたい。)に基づいている。CPPA V3 が完成した場合、このプロファイリングの主な目標となる。CPPA V3のプロファイリングの多くの部分は、CPPA 2.1からの再利用ができると考えられる。

9.2 CPA 関連書類名と参照のプロファイリング (Profiling the CPA Artifact Names and References)

This form is used to identify the CPA profile, and also any CPA instance that is derived from a profile. It recommends some naming conventions for the CPA artifacts.

このフォームは、CPAプロファイルならびにプロファイルに由来する全てのCPAインスタンスを識別するために使用される。それは、CPA関連書類アーティファクトのいくつかの命名規則を推奨する。

CPA Profile Info

CPA Profile Info **Name** [Provide a name for the Collaboration Protocol Agreement profile. The name should identify when applicable: (a) the version of CPA, (b) the community sharing this profile (here, RN), (c) type of artifact (here a profile), (d) name of profile, (e) party ID if this profile is attached to a party.]

[コラボレーション・プロトコル合意書 (CPA) プロファイルの名前付けをおこなう。適用する場合、この名前により以下を識別するものとする。:(a)CPA のバージョン、(b)このプロファイルを共有するコミュニティ (ここでは RN)、(c)書類のタイプ (ここではプロファイル)、(d)プロファイル名、(e)もしこのプロファイルが当事者に添付される場合には、パーティーID。]

Recommended:

“CPA2.1-RN-Profile-“<profileID>”-“<partner1>”

Examples:

CPA2.1-RN-Profile-PIP3A4-222222

CPA2.1-RN-Profile-TP31-222222

File name [Provide a file name for the Collaboration Protocol Agreement profile file.]

[コラボレーション・プロトコル合意書プロファイル書類に書類名を付ける。]

“CPA2.1-RN-Profile-“<profileID>”-“<partner1>”-file”

(followed by appropriate suffix – e.g. .xml for the XML definition.)

Examples:

CPA2.1-RN-Profile-PIP3A4-222222-file.pdf

CPA2.1-RN-Profile-TP31-222222-file.xml

CPA Instance Info **Name**

[Define the name format for the CPA instances resulting from using this profile. The name should identify when applicable: (a) the version of CPA, (b) the community sharing this profile, (c) name of profile, (d) ID of instance, (e) party IDs.]

[このプロファイルの使用に起因する CPA インスタンスの名前フォーマットを定義する。適用する場合、この名前により以下を識別するものとする。(a)CPA のバージョン (b)このプロファイルを共有するコミュニティ (c)プロファイル名 (d)インスタンスの ID (e) パーティーID。]

Recommended:

“CPA2.1-RN-“<profileID>”-“<instID>”-“<partner1-partner2>”

Example:

CPA2.1-RN -P15-001-222222-333333

CPA2.1-RN -TP2-004-222222-333333

File name [Define the file name format for a Collaboration Protocol Agreement instance.]

[コラボレーション・プロトコル合意書インスタンスの書類名フォーマットを定義する。]

Recommended:

“CPA2.1-RN-“< profileID >”-“<instID>”-“<partner1-partner2>”-file”

(followed by appropriate suffix – e.g. .xml for the XML definition.)

Example:

CPA2.1-RN-P15-001-222222-333333-file.pdf

CPA2.1-RN-TP2-004-222222-333333-file.xml

CPA Id [Define the format of the CPA Id. Must align with CPAId in message header.]
[CPA Id のフォーマットを定義する。メッセージ・ヘッダの CPAID と連携すること]

Recommended: same as CPA name, i.e.:

“CPA2.1-RN-“< profileID >”-“<instID>”-“<partner1-partner2>”

Lifetime of CPA	Start: [The starting date and time of the agreement.] End: [The end date and time of the agreement. The start and end date/times define the duration that the agreement is in effect.]
Context of application	ConversationLimit: [NONE or numeric value. The agreement is terminated (no longer valid) when the conversation limit is reached.] 会話限界: [NONE または数値。会話限界に到達すると、この合意は終了する (有効ではなくなる)。] Concurrent Conversation Limit: [NONE or numeric value. The maximum number of conversations that can be in process at the same time. Provide this value when there are constraints that limit the number of business transactions that one or more of the parties can process simultaneously.] 同時会話限界: [NONE または数値。同時に処理できる会話の最大数。1名または複数名のパーティーが同時に処理できるビジネス取引数を制限する制約がある場合は、この値を提供する。]

9.3 当事者情報のプロファイリング (Profiling the Party Info)

This form is used to identify the parties involve. A CPA profile will typically contain one of these fully instantiated. At least another one of these will need to be filled by another business partner in order to produce a complete CPA instance.

このフォームは、関連当事者の識別に使用される。CPAプロファイルは通常、十分に例示された当事者情報の1つを持つ。完全なCPAインスタンスを生成するために、少なくとも当事者情報のもう1つが相手方ビジネス・パートナーによって作成される必要がある。

Profiling (alignment with data or QoS in RosettaNet PIPs, or with ebMS header data that is itself profiled) is required for some entries of this table. The rest of this table is provided as a support for users.

プロファイリング (Rosettanet PIPにおけるデータまたはQoSとの合わせ、あるいはそれ自身がプロファイルされた ebMSヘッダ・データとの合わせ) はこのテーブルの一部のエントリーに要求される。このテーブルの残りはユーザーのサポートとして提供される。

Party Info

CPA Reference	[CPA Profile name] [CPA Instance name, if used for instantiating a particular CPA] [もし特定の CPA を例示するために使用されるならば、CPA インスタンス名。]
Party element	PartyId [The formal unique identifier for the organization. Must align with eb:PartyId in message header (section 4)] All Party ID elements present in CPA must appear in the message header. [組織のための正式な一意の識別子。メッセージ・ヘッダの eb:PartyId と合わせなければならない。(4項)] CPA に存在する全ての当事者 ID 要素はメッセージ・ヘッダに表示されなければならない。
	Type [Must align with eb:PartyId/@type in message header (section 4)] [メッセージ・ヘッダの eb:PartyId/@type と合わせなければならない (4項)。]
	Reference [A URL or URI that points to a location (e.g. web page or directory) where more information can be found on the party.] 当事者のより多くの情報が見つかる場所 (ウェブ・ページまたはディレクトリなど) を指す URL あるいは URI。]

Collaboration Roles elements	[List the collaboration role names that this party is expected to fulfill. The role names need to be unique within this list. Each role will be detailed in a CollaborationRole form.]	
	[この当事者が実行することが求められるコラボレーション役割名をリストする。役割名はこのリスト内で一意である必要がある。各役割は CollaborationRole フォームで詳述される。]	
	CollaborationRole 1	Process Name [maps to eb:Service I header] Role Name [maps to eb:Role in header]
	CollaborationRole 2	Process Name [maps to eb:Service I header] Role Name [maps to eb:Role in header]
	(others?)	(there may be additional roles)
Certificates elements	[List the certificates info and ID.]	
	Certificate 1	
	Certificate 2	
	(others?)	(there may be additional certificates)
Delivery Channels Elements	[Describes a <i>Party's Message</i> -receiving and <i>Message</i> -sending characteristics. It consists of one document-exchange definition and one transport definition. The details of each DeliveryChannel element will be specified in a different form.]	
	[当事者のメッセージ(受信ならびにメッセージ送信特性)を記述する。それは、1つの文書交換定義ならびに1つのトランスポート定義から成る。各 DeliveryChannel 要素の詳細は、別のフォームで指定する。]	
	DeliveryChannel 1	[give only the tp:channelId]
	DeliveryChannel 2	[give only the tp:channelId]
	(others?)	
Transports Elements	Transport ID	[tp:TransportId]
Documents Exchanges	Exchange ID	[tp:docExchangeId]

9.4 コラボレーションの際の役割のプロファイリング (Profiling the Collaboration Roles)

This form is used to identify the roles in which a party may be acting under this CPA or CPA profile. One form will be filled for each role.

このフォームは、当事者がこのCPAまたはCPAプロファイル下で作用する可能性がある役割を識別するために使用される。各役割につき1枚のフォームに記入する。

Profiling (alignment with data or QoS in Rosettanet PIPs) is required for some entries of this table. The rest of this table is provided as a support for users.

プロファイリング(Rosettanet PIPのデータまたはQoSとの合わせ)はこの表の一部の記載に要求される。この表の残りはユーザーのサポートとして提供される。

ColaborationRole Info

CPA Reference	[CPA Profile name]		
	[CPA Instance name, if used for instantiating a particular CPA]		
Role Identification	Name	[maps to eb:Role] Ref-1 in Tables 7,10 (see section 9.8)	
	Type	[xlink:type], e.g. "simple"	
	Href	[xlink:href] Example: xlink:href="http://www.rosettanet.org/processes/3A4.xml#Buyer">	
Application Certificate	ID:		
	Comments:		
Process Specification	name	[The name of the business process specification that this role applies to] maps to ProcessSpecification nameID attribute in ebBP guideline (e.g. urn:rosettanet:specification:interchange:PIP3A4:xml:ebbp:v11_00), i.e. to eb:Service (see Section 4 Message Description) xlink:href : contains a reference to the ebBP definition (e.g. = http://www.rosettanet.org/processes/3A4.xml)	
	Version	[Version of the business process specification]	
	Type		
	Uuid/nameId	tradingpartner uuid → attribute uuid of ebBP definition when present (attr in process specification top element) (Example= "urn:icann:rosettanet.org:bpid:3A4\$2.0")	
Service Binding item (One for every Action or Signal message)	Associated Service name	[tp:ServiceBinding/tp:Service] Maps to eb:Service (see Section 4, Message Description) Example: < tp:Service>urn:rosettanet:specification:interchange:PIP3A4:xml:ebbp:d11_00</tp:Service>	
	Action direction	[send/ receive]	
	Action Binding	[tp:id] example: companyA_ABID1 (to be used for further references. Unique) [tp:action] example: "Purchase Order Request Action" maps to eb:Action (see Section 4, Message Description)(e.g. = "PurchaseOrderRequestAction") [tp:packageId] Example: tp:packageId="CompanyA_RequestPackage" . Refers to MIME structure of payload.	
	Business Transaction Characteristics	tp:isNonRepudiation Required	maps to "Non-Repudiation of Origin and Content", column 8 in PIP definition tables below. (= "true" in below example) Ref-8 in Tables 7,10 (see section 9.8)
		tp:isNonRepudiation	maps to "Non-Repudiation Required" column 3 in PIP tables below. (= "true"

ReceiptRequired	in below example) Ref-3 in Tables 7,10 (see section 9.8)
tp:isConfidential	(using SSL or digital envelope) Ref-9 in Tables 7,10 (see section 9.8)
tp:isAuthenticated	NOTE: should map to DTD related docs
tp:isTamperProof	(NOTE: authenticated gives integrity)
tp:isAuthorizationRequired	maps to "Is Authorization Required" column 7 in PIP tables below. (= "true" in below example) Ref-7 in Tables 7,10 (see section 9.8)
tp:timeToAcknowledgeReceipt	maps to "Time to Acknowledge" column 4 in PIP tables below. (= "PT2H" in below example) NOTE: it should be equivalent to (retryInterval * Retries) in ebMS. Ref-4 in Tables 7,10 (see section 9.8)
tp:timeToPerform	maps to "Time to Perform" column 5 in PIP tables below (not really captured in CPA, about same as time to Ack) Ref-5 in Tables 7,10 (see section 9.8)
tp:isIntelligibleCheckRequired	(no map to PIP attributes)
tp:timeToAcknowledgeAcceptance	(no map to PIP attributes)
Tp: <i>retryCount</i>	Must NOT be used. Instead, the Retries element of the Reliable Messaging CPA element will map to "Retry Count" column in PIP tables below: Ref-6 in Tables 7,10 (see section 9.8)

9.5 配信チャンネルのプロファイリング (Profiling the Delivery Channels)

Delivery Channels - A delivery channel describes a *Party's Message*-receiving and *Message*-sending characteristics. It consists of one document-exchange definition and one transport definition.

配信チャンネル - 配信チャンネルは、メッセージ受信ならびにメッセージ送信特性を記述する。それは、1つの文書交換定義ならびに1つのトランスポート定義から成る。

No profiling is required for this data. This table is provided as a support for users.
このデータに関するプロファイリングは必要としない。この表は、ユーザーをサポートするためのものである。

Delivery Channel Info

CPA Reference [CPA Profile name]

[CPA Instance name, if used for instantiating a particular CPA]

Identity and channelId

Components	transportId	
	docExchangeId	
Messaging Characteristics	ackRequested	Reliable Messaging parameter for Guaranteed Delivery (At Least Once)
	ackSignatureRequested	NOTE: this is a way to support a form of non-repudiation of Receipt, that is generally not sufficient for RosettaNet.
	duplicateElimination	Reliable Messaging parameter for No Duplicate Delivery (At Most Once)
	Actor	

9.6 文書交換のためのプロファイリング (Profiling the Document Exchanges)

Document Exchange - The Document-exchange layer specifies processing of the business documents by the Message-exchange function. Properties specified include encryption, digital signature, and reliable-messaging characteristics. The options selected for the Document-exchange layer are complementary to those selected for the transport layer. For example, if Message security is desired and the selected transport protocol does not provide *Message* encryption, then *Message* encryption must be specified in the Document-exchange layer.

文書交換 - 文書交換層は、メッセージ交換機能によってビジネス文書の処理を指定する。指定された特性には、暗号化、デジタル署名、及び信頼性メッセージング特性が含まれる。文書交換層に選ばれたオプションは、トランスポート層に選ばれたものと補完的である。例えば、メッセージセキュリティが望まれ、選択されたトランスポート・プロトコルがメッセージ暗号化を提供しない場合、メッセージの暗号化は文書交換層で指定されなければならない。

Profiling (alignment with data or QoS in Rosettanet PIPs) is required for some entries of this table. The rest of this table is provided as a support for users.

プロファイリング(Rosettanet PIPのデータまたはQoSとの合わせ)はこの表の一部の記載に要求される。この表の残りはユーザーのサポートとして提供される。

Document Exchange Info

CPA Reference	[CPA Template name]
	[CPA Instance name, if used for instantiating a particular CPA]
Doc Exchange ID	[tp:docExchangeId]
Sender Binding	Reliable Messaging [tp:ReliableMessaging] tp:Retries: [maps to "Retry Count" column 6 in above tables.] tp:RetryInterval: [Example: <tp:RetryInterval>PT2H</tp:RetryInterval>] tp:MessageOrderSemantics: [Example: "Guaranteed"]
	Persist Duration [tp:PersistDuration]
	Non Repudiation of Origin - [tp:SenderNonRepudiation] tp:NonRepudiationProtocol tp:HashFunction tp:SignatureAlgorithm tp:SigningCertificateRef

Digital Envelope	[tp:SenderDigitalEnvelope]
	- tp:DigitalEnvelopeProtocol
	- tp:EncryptionAlgorithm
	- tp:EncryptionSecurityDetailsRef
Nemespaces	[tp:NamespaceSupported]
Receiver Binding	
Reliable Messaging	[tp:ReliableMessaging]
	- tp:Retries
	- tp:RetryInterval
	- tp:MessageOrderSemantics
Persist Duration	[tp:PersistDuration]
Non Repudiation of Receipt	[tp:ReceiverNonRepudiation]
	- tp:NonRepudiationProtocol
	- tp:HashFunction
	- tp:SignatureAlgorithm
	- tp:SigningSecurityDetailsRef
Digital Envelope	[tp:ReceiverDigitalEnvelope]
	- tp:DigitalEnvelopeProtocol
	- tp:EncryptionAlgorithm
	- tp:EncryptionCertificateRef
Nemespaces	[tp:NamespaceSupported]

9.7 トランスポート層のプロファイリング (Profiling the Transport Protocol)

The transport layer identifies the transport protocol to be used in sending messages through the network and defines the endpoint addresses, along with various other properties of the transport protocol. Choices of properties in the transport layer are complementary to those in the document-exchange layer (see "Document-Exchange Layer" directly above.)

トランスポート層は、ネットワークを介したメッセージの送信で使用されるトランスポート・プロトコルを識別し、他の様々なトランスポート・プロトコルの特性と共に、終端アドレスを定義する。トランスポート層における特性の選択は文書交換層における特性の選択と補完的である(すぐ上の「文書交換層」を参照)。

No profiling is required for this data. This table is provided as a support for users.

プロファイリングはこのデータには要求されない。この表はユーザーのサポートとして提供される。

Transport Info

CPA Reference	[CPA Template name]
	[CPA Instance name, if used for instantiating a particular CPA]
Transport Sender	Protocol [tp:TransportProtocol]
	Client security [tp:TransportSecurityProtocol]
	[tp:ClientCertificateRef]
Transport Receiver	Protocol [tp:TransportProtocol]

End Point [tp:Endpoint/@uri, tp:Endpoint/@type]
 Server security [tp:TransportSecurityProtocol]
 [tp:ServerCertificateRef]
 [tp:ClientSecurityDetailsRef]

9.8 PIP 定義における表の利用実例 (Examples of Tables Used in PIP Definitions)

These tables are extracted from the PIP7C7 definition. Their purpose here is to illustrate the terms and properties that map to the concepts in above CPA forms. The last row in these tables has been added to identify columns that are referred to (Ref-n) in the above CPA forms.

これらのテーブルはPIP7C7定義から抜粋したものである。ここでこれらの目的は、上記のCPAフォームのコンセプトにマッピングする用語および特性を例証することである。これらの表の最後列は、上記のCPAフォームで言及しているカラムを識別するために追加された。

表 7: ビジネスアクティビティの実行管理							
役割名	アクティビティ名	受領の確認			再試行回数	許可が必要か	発信元および内容の否認防止
		否認防止が必要か	確認までの時間	実行までの時間			
ファウンダリーテストサービス	半導体テストデータの通知	Y	2 時間	N/A	3	Y	Y
Ref-1	Ref-2	Ref-3	Ref-4	Ref-5	Ref-6	Ref-7	Ref-8

表 10: メッセージ交換管理							
番号	名前	確認までの時間	アクションに答えるまでの時間	実行時間を含む	許可が必要か?	否認防止が必要か?	安全な転送が必要か?
1.	半導体テストデータ通知の実行	2時間	N/A	N/A	Y	Y	Y
1.1.	受領確認	N/A	N/A	N/A	N	N	Y
		Ref-4	Ref-10		Ref-7	Ref-3, Ref-8	Ref-9

10 付録(Appendix) B: 用語集(Glossary)

AMD	Abstract Message Service
ATPA	Abstract Trading Partner Agreement
MEP	Message Exchange Pattern
RNIF	RosettaNet™ Implementation Framework
PIP	(RosettaNet terminology): Partner Interface Process
TP	Trading Profile
ebMS	ebXML Messaging Services specification (an ebXML standard)
BPSS	ebXML Business Process Specification Schema (an ebXML standard)
ebBP	ebXML Business Process specification (applies to new version of BPSS, renamed)
CPP	ebXML Collaboration Protocole Profile (described in CPPA specification, an ebXML standard)
CPA	ebXML Collaboration Protocole Agreement (described in CPPA specification, an ebXML standard)
SBDH	Standard Business Document Header (also known as “Generic Header”)
TPP	Trading Partner Profile

11 参照 (References)

Source	Description
[AMD]	Title: MMS Abstract Message Definition, Draft 00.07.00, January 7, 2005 RosettaNet Retrieved from : http://members.rosettanet.org/dnn_rose/DMX/tabid/2979/DMXModule/624/Command/Core_ViewDetails/Default.aspx?EntryId=346
[ebBP-SIG]	Title: ebXML Business Signals Schema, 2006. OASIS Retrieved from: http://docs.oasis-open.org/ebxml-bp/ebbp-signals-2.0
[ebMS2]	Title: ebXML Message Service Specification Version 2.0, April 1, 2002. OASIS Retrieved from: http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf
[ebMS3]	Title: ebXML Message Service Specification Version 3.0 Part 1, Core Features, September 30, 2007 OASIS Retrieved from: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf
[ebMS3-CP]	Title: ebXML Messaging Services 3.0 Conformance Profiles, July 25, 2007 OASIS Retrieved from: http://www.oasis-open.org/committees/download.php/29854/ebms-3%5B1%5D.0-confprof-cd-03.pdf
[ebCPPA2]	Title: Collaboration-Protocol Profile and Agreement Specification Version 2.0, May 20, 2002. OASIS Retrieved from: http://www.oasis-open.org/committees/download.php/202/ebCPP-2_0.pdf
[DPT-ebMS2]	Title: Deployment Profile Template 1.1 for ebMS 2.0, OASIS IIC Committee draft, July 2005. OASIS

	Retrieved from: http://www.oasis-open.org/committees/document.php?document_id=21667&wg_abbrev=ebxml-iic
[DPT-CPPA2]	Title: Deployment Profile Template 0.2 for CPPA 2.0, OASIS IIC working draft, August 2005. OASIS Retrieved from: http://www.oasis-open.org/committees/document.php?document_id=21667&wg_abbrev=ebxml-iic
[BPSS-PIP]	Title: ebXML BPSS Guideline, v1.11, August 2004. RosettaNet Retrieved from : http://members.rosettanet.org/dnn_rose/DMX/tabid/2979/DMXModule/624/Command/Core_ViewDetails/Default.aspx?EntryId=5726
[RFC2119]	Author: Scott Bradner Title: Key words for use in RFCs to Indicate Requirement Levels, March 1997. The Internet Engineering Task Force Retrieved from: http://www.ietf.org/rfc/rfc2119.txt
[RFC2045]	Author: N. Freed Title: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, 1996. The Internet Engineering Task Force Retrieved from: http://www.ietf.org/rfc/rfc2045.txt
[RN-NameSpaces]	Title: RosettaNet Namespace Specification and Management, v1.0, December, 2003. RosettaNet Retrieved from : http://members.rosettanet.org/dnn_rose/DMX/tabid/2979/DMXModule/624/Command/Core_ViewDetails/Default.aspx?EntryId=5726
[SOAPATTACH]	Author: John J. Barton, et al. Title: SOAP Messages with Attachments, 2000 W3C Retrieved from: http://www.w3.org/TR/SOAP-attachments
[WS-I]	Author: C.Ferris, et al. Title: WS-I Basic Profile (1.2 and 2.0) WS-Interoperability Retrieved from:

	http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile
[WSS11]	Author: Anthony Nadalin, et al. Title: Web Services Security: SOAP Message Security 1.1, June 2005. OASIS Retrived from: http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-pr-SOAPMessageSecurity-01.pdf
[WSS11-X509]	Editor: Anthony Nadalin Title: Web Services Security X.509 Certificate Token Profile 1.1, 2006. OASIS Retrieved from: http://docs.oasis-open.org/wss/v1.1/wss-v1.1-errata-os-x509TokenProfile.pdf (obtained from: http://docs.oasis-open.org/wss/v1.1/)