

Message Control and Choreography (MCC) Profile-ebMS-V3

リリース版 R 11.00.00A

仕様書情報	
名前	MCC – Profile-ebMS V3
公開日	2010年6月1日
Version情報	R 11.00.00A

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。
又、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	ドキュメント管理 (Document Management)	3
1.1	免責事項 (Legal Disclaimer).....	3
1.2	著作権 (Copyright).....	3
1.3	商標 (Trademarks).....	3
1.4	謝辞 (Acknowledgments).....	3
1.5	関連ドキュメント (Related Documents).....	4
1.6	ドキュメントのバージョン履歴 (Document Version History).....	4
1.7	文書の目的 (Document Purpose).....	4
2	ebMS V3の単一ビジネス文書PIPプロフィール (Single Business Document PIP Profiling for ebMS V3)	5
2.1	PIP定義機能 (PIP Definition Features).....	6
2.2	PIP実行結果 (PIP execution outcome).....	9
2.3	QoSの機能 (Quality of Service Features).....	10
3	PIPパラメータ化と実行管理 (PIP Parameterization and Execution Control)	13
3.1	PIP プロパティ パラメータ (PIP Property Parameters).....	14
3.2	PIP実行形式と関連パラメータ (PIP execution modes and related parameters).....	16
3.3	PIPインスタンス相関及び識別 (PIP Instance Correlation and Identification).....	16
4	PIP定義の事例 (Use Cases of PIP definition)	18
4.1	事例 1 - 全機能 (Use Case 1 – Full features).....	18
4.2	事例 2 ビジネス文書のみ (Use Case 2 – Business Document Only).....	19
4.3	メッセージ交換例 (Sample Message Exchange).....	20

1 ドキュメント管理 (Document Management)

1.1 免責事項 (Legal Disclaimer)

RosettaNet™ およびそのメンバー、職員、管理者、従業員、代理店は、本書や本書で提示する仕様およ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。

1.2 著作権 (Copyright)

©2010 RosettaNet. All rights reserved. 本書の一部あるいは全部について、この著作権告示を含むことなく、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、あるいは転送を行うことを禁じる。いかなる派生物にも著作権告示を特記しなければならない。本出版物の一般への再配布または販売、あるいは派生作業を行う前には、出版元からの文書による許諾が必要である。

1.3 商標 (Trademarks)

RosettaNet、Partner Interface Process、PIP およびRosettaNet ロゴは、非営利組織「RosettaNet」の商標または登録商標である。その他の製品名および企業のロゴは、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。

1.4 謝辞 (Acknowledgments)

本書は、RosettaNet (<http://www.rosettanet.org/>) により準備されたものであり、マイルストーン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 の設計および開発に携わった法人は次の通りである。

Axway	Cisco
DHL	IBM
KJC Solutions	Oracle
OASIS	Software AG
Tibco	University Bamberg
Vienna University of Technology	

1.5 関連ドキュメント (Related Documents)

- MCC Single Business Document PIP Template R11.00.00A
- MMS ebMS V3 Profile R12.00.00A

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

バージョン	日付	解説
リリース版 R 11.00.00A	2010年6月1日	リリース版

1.7 文書の目的 (Document Purpose)

文書の目的は、一般の読者(非技術者)に、構造、オブジェクト間の関係、オブジェクトの内容、要素の定義等を説明することである。

2 ebMS V3のための1方向ビジネス文書用PIPプロファイル (Single Business Document PIP Profiling for ebMS V3)

The “Single business document PIP Template” [MCC-PIP-Template] defines a model for single business document PIPs. It is abstract in two different ways:

“1方向ビジネス文書用PIPモデル” [MCC-PIP-Template]は、1方向ビジネス文書用PIPのためのモデルを定義する。これは、2つの異なる方法において抽象的である。

1. The realization of a PIP definition component may vary with the communication technology selected for implementing the PIP.
PIP 明確化は、PIP の実装に対して選定される通信技術によって、異なる可能性がある。
2. The realization of a PIP definition may vary depending on the execution context assumed.
PIP 明確化は、想定される実行コンテキストによって、異なる可能性がある。

This template can be used to define PIPs (PIP definitions) in a way that does not depend on specific messaging solutions and protocols.

このテンプレートは、特定の通信方法及びプロトコルに依存しないで、PIPを決定(PIP明確化)するために使用できる。

In a next step, such PIP definitions need to be implemented as “concrete PIPs” or customized PIPs, which defines all execution details including the messaging solution to be used. This profiling document is concerned with defining how the different features and execution aspects of a PIP definition will map to the ebMS V3 messaging solution.

次のステップにおいて、当該PIPは要素まで決められた“実際のPIP”あるいはカスタマイズされたPIPとして実装される必要があり、使用される通信方法を含む全ての実装の詳細を定義する。このプロファイル文書は、PIPを決める際に異なる特徴及び実行の側面がどのようにebMS V3 通信方法にマップするかを定義することに対応する。

To summarize, this profile is relevant to the two lowest levels at which PIP material is defined:

要約すると、このプロファイルは、PIPデータを定義する2つの最も低いレベルに該当する：

- (1) Customized PIP: (or concrete PIP): At this level, all elements of a PIP are fully defined, and all parameters (such as QoS, timing) are given a specific value or specific range that is agreed between partners. The execution of such PIPs is determined in terms of QoS, alignment features and execution mode. The factors that condition a successful or a failed outcome are fully determined and known from partners.

カスタマイズされたPIP: (又は実際のPIP): このレベルでは、PIPの全ての要素が完全に定義され、全てのパラメータ(QoS、タイミング等)はパートナー間で合意される特定の値または特定の範囲値として与えられる。当該PIPの実行は、QoS、合意機能及び実行モードの観点から決定される。成功、又は失敗の結果を条件付ける要因は、全てパートナー間で決定されて知らされる。

(2) PIP instance: This is an image of a particular execution of a PIP, i.e. a particular sequence of concrete messages where all components and PIP properties are given a value – e.g. a fully defined business document between two identified partners, a particular timing between these messages, etc.

PIPインスタンス: これは、PIPの特別な実行のイメージ、即ち、全てのコンポーネント及びPIP属性が値を与えられる具体的なメッセージの特定のシーケンスである。例えば、2つの特定されたパートナー間の完全に定義されたビジネス文書、これらのメッセージ間の特定のタイミングなど。

2.1 PIP明確化の特徴 (PIP Definition Features)

2.1.1関係者 (Parties involved)

Party IDs and roles are represented in the message header. See Profiling requirements described in the MMS ebMS V3 Profile, section 4.2. “ebMS Header Profiling”.

当事者ID及び役割は、メッセージ・ヘッダに表示される。MMS ebMS V3 プロファイル 第4.2章の“ebMS Header Profiling”に記載のプロファイル要件を参照のこと。

In particular, the following items describing parties are represented, and mapped to related RNIF document header elements:

特に、当事者を記述している次のアイテムが示され、関連RNIF文書ヘッダ要素にマップされる。

- Party IDs (section 4.2.1) 当事者ID
- Party roles (section 4.2.2) 当事者役割
- Service invoked (section 4.2.3) 行うサービス
- Action invoked (section 4.2.4) 行う行動
- Conversation Id (section 4.2.5) 会話ID

2.1.2 ビジネス文書 (Business Document)

The Rosettanet payload may either be packaged in the SOAP Body or as an attachment. In both cases the referencing from the ebMS header must follow the MMS profile requirements:

Rosettanet本文は、SOAP本体の中にパッケージ化されるか、添付としてされるであろう。どちらのケースでも、ebMSヘッダーからの参照は、MMSプロファイル要件を遵守しなければならない。

Specification Header element:
Feature eb:UserMessage/eb:PayloadInfo/eb:PartInfo
eb:UserMessage/eb:PayloadInfo/eb:PartInfo/eb:Schema

Specification ebMS 3, section 5.2.2.12, 5.2.2.13
Reference

Profiling 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].
eb:PartInfo要素: eb:PartInfo要素が、PIP本体のサービス内容の一部(主要なXML文書)を参照しているか、XML RosettaNet信号を参照している場合、eb:Schema要素を含まなければならない。スキーマのURN IDは、[RN-NameSpaces]に従わなければならない。

Example for a PIP service content with XML schema:

XMLスキーマによるPIPサービス・コンテンツの例:

urn:rosettanet:specification:interchange:PIP3A4PurchaseOrderRequest:xsd:schema:1.0

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].

既存のRNIFヘッダー(サービスヘッダー)がメッセージに含まれる場合、単一の添付資料として追加する必要がある。eb:Reference要素はそれを識別するため、eb:Schema要素を含む必要があり、[RN-NameSpaces]に従う。

Example for a Service header: サービスヘッダーの事例:

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

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

注記: XLINKプロセッサの使用は、要求されない。

Alignment

Test
References

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.

SBDH (Standard Business Document Header)がそのまま保存される必要がある場合、例えば、既存のバックエンド統合の再使用のためなど、全てのSBDH ヘッダーは、別個の本文部(SOAP本体のManifest要素で参照される)として加えることができる。添付資料ではなくSOAP本体にそれを加えることが推奨される。

2.1.3 ビジネス状態に関する合意の特徴 (Business State Alignment features)

(1) 配信に関する合意 (Delivery Alignment)

The Reliable Messaging (RM) feature of ebMS V3 (WS-ReliableMessaging used in compliance with WS-I Reliable and Secure Profile) provides state alignment about message reception. There is no explicit signaling confirming that a message has actually been delivered to the application. However, only reception failures are expected to be reported on the Sender side.

ebMS V3の高信頼メッセージング(RM)機能は、メッセージ受信についての状態に関する合意内容を提供する(WS-I Reliable and Secure Profileに基づいたWS-ReliableMessagingで)。メッセージが実際にアプリケーションに配信されたという、明確な信号送達の確認は存在しない。しかし、受信の失敗だけは送信側に報告されることが期待される。

See in the MMS ebMS V3 Profile, section 6.4.1 for the use of RM for state alignment, in case Receipts are not used.

受信確認が使用されない場合、状態に関する RM 使用に関しては、MMS ebMS V3 Profile の第 6.4.1 章を参照のこと。

Unlike the RM acknowledgement, the ebMS Receipt signal provides a positive acknowledgement for delivery alignment, that has visibility at application level on the Sender side.

RM 確認とは違って、ebMS 受信信号は納入状態の肯定確認応答とし、送信者側のアプリケーション・レベルで確認することができる。

Relevant PMode parameters: PMode[1].Reliability and below.

(2) 検証に関する合意 (Validity Alignment)

The ebMS Receipt signal is generally sent back by the MSH before payload validation occurs. In general it cannot be counted on to implement this semantics. However, the ebMS Receipt can be given a Non-Repudiation of Receipt semantics, in which case MMS ebMS V3 profile offers these options:

一般的に ebMS 受領信号は、本文の検証を行う前に MSH により返信される。一般的に、この動作を実装することは、期待できない。しかしながら、ebMS 受信には、受領動作の否認防止を与えることができ、この場合、MMS ebMS V3 プロファイルは次の様なオプションを提示する：

- 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、署名付き eb:Receipt は、ドキュメント確認が行われる前に受領が返信される。eb:Receipt の意味は、メッセージが確かに受領され、その後の処理 (本文の検証を含む) は、受領者側が責任を持つことを意味する。

- 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.

否認防止の検証: この変形では、署名付き eb:Receipt は、ドキュメントの検証が終了してから、受領が返信される。eb:Receipt の意味は、メッセージが確かに受領され、その後の処理に有効であることを意味する。

See the MMS ebMS V3 profile for more details.

- Relevant PMode parameters: **PMode[1].Security.SendReceipt**

and below.

2.2 PIP実行結果 (PIP execution outcome)

As a general rule, a positive outcome (success) will be manifest on the Sender side with the ebMS protocol as (a) reception of expected Receipt(s) or acknowledgements, (b) no critical ebMS error being generated.

一般ルールとして、肯定的結果(成功)は、ebMS プロトコルによる送信者側で、(a) 予定された受信通知の受領があった、又は (b) 重大な ebMS エラーは発生していない、ということを示している。

Some failures such as timeout failures for Receipts and for overall PIP execution, will however not be detected by the ebMS V3 layer and must be established at the layer above.

しかしながら、受信及び全体的な PIP 実行についてのタイムアウト障害の様ないくつかの不具合は、ebMS V3 レイヤーによっては検出されず、上位のレイヤーで確定されなければならない。

2.3 QoS(サービス品質)の特徴 (Quality of Service Features)

2.3.1 安全に関する選択肢 (Security options)

認証 (Authentication:)

- in ebMS V3, supported by WS-Security. Profiling requirements described in the MMS ebMS V3 Profile, section 7.1 “General Security Policies” apply.
ebMS V3 においては、WS-Security でサポートされる。プロファイリングの要件に関しては MMS ebMS V3 Profile 第 7.1 章 “General Security Policies” が適用される。

See PMode parameters:

- PMode[1].Security.X509.Sign
- PMode[1].Security.X509.Signature

機密性 (Confidentiality:)

- in ebMS V3, supported by WS-Security. Profiling requirements described in the MMS ebMS V3 Profile, section 7.1 “General Security Policies” apply.

ebMS V3 においては、WS-Security でサポートされる。プロファイリングの要件に関しては MMS ebMS V3 Profile 第 7.1 章 “General Security Policies” が適用される。

See PMode parameters:

- PMode[1].Security.X509.Encryption

完全性 (Integrity)

- in ebMS V3, supported by WS-Security. Profiling requirements described in the MMS ebMS V3 Profile, section 7.1 “General Security Policies” apply.

ebMS V3 においては、WS-Security でサポートされる。プロファイリングの要件に関しては MMS ebMS V3 Profile 第 7.1 章 “General Security Policies” が適用される。

否認防止/受領の否認防止 (Non Repudiation/Non Repudiation Of Receipt:):

- in ebMS V3: Non Repudiation or Receipt is supported by the ebMS V3 protocol with Receipt messages containing digests, as described in Core ebMS V3. Profiling requirements described in the MMS ebMS V3 Profile, section 6.3 “Receipt Semantics” and section 7.2 “Handling of Receipts” apply.

Two flavors of NRR are supported by the MMS profile: Simple and Validating NRR.

ebMS V3 において、否認防止、又は受領の否認防止は、Core ebMS V3 で解説されるように、認証方式が含まれる受領メッセージを持つ V3 プロトコルによりサポートされる。MMS ebMS V3 プロファイルで説明されるプロファイルの要件に関しては、第 6.3 章の“Receipt Semantics”と第 7.2 章の“Handling of Receipts”が適用される。2 種類の NRR は、MMS プロファイルによってサポートされる：単純なもの及び検証を行う NRR である。

- NRR SHOULD be accomplished by generating Receipts that comply with the AS4 Profile (Section 4.1.8 in the AS4 Profile specification [...]).

NRR は、AS4 プロファイルに従う受領を発生させることで達成させる (AS4 Profile specification [...]の第 4.1.8 章)。

See PMode parameters:

- PMode[1].Security.X509 (for signature of the action message)
- PMode[1].Security.SendReceipt

認可 (Authorization:)

- in ebMS V3, supported by WS-Security. Also allows for fine-grain access control (e.g. to specific Service/Action or specific MPC), based on the “message authorization” feature (section 7.10 in ebMS V3 standard). Profiling requirements described in the MMS ebMS V3 Profile, section 7.1 “General Security Policies” apply. Authorization of pulling is described in 7.1.2.
- ebMS V3 において、WS-セキュリティでサポートされる。又、“message authorization”機能 (ebMS V3 標準第 7.10 章)に基づき、(特定のサービス/アクション又は特定の MPC などに対する)きめの細かいアクセス制御を可能にする。プロファイルの要件に関しては、MMS ebMS V3 プロファイル 第 7.1 章の“General Security Policies”が適用される。引き取り認可は第 7.1.2 章に記載されている。

See PMode parameters:

- PMode[1].Security.PModeAuthorize
- PMode.Responder.Authorization

2.3.2 高信頼性メッセージング (Reliable Messaging)

Guaranteed delivery (At-least-Once delivery): Supported by the reliable messaging feature (WS-ReliableMessaging) in ebMS V3. Profiling requirements described in the MMS ebMS V3 Profile, section 7.1 “General Reliability Policies” apply: duplicate elimination is expected to be used when guaranteed delivery is used.

保証された配信(最低でも一度の保証された配信):

ebMS V3の高信頼性メッセージング機能(WS-ReliableMessaging)でサポートされる。MMS ebMS V3プロファイル第7.1章に記載の“General Reliability Policies”が適用される: 配信保証が使用される場合、重複削除が使われることになっている。

- PMode[1].Reliability.AtLeastOnce.Contract (true/false, for “guaranteed delivery”)
- PMode[1].Reliability.AtLeastOnce.Contract.AckOnDelivery (false= Ack on reception by gateway, true= Ack on delivery to the application layer. Usually constrained by the implementation.)
- PMode[1].Reliability.AtLeastOnce.Contract.AcksTo
- PMode[1].Reliability.AtLeastOnce.Contract.AckResponse
- PMode[1].Reliability.AtLeastOnce.ReplyPattern

Duplicate elimination (At-Most-Once delivery):

Supported by the reliable messaging feature (WS-ReliableMessaging) in ebMS V3.

重複排除(最大で一度の重複なしの配信):

ebMS V3の高信頼メッセージング機能(WS-ReliableMessaging)でサポートされる。

- PMode[1].Reliability.AtMostOnce.Contract

2.3.3 時間的制約 (Timing Constraints)

Time to acknowledge validity (or invalidity): There is no capability in the ebMS V3 protocol for detecting timeouts. Such timeouts must be detected at the layer above the messaging layer.

有効(あるいは無効)な受領通知までの時間:

ebMS V3プロトコルにはタイムアウト検出用の機能はない。そのようなタイムアウトについては、メッセージング・レイヤーの上位のレイヤーで検出されなければならない。

Time to Perform: There is no capability in the ebMS V3 protocol for detecting timeouts. Such timeouts must be detected at the layer above the messaging layer.

実行までの時間:

ebMS V3プロトコルにはタイムアウト検出用の機能はない。そのようなタイムアウトについては、メッセージング・レイヤーの上位のレイヤーで検出されなければならない。

3 PIPパラメータ化と実行管理 (PIP Parameterization and Execution Control)

Parameterization of the messaging behavior for PIP definitions as well as PIP instance customization, is represented by PMode abstract parameters. These have been classified in two categories in the PIP Template document:

PIP明確化に対するメッセージング動作のパラメータ化は、PIPインスタンスのカスタマイズと同様に、PMode抽象パラメータによって表現される。これらは、PIPテンプレート文章中で2つのカテゴリに分類された。

1. PIP property parameters
2. PIP execution parameters

3.1 PIP プロパティ パラメータ (PIP Property Parameters)

The following parameters are configurable on a PIP definition and a PIP implementation instance basis:

以下のパラメータは、PIP明確化およびPIP実装インスタンスのベースで構成可能である。

Specification item	Configurable	Implication	Explanation
Send Request Document	No		(part of the PIP definition) A request document always has to be sent. The MSH does not itself create/controls the document and its sending. (Identified with GlobalBusinessActionCode) いつも要求書を送付しなければならない。 MSH自体は、文書を作成も管理もせずその送信もしない。
Overall Time-To-Perform	No	Not ebMS configurable.	Time for performing the messaging Technology-specific PIP protocol. Controlled at a higher level than MSH. メッセージ技術、特定PIPプロトコルを実行するための時間。 MSHより、高レベルとして管理。
Receipt Acknowledgement	Yes	Controlled by ebMS V3 PMode: PMode[1].Security.SendReceipt	Use of ebMS Receipt signal. ebMS 受信信号を使用。
Non-Repudiation of-origin	Yes		Controlled by Digital signature of action message. Requires persistence of the message. アクション・メッセージのデジタル署名によって制御される。 メッセージの永続性を必要とする。
Non-Repudiation of-Receipt	Yes	Controlled by ebMS V3 PMode: See MMS ebMS V3 Profile, section 6.6.2 See PMode[1].Security.SendReceipt	Based on ebMS Receipt signal. ebMS 受信信号に基づく。
TimeTo Acknowledge Receipt	No	Sending a ReceiptAcknowledgement is controlled by PMode[1].Security.SendReceipt Timing is not ebMS configurable.	Time for sending a ValidityAcknowledgement measured from the receipt of the action message. アクション・メッセージの受信から、検証通知 (ValidityAcknowledgement) を送信するまでの時間
Reliability	Yes	ebMS V3 PMode: see PMode[1].Reliability	

Specification item	Configurable	Implication	Explanation
Confidentiality	Yes	ebMS V3 PMode: see PMode[1].Security	
Integrity	Yes	ebMS V3 PMode: see PMode[1].Security	
Authentication	Yes	ebMS V3 PMode: see PMode[1].Security	
Authorization	Yes	ebMS V3 PMode: see PMode[1].Security and PMode.Responder.Authorization	Possibility to control what message header content is allowed for which sender. (which PMode can be used by which user, which MPC channel can be pulled by which user)
IntelligibleCheck Required	No	Sending an Acceptance Acknowledgement reflecting business rule and semantic checks. Sending a ReceiptAcknowledgement reflecting Message and possibly Document syntax checks. ビジネスルール及び意味の確認を反映した許諾通知を送ること。 メッセージ及び可能なら文書構文チェックを反映した受領通知を送ること。	Integration partners have to define the additional validation steps that have to be performed in case this flag is used. このフラグが使用される場合、統合パートナーは実行されるべき追加の検証ステップを定義しなければならない
RetryCount	No	Reliable Messaging feature is not a substitute for this level of retry. Message-layer retries are handled by RM feature. 高信頼メッセージング機能はこのレベルのリトライに対する代替手段ではない。メッセージ・レイヤーのリトライは、RM機能によって扱われる。	Describes how often a business document/signal can be submitted by the PIP process engine to the messaging layer. (would belong to a new PIP instance identifier) This is not a feature at the level of Reliable Messaging. ビジネス文書/信号はメッセージング・レイヤーへ、どれ位の頻度でPIP処理エンジンによって提出されるかを記述する。 (新しいPIPインスタンスIDに属するだろう) これは、高信頼メッセージングのレベルでの機能ではない。

Examples for defining PIPs will be given in the use cases section.

PIP明確化についての例は、4 PIP定義の事例の章で説明される。

3.2 PIP実行形式と関連パラメータ (PIP execution modes and related parameters)

3.2.1 通信プロトコル (Messaging Protocols)

Specifying the protocol in use, see PMode parameter: **PMode[1].Protocol.Address**

Specifying the SOAP version in use, see PMode parameter: **PMode[1].Protocol.SOAPVersion:**

3.2.2 メッセージ交換パターン (Message Exchange Patterns)

同期実行 (Synchronous execution)

For ebMS V3: In MMS ebMS V3 Profile:

See Section 6.4.1: One-action PIP without Non-Repudiation of Receipt

See Section 6.4.2: One-action PIP, with Simple Non-Repudiation of Receipt

See Section 6.4.3: One-action PIP, with Validating Non-Repudiation of Receipt

Also: “Pure client” cases in 6.5.1, 6.5.2 and 6.5.3.

コールバック付き 非同期 実行 (Asynchronous execution with callback)

See Section 6.4.4: One-action PIP, with Callback Receipt for Non-Repudiation

引き取り機能付き 非同期 実行 Asynchronous execution with pulling

See Section 6.5.4: One-action PIP, with Pulled Receipt for Validating Non-Repudiation

3.3 PIPインスタンスの相関関係及び識別 (PIP Instance Correlation and Identification)

3.3.1 PIPの識別 (PIP Identification)

Generation of Globally Unique Ids (GUIDs) for PIP instances

PIPインスタンスに対するグローバルに一意的識別子(GUID)の生成:

See section 4.2.5 MMS ebMS V3 Profile:

The ConversationId header element represents the PIP instance ID value,
It MUST map to Standard Business Doc Header (SBDH) element when applicable:

会話ID(ConversationId)ヘッダーがPIPインスタンスID値を表す。可能であれば、SBDH(Standard Business Doc Header)要素へ、マップすること。

RequestingDocumentInformation / BusinessProcessInstanceIdentifier

It MUST map to (in RNIF Service header) element:

ServiceHeader/ProcessControl/pipInstanceId/InstanceIdentifier

Inclusion of PIP instance GUIDs within RosettaNet message definitions

RosettaNetメッセージで定義するPIPインスタンスGUIDの内包

In ebMS V3: See section 4.2.5 MMS ebMS V3 Profile

ebMS V3 : MMS ebMS V3 プロファイルの第4.2.6章参照:

It is RECOMMENDED that ConversationId header element represents the PIP instance ID value, i.e. has same value for all messages related to the same PIP instance.

会話ID(ConversationId)ヘッダーがPIPインスタンスID値を表す。即ち、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て同じ値であることが、強く推奨される。

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).

言い換えると、同一PIPインスタンスからのメッセージは同一の会話IDを持たなければならない、この会話IDはこのPIPインスタンスに固有である(他のPIPインスタンスと共有されない)ことが勧められる。

3.3.2 メッセージの相関関係 (Message Correlation)

ebMS V3: See section 4.2.6 MMS ebMS V3 Profile:

Every message involved in a PIP instance MUST refer to another previous message of this instance with RefToMessageId header element (except for the initial message of the instance, which MUST NOT have a RefToMessageId element.)

PIPインスタンスに含まれる全てのメッセージは、このインスタンスのもう一つ前のメッセージの RefToMessageId header 要素を参照していなければならない(インスタンスの最初のメッセージは例外であり、RefToMessageId要素を持ってはならない)。

4 PIP明確化の事例 (Use Cases of PIP definition)

This section gives some sample configurations of PIPs according to the configurability matrix above. The MCC messaging technology profiles are expected to describe the implementation of these use cases.

この章では、前述の構成可能マトリックスによるいくつかのPIPの構成サンプルを示す。MCCメッセージング技術のプロファイルは、これらの事例を説明することが期待される。

4.1 事例 1 - 全て包含 (Use Case 1 – Full features)

```
<DataExchange
  name= "bt-PIP3A20"
  nameID= "bt-PIP3A20"
  isGuaranteedDeliveryRequired= "true">
  <RequestingRole name= "Purchase Order Confirmation Sender" nameID= "bt-
PIP3A20-role-sender"/>
  <RespondingRole name= "Purchase Order Confirmation Receiver" nameID= "bt-
PIP3A20-role-receiver"/>
  <RequestingBusinessActivity
    name= "Send Purchase Order Confirmation"
    nameID= "bt-PIP3A20-ba-req"
    isIntelligibleCheckRequired= "true"
    isNonRepudiationRequired= "true"
    isNonRepudiationReceiptRequired= "true"
    retryCount= "3"
    timeToAcknowledgeReceipt= "PT3M"
  >
  <DocumentEnvelope
    name= "doc-PIP3A20-PurchaseOrderConfirmation"
    businessDocumentRef= "doc-PIP3A20-PurchaseOrderConfirmation"
    nameID= "doc-PIP3A20-PurchaseOrderConfirmation-de"
    isAuthenticated= "transient"
    isConfidential= "transient"
    isTamperDetectable= "transient"
  />
  <ReceiptAcknowledgement
    name= "ra"
    nameID= "bt-PIP3A20-ack-ra"
    signalDefinitionRef= "ra2"/>
  <ReceiptAcknowledgementException
    name= "rae"
    nameID= "bt-PIP3A20-ack-rae"
    signalDefinitionRef= "rae2"/>
</RequestingBusinessActivity>
<RespondingBusinessActivity name= "xsd-pacifier" nameID= "bt-PIP3A20-ba-
resp"/>
</DataExchange>
```

4.2 事例 2 ビジネス文書のみ (Use Case 2 – Business Document Only)

```
<DataExchange
  name= "bt-PIP3A20"
  nameID= "bt-PIP3A20"
  isGuaranteedDeliveryRequired= "true">
  <RequestingRole name= "Purchase Order Confirmation Sender" nameID= "bt-
PIP3A20-role-sender"/>
  <RespondingRole name= "Purchase Order Confirmation Receiver" nameID= "bt-
PIP3A20-role-receiver"/>
  <!-- No TTAR, nor isIntelligibleCheckRequired -->
  <RequestingBusinessActivity
    name= "Send Purchase Order Confirmation"
    nameID= "bt-PIP3A20-ba-req"
    isNonRepudiationRequired= "true"
    isNonRepudiationReceiptRequired= "true"
    retryCount= "1"
  >
  <DocumentEnvelope
    name= "doc-PIP3A20-PurchaseOrderConfirmation"
    businessDocumentRef= "doc-PIP3A20-PurchaseOrderConfirmation"
    nameID= "doc-PIP3A20-PurchaseOrderConfirmation-de"
    isAuthenticated= "transient"
    isConfidential= "transient"
    isTamperDetectable= "transient"
  />
  <!-- No ReceiptAcknowledgement/Exception definitions here -->
</RequestingBusinessActivity>
  <RespondingBusinessActivity name= "xsd-pacifier" nameID= "bt-PIP3A20-ba-
resp"/>
</DataExchange>
```

4.3 メッセージ交換例 (Sample Message Exchange)

4.3.1 1方向メッセージ (1-Action Message)

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
<S11:Header>
<eb:Messaging S11:mustUnderstand="1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/core/ebms-header-3_0-200704.xsd"> <eb:UserMessage>
<eb:MessageInfo>
  <eb:Timestamp>2006-07-25T12:19:05</eb:Timestamp>
  <eb:MessageId>12345@requester.example.com</eb:MessageId>
</eb:MessageInfo>
<eb:PartyInfo>
  <eb:From>
    <eb:PartyId tp:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:D-U-N-
SNumber:0060">123456789</eb:PartyId>
    <eb:Role>bt-PIP3A20-role-sender</eb:Role>
  </eb:From>
  <eb:To>
    <eb:PartyId tp:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:D-U-N-
SNumber:0060">112233445</eb:PartyId>
    <eb:Role>bt-PIP3A20-role-receiver</eb:Role>
  </eb:To>
</eb:PartyInfo>
<eb:CollaborationInfo>
  <eb:AgreementRef>http://registry.example.com/cpa/123456
</eb:AgreementRef>
  <eb:Service>urn:rosettanet:specification:interchange:bt-
PIP3A20:xml:ebbp:v11_00</eb:Service>
  <eb:Action>doc-PIP3A20-PurchaseOrderConfirmation-de</eb:Action>
  <eb:ConversationId>4321</eb:ConversationId>
</eb:CollaborationInfo>
<eb:PayloadInfo>
  <eb:PartInfo href="cid:part@example.com">
  <eb:Schema location="http://registry.example.org/po.xsd" version="2.0"/>
  <eb:PartProperties>
    <eb:Property name="Description">Purchase Order Confirmation</eb:Property>
    <eb:Property name="MimeType">application/xml</eb:Property>
  </eb:PartProperties>
  </eb:PartInfo>
</eb:PayloadInfo>
</eb:UserMessage>
</eb:Messaging>
</S11:Header>
<S11:Body>
...
</S11:Body>
</S11:Envelope>
```

4.3.2 応答メッセージ (Response Message)

In this exchange NRR is required, so the ebMS Receipt contains a NonRepudiationInformation element, which contains a sequence of MessagePartNRInformation items for each message part for which evidence of non repudiation of receipt is being provided. In the normal default usage, these message parts are those that have been signed in the original message. Each message part is described with information defined by an XML Digital Signature Reference information item. The following example illustrates the ebMS V3 Signal Message header.

この交換では、NRRは必要であるので、ebMS 受領は、NonRepudiationInformation要素を含む。そして、受領の否認防止の証拠が提供されているメッセージ・パート毎に一連の MessagePartNRInformation アイテムを含む。通常のデフォルト使用法では、これらのメッセージ部分は、元のメッセージにおいて署名されたものである。各々のメッセージ・パートは、XML 電子署名関連情報アイテムによって定義される情報で記述される。以下の例は、ebMS V3 Signal Message ヘッダーを例示する。

```
<eb3:Messaging Soap12:mustUnderstand="true" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="ValueOfMessagingHeader">
<eb3:SignalMessage>
  <eb3:MessageInfo>
    <eb3:Timestamp>2009-11-06T08:00:09Z</eb3:Timestamp>
    <eb3:MessageId>orderreceipt1234@seller.com</eb3:MessageId>
    <eb3:RefToMessageId>12345@requester.example.com
  </eb3:RefToMessageId>
  </eb3:MessageInfo>
  <eb3:Receipt>
    <ebbp:NonRepudiationInformation>
      <ebbp:MessagePartNRInformation>
        <dsig:Reference URI="#5cb44655-5720-4cf4-a772-19cd480b0ad4">
          <dsig:Transforms>
            <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </dsig:Transforms>
          <dsig:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        </dsig:Reference>
      </ebbp:MessagePartNRInformation>
      <ebbp:MessagePartNRInformation>
        <dsig:Reference URI="cid:a1d7fdf5-d67e-403a-ad92-3b9deff25d43@buyer.com">
          <dsig:Transforms>
            <dsig:Transform Algorithm="http://docs.oasis-open.org/wss/oasis-wss-SwAProfile-1.1#Attachment-Content-Signature-Transform" />
          </dsig:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <dsig:DigestValue>iWNSv2W6SxbOYZliPzZDcXAxrWI=</dsig:DigestValue>
        </dsig:Reference>
      </ebbp:MessagePartNRInformation>
```

```
</ebbp:NonRepudiationInformation>  
</eb3:Receipt>  
</eb3:SignalMessage>  
</eb3:Messaging>
```

For a signed receipt, a Web Services Security header signing over (at least) the signal header is required. An example WS-Security header is as follows :

```
<wsse:Security s:mustUnderstand="1" xmlns:wsse="http://docs.oasis-  
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"  
xmlns:s="http://www.w3.org/2003/05/soap-envelope">  
  <wsu:Timestamp wsu:Id="_1" xmlns:wsu="http://docs.oasis-  
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">  
    <wsu:Created>2009-11-06T08:00:10Z</wsu:Created>  
    <wsu:Expires>2009-11-06T08:50:00Z</wsu:Expires>  
  </wsu:Timestamp>  
  <wsse:BinarySecurityToken EncodingType="http://docs.oasis-  
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-  
1.0#Base64Binary"  
  ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-  
token-profile-1.0#X509v3" wsu:Id="_2"  
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
wssecurity-utility-  
1.0.xsd">MIIFADCCBGmgAwIBAgIEOmitted</wsse:BinarySecurityToken>  
  <ds:Signature Id="_3" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
    <ds:SignedInfo>  
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-  
c14n#" />  
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"  
      />  
      <ds:Reference URI="#ValueOfMessagingHeader">  
        <ds:Transforms>  
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">  
            <InclusiveNamespaces PrefixList="xsd" xmlns="http://www.w3.org/2001/10/xml-  
exc-c14n#" />  
          </ds:Transform>  
        </ds:Transforms>  
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  
        <ds:DigestValue>ZXnOmitted=</ds:DigestValue>  
      </ds:Reference>  
    </ds:SignedInfo>  
    <ds:SignatureValue>rxnP4of8JCpUkOmitted=</ds:SignatureValue>  
    <ds:KeyInfo>  
      <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-  
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">  
        <wsse:Reference URI="#_2" ValueType="http://docs.oasis-  
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />  
      </wsse:SecurityTokenReference>  
    </ds:KeyInfo>  
  </ds:Signature>  
</wsse:Security>
```