Message Control and Choreography (MCC) Profile-Applicability Statement 2 (AS2)

Validated 11.00.00

	Specification Information
Name	MCC – Profile-AS2
Publication Date	13 April 2011
Version Identifier	V11.00.00

Table of Content

1. Document Management

1.1 Legal Disclaimer

RosettaNet, its members, officers, directors, employees, or agents shall not be liable for any injury, loss, damages, financial or otherwise, arising from, related to, or caused by the use of this document or the specifications herein, as well as associated guidelines and schemas. The use of said specifications shall constitute your express consent to the foregoing exculpation.

1.2 Copyright

1.3 Trademarks

RosettaNet, Partner Interface Process, PIP and the RosettaNet logo are trademarks or registered trademarks of "RosettaNet," a non-profit organization. All other product names and company logos mentioned herein are the trademarks of their respective owners. In the best effort, all terms mentioned in this document that are known to be trademarks or registered trademarks have been appropriately recognized in the first occurrence of the term.

1.4 Acknowledgments

This document has been prepared by RosettaNet (http://www.rosettanet.org/) from requirements gathered during the Milestone Program and in conformance with the methodology. Listed below are the legal entities that contributed to the design and development of this PIP.

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

1.5 Related Documents

- MCC Single Business Document PIP Template V11.00.00

1.6 Document Version History

Version	**Date**	**Description**
Validated 11.00.00	13 April 2011	Validated Version

1.7 Document Purpose

The purpose of the document is to explain the structure, the association between objects, the content of objects and the definition for single elements to a non-technical audience.

2. Single Business Document PIP Definition and Requirements

The “Single Business Document Template” section defines a model for single business document PIPs that is aligned with ebBP Single business document BusinessTransactions. It is abstract in two different ways:

1. The realization of a PIP definition component may vary with the communication technology selected for implementing the PIP.
2. The realization of a PIP definition may vary depending on the execution context assumed.

Also, the template for Single Business Document PIP definition is general in the sense that the definition of a concrete PIP will select from the model components offered. Section “Execution Parameters and Configuration” therefore describes rules for defining a customized, or “concrete” PIP.

To summarize, there are four levels at which PIP material is defined:

(1) **PIP template**: This level defines the general structure – or model - of a PIP and the features that may be used in a particular PIP definition. This is the object of this document.

(2) **PIP definition**: This level defines particular PIPs usable for business exchanges. These will usually contain parameters that are left for users to define, e.g. via an agreement between members of a supply chain. A PIP definition is prescriptive and states the conditions for a PIP instance to be considered conforming to a PIP definition.

(3) **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.

(4) **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.

2.1 Single business document Template

2.1.1 Parties involved

In RosettaNet there is the concept of "Party and "Role"

- The **PIP requester** party (or Requester), sending the Single Business Document message
- The **PIP responder** party (or Responder), receiving the Single Business Document message

Properties that are associated with each party are:

- Requester role for the PIP (specific to a PIP definition).
- Responder role for the PIP (specific to a PIP definition).

The "Party ID" associated with each role (varies across instances of the same PIP definition)

- The PIP Business Document contains two structures "fromRole" and "toRole", that contain the following definitions:
  - o Party: <GlobalBusinessIdentifier>**123456789**</GlobalBusinessIdentifier>
  - o Role: <GlobalPartnerRoleClassificationCode>**Buyer**</GlobalPartnerRoleClassificationCode>
- The RosettaNet Implementation Framework (RNIF) contains:
  - o Service and Delivery Header contains: <GlobalBusinessIdentifier>**123456789**</GlobalBusinessIdentifier>
  - o Service Header contains: <GlobalPartnerRoleClassificationCode>**Buyer**</GlobalPartnerRoleClassificationCode>

The "Party / Role" would not be used for the AS2 exchange. AS2 is defined to be independent of any business intelligence. Concepts such as business roles are not supported. The sender and intended receiver of a document exchanged using AS2 are identified by AS2-specific HTTP headers, which are prepended to the data being exchanged. The header "AS2-From" is used to identify the sender of a message and the header "AS2-To" is used to identify the intended recipient of a message.

Reference:

- RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1"
- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)

2.1.2 Business Document

The Business Document Represents the actual business content of the PIP as defined in RosettaNet business document definitions, as well as additional collateral, like drawings.

In AS2 business data may be XML, Electronic Data Interchange (EDI) in either the American National Standards Committee (ANSI) X12 format or in the UN Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) format, or in other structured data formats.

The business document is encapsulated in a MIME message and can be signed, encrypted and/or compressed.

Reference:

- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)
- RFC1767 - MIME Encapsulation of EDI Objects
- RFC3023 - XML Media Types
- RFC5322 - Internet Message Format
- RFC1847 - Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
- RFC3850 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling
- RFC3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification
- RFC3852 - Cryptographic Message Syntax (CMS)
- RFC3274 - Compressed Data Content Type for Cryptographic Message Syntax (CMS)

2.1.3 Business State Alignment features

The objective of these alignment features is to provide to each business party participating to a PIP, a common understanding about the status of the action message in terms of its reception, validity and processing prospects. Two features stand out:

- (1) **Delivery Alignment:** Gives the Requester party an assurance that the Responder e.g. has received the action message. **Acknowledgement of Receipt**), or on the contrary that it has not been received (eg. **Notification of Reception Failure**). Semantic variants of this reception can be: (a) simple acknowledgement of reception by the messaging layer, (b) confirmation that the message has been delivered to the application layer
- *NOTE: Some QoS capability such as reliable messaging may support this alignment feature. However proper relay to the business layer is required for this feature to be fulfilled.*

  In AS2 the sender of a message can optionally request that the receiver of the message return a Message Disposition Notification (MDN). The MDN only indicates that either the message was received and successfully unpackaged (e.g. decrypted and signature verified) or it will relay information about the errors that occurred while the message was being unpackaged.

  For our purposes, the sender of an AS2 message should always request a signed MDN to be returned. When the signed MDN is received and processed, the sender of the message will know whether the intended recipient received the message and whether the message was successfully retrieved from its MIME packaging.

- **(2) Validity Alignment**

  Gives the Requester an assurance that the action message has been statically validated by the Responder’s integration system (**Acknowledgement of Validity)** or on the contrary that it failed to validate (**Notification of Validation Failure**)**.**

  Different types of validation may be performed before aligning states about validity (e.g. before sending a ValidityAcknowledgement message, or by sending a validation failure notice). “Within an EDI trading relationship, if a signed receipt is expected and is not returned, then the validity of the transaction is up to the trading partners to resolve.” “In general, if a signed receipt is required in the trading relationship and is not received, the transaction will likely not be considered valid”

AS2 does not validate the payload. This functionality may be provided by the gateway software but is not part of the specification. This template defines the following validation steps or levels:

- **Syntax validation:** Check whether the business document is a well-formed document.
- **Type validation:** Check whether the business document is valid according to a schema definition file.
- **Business Rules validation**: Check whether the business document is in line with a set of business rules that can be automatically checked without touching business applications.
- **Sequence validation**: Check whether this kind of business document is expected at the current state of the super-ordinate collaboration (applies only to execution context

Additional steps

This functionality is NOT part of the AS2 specification.

- **Business entity dereferencing:** Check whether the business entities defined in the business document can be resolved within the business application.
- **Document completeness check**: Check whether the business document is complete from a business perspective. This may concern completeness of line items as defined in a business document of a prior PIP or as required by a business application.
- **Business application check:** The responder party must make sure that any validation checks have been applied to the action message that are necessary for ensuring processability of the business message.
- **Delegation to business application:** The business document has successfully been imported by the business application.

Reference:

- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)
- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using

2.2 PIP execution outcome

The state alignment features above will be used by the MCC messaging technology profiles to compute one of the following result values of a PIP execution (aligned with ebBP).

The AS2 MDNs response status is at the Messaging Service level

- Successful processing status indication
- Unsuccessful processed content
- Unsuccessful non-content processing
- Processing warnings

- **Protocol-outcome**
  - SUCCESS means: The PIP execution can be considered as fully conforming to the PIP definition or to the concrete PIP: alignment requirements, QoS requirements and other execution mode requirements have been satisfied.
  - FAILURE means: The PIP execution has been deficient in some way and violated some requirements in the PIP definition or the concrete PIP: alignment requirements, QoS requirements and other execution mode requirements, have not been observed.

2.3 Quality of Service features

(1) Security options

The data is packaged using standard MIME structures. Using Cryptographic Message Syntax with S/MIME security body parts obtains authentication and data confidentiality. Authenticated acknowledgements make use of multipart/signed Message Disposition Notification (MDN) responses to the original HTTP message.

- **Authentication**

  Authentication is accomplished digitally signing the message and/or receipt. At the transport level by HTTP Secure Socket Layer (SSL)

  1. Digitally sign the message
     - SMIME 3.0 with MD5 - RSA
     - SMIME 3.0 with SHA1 – RSA

     Note:

     - SHA1 supported by all AS2 Certified Products.
     - No guarantee of vendor support for MD5.
  2. HTTP Secure Socket Layer (SSL)

- **Confidentiality**

  Confidentiality is accomplished by encrypting the business document.

  - Encryption:

  - SMIME 3.0 with DES
  - SMIME 3.0 with 3DES
  - SMIME 3.0 with RC2 - 40
  - SMIME 3.0 with RC2 – 64
  - SMIME 3.0 with RC2 – 128

Note:

3DES supported by all AS2 Certified products. No guarantee of vendor support for encryption algorithms such as DES, RC2 variants and AES variants.

- **Integrity**

The message sender creates a message digest using a hash algorithm, also referred to as the message integrity check (MIC). The sender then computes a digital signature over the MIC. When the recipient receives the message, the recipient verifies the digital signature and MIC.

- Digital Signature
  - SMIME 3.0 with MD5 – RSA
  - SMIME 3.0 with SHA1 - RSA

- **Non Repudiation of Origin / Non Repudiation Of Receipt**

The receipt contains data identifying the original message for which it is a receipt, including the message-ID and a cryptographic hash (MIC). The original sender must retain suitable records providing evidence concerning the message content, its message-ID, and its hash value. The original sender verifies that the retained hash value is the same as the digest of the original message, as reported in the signed receipt.

- Authentication is accomplished digitally signing the message and/or receipt

- Digital Signature
  - SMIME 3.0 with MD5 – RSA
  - SMIME 3.0 with SHA1 – RSA

- **Authorization**

Authorization is accomplished by the trading partner agreement.

(2) Reliable Messaging:

- **Guaranteed delivery (At-least-Once delivery)**

  Guaranteed delivery is accomplished by using the Message Disposition Notification (MDN). This is an optional specification for AS2 and may not implement by all AS2 vendors. However, most AS2 vendors provide for some level of reliable messaging.

- **Duplicate elimination (At-Most-Once delivery)**

  In the AS2 standard, detection of duplicates by Message-Id or by business transaction identifiers is recommended.

(3) Timing Constraints

- **Time to acknowledge validity (or invalidity):**

  This QoS setting is part of the trading partner agreement.

- **Time to Perform**:
  This QoS setting is part of the trading partner agreement.

Reference: Operational Reliability for EDIINT AS2

3. PIP Parameterization and Execution Control

1. **PIP property parameters:** these are parameters that control the use of features defined above as PIP properties: level of state alignment and various QoS features.

2. **PIP execution parameters:** these are parameters that control the actual execution of the PIP.

3.1 PIP Property Parameters

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

Specification item	Configurable	Implication	Explanation
Send Request Document	NO		A request document must be sent
Overall Time To Perform	YES	In Trading Partner Agreement	• AS2 exchanges a single document with a receipt (MDN). This setting equals Time To Acknowledge • The "Operational Reliability for EDIINT AS2" specifications are more about "fire and forget" and how long before you ultimately give up on sending the message. • The MDN timeout is part of AS2
Receipt-Acknowledgement	YES	Message Disposition Notification (MDN)	Sync / Async / None
Non Repudiation	YES	Digitally signing the Payload	Refer to: RFC4130
Non Repudiation of Receipt	YES	Digitally signing the MDN	Refer to: RFC4130
Time To Acknowledge Receipt	YES	In Trading Partner Agreement	The MDN timeout is part of AS2
Reliability	Yes	In Trading Partner Agreement	• Retry sending unsuccessful POSTs. • Resend messages when MDNs not received. • Refer to: Operational Reliability for EDIINT AS2 Operational Reliability for EDIINT AS2 Retry when message not successfully POSTed. Resend exact same message when MDN not received in a timely manner.Retry when message not successfully POSTed. Resend exact same message when MDN not received in a timely manner.Retry when message not successfully POSTed. Resend exact same message when MDN not received in a timely manner.Refer to: Operational Reliability for EDIINT AS2 Refer to: Operational Reliability for EDIINT AS2 Refer to: Operational Reliability for EDIINT AS2

Specification item	Configurable	Implication	Explanation
Confidentiality	YES	HTTPs and/or Encryption	• HTTPs is an encrypted channel. • AS2 messages can also be encrypted before they are sent.
Integrity	YES	Message Integrity Check (MIC) calculation of signed messages	Calculating the MIC of the message received and verifying that MIC with the MIC extracted from the signature applied to the message will ensure that the message has not been tampered with.
Authentication	YES	Digital Signatures	The receiver of a message can authenticate the sender of a message if digital signatures are used.
Authorization	YES	In Trading Partner Agreement	Valid relationship exist between the agreement in sender / recipient
Intelligible Check Required	YES	In Trading Partner Agreement	Validation of message not in AS2 Specification
RetryCount	YES	In Trading Partner Agreement	Refers to HTTP Error Recovery

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

3.2 PIP execution modes and related parameters

AS2 exchanges a single document with a receipt Acknowledgement, the Message Disposition Notification (MDN). These modes are related to it.

- **Synchronous execution**

  Synchronous Receipt - A receipt returned to the sender during the same HTTP session as the sender's original message.

- **Asynchronous execution with callback**

  Asynchronous Receipt - A receipt returned to the sender on a different communication session than the sender's original message session.

- **Asynchronous execution with pulling**

  Asynchronous Receipt - A receipt returned to the sender on a different communication session than the sender's original message session.

3.3 PIP Instance Correlation and Identification

3.3.1 PIP Identification

Generation of Globally Unique Ids (GUIDs) for PIP instances

PIP instance ids are to be generated by the PIP requester by appending an id that is unique within their systems to their globally unique partner id, preferably a GLN or a DUNS number. This is locate in the PIP Business Document, the Service Header and Delivery Header

The AS2 Header contains a unique messaging id “Message-ID”

Note: A ‘n’ Action PIP will require PIP instance ID

Inclusion of PIP instance GUIDs within RosettaNet message definitions

The inclusion of PIP instance GUIDs is not addressed at this point in time. MCC Phase 2 will address this topic and provide a detailed specification for this topic.

3.3.2 Message Correlation

Message correlation denotes the act of associating messages with process instances, which may be implemented at the messaging level or at the PIP process level.

- MDNs are automatically correlated per the specification.
- Business document correlation (n-Action PIPs) and is in the payload

```
Requestor   <thisDocumentIdentifier>
                <ProprietaryDocumentIdentifier>2222</ProprietaryDocumentIdentifier
            </thisDocumentIdentifier>
Responder   <requestingDocumentIdentifier>
              <ProprietaryDocumentIdentifier>2222</ProprietaryDocumentIdentifier>
            </requestingDocumentIdentifier>
```

4. 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.

4.1 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 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>
```

The following specifications' requirements are incorporated into the Profile by reference, except where superseded by the Profile: (http://ietfreport.isoc.org/)

- RFC1767 - MIME Encapsulation of EDI Objects
- RFC1847 - Security Multiparts for MIME: Multipart/Signed & Multipart / Encrypted
- RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1
- RFC2634 - Enhanced Security Services for S/MIME
- RFC3023 - XML Media Types
- RFC3274 - Compressed Data Content Type for Cryptographic Message Syntax (CMS)
- RFC3798 - Message Disposition Notification
- RFC3850 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1
- Certificate Handling
- RFC3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification
- RFC3852 - Cryptographic Message Syntax (CMS)
- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)
- RFC5322 - Internet Message Format
- RFC5323 - Web Distributed Authoring and Versioning (WebDAV) SEARCH
- Operational Reliability for EDIINT AS2: draft-duker-as2-reliability-06