1 Business Scenario

2 Introduction

2.1 Component Monitoring

2.2 Message Monitoring

2.3 End-to-End Monitoring

2.4 Alerting

2.5 Acknowledgments

3 Prerequisites

4 Test Landscape

4.1 Single-Action PIP: PIP0C1 Asynchronous Test Notification

4.2 Two-Action PIP: PIP0C2 Asynchronous Test Request/Confirmation

5 Best Practices

5.1 Industry-Standard-Specific Configuration Steps

5.2 Good Day Scenario 1: Strong Receipt Acknowledgment (Single-Action PIP)

5.3 Good Day Scenario 2: Weak Receipt Acknowledgment (Single-Action PIP)

5.4 Good Day Scenario 3: Secure Communication (Single-Action PIP)

5.5 Good Day Scenario 4: End-to-End Monitoring (Single-Action PIP)

5.6 Bad Day Scenario 1: System Error in Integration Server (Single-Action PIP)

5.7 Bad Day Scenario 2: Time to Acknowledge Fails (Single-Action PIP)

5.8 Bad Day Scenario 3: Validation Fails Due to Mismatch in Partner Agreement (Single-Action PIP)

5.9 Bad Day Scenario 4: Security Verification Fails (Single-Action PIP)

5.10 Bad Day Scenario 5: Time to Perform Fails (Two-Action PIP)
1 Business Scenario

Several industry standard organizations have been founded by companies within the same business sector in order to define industry-wide and open standards for their business processes, mainly focusing on their business-to-business (B2B) processes. These standards include RosettaNet for the high tech industry, CIDX (Chemical Industry Data Exchange) for the chemical industry, PIDX (Petroleum Industry Data Exchange) for the oil and gas industry, and UCCNet (Uniform Code Council) for the consumer products and retail industry.


Business processes between trading partners are based on Partner Interface Processes (PIP). PIPs are system-to-system XML-based dialogs. Each PIP includes a business document, and specifies the choreography of the business transaction dialog (BTD).

There are two message types:
- RosettaNet action message: contains business content, for example purchase order data.
- RosettaNet signal message: acknowledgment/exception sent in response to an action message.

PIPs do not describe complex business processes, but rather a simple, transactional exchange of business documents that could be either:
- Single-action: one-way notification
- Two-action: request and confirmation

In addition to the document itself, PIPs specify the partner business roles (for example, buyer, seller, initiator, responder), activities between roles, the sequence of documents that are exchanged, timeouts, retry mechanisms, security settings (signature, encryption, non-repudiation of receipt, of origin, and of content) and so on.

2 Introduction

The B2B adapters provided by SAP XI 3.0 follow the industry-specific standards based on the industry they are aligned to:
- RNIF adapters for the high tech industry, based on RosettaNet protocol RNIF 1.1 and RNIF 2.0
- CIDX adapter for the chemical industry, based on RNIF 1.1 protocol

For more information about the RNIF adapter and CIDX adapter, see SAP Help Portal at help.sap.com → SAP NetWeaver → SAP NetWeaver 2004. In the documentation, choose SAP NetWeaver → Process Integration → SAP Exchange Infrastructure → Runtime → Connectivity → Adapters → RNIF Adapters/CIDX Adapter.

For more information about the configuration of the related business packages, see the corresponding configuration guides.
You can find the configuration guide for the RosettaNet business package on SAP Service Marketplace at service.sap.com/ibc → Industry Solutions → SAP for HighTech → Order to Invoice – RosettaNet.

You can find the configuration guide for the CIDX business package on SAP Service Marketplace at service.sap.com/ibc → Industry Solutions → SAP for Chemicals → Order to Invoice.

This How-to Guide deals with the monitoring concepts that are available for the industry standard adapters within SAP XI 3.0. The different monitoring concepts are described in relation to the RNIF 1.1 protocol. However, the concepts are also applicable to RNIF 2.0 and CIDX.

The following monitoring mechanisms are adopted in SAP XI:

- Component monitoring
- Message monitoring
- End-to-end monitoring
- Alerting
- Acknowledgments

This chapter provides a brief introduction to the different monitoring tools, focusing in particular on the monitoring of the RNIF adapters. For more information about the monitoring functions of SAP XI in general, see the following two information sources:

- Documentation on SAP Help Portal
  You can find the documentation on SAP Help Portal at help.sap.com → SAP NetWeaver → SAP NetWeaver 2004. In the documentation, choose SAP NetWeaver → Process Integration → SAP Exchange Infrastructure → Runtime → Central Monitoring.

- How-to Guide How To Monitor Exchange Infrastructure 3.0
  You can find this How-to Guide on SAP Service Marketplace at service.sap.com/nw-howtoguides. Choose Exchange Infrastructure. This How-to Guide also deals with the configuration steps necessary to set up the individual monitoring tools.

### 2.1 Component Monitoring

Component monitoring can be accessed using the Runtime Workbench (RWB), the central monitoring tool of SAP XI. It enables you to display an overview of the status of each component of SAP XI.

For the Adapter Engines, you can launch the adapter monitor, which provides an overview of the status of the individual adapters and communication channels. Here, you can check whether the configured RNIF adapters are working properly.

### 2.2 Message Monitoring

The Runtime Workbench (RWB) provides central access to all message monitoring tools, for example for the Integration Server of SAP XI, Integration Engines of SAP Web Application Server based application systems, and Adapter Engines. It allows you to study the messages in detail in order to find errors that occurred during message processing.

For the Adapter Engine, the following type of information is displayed in the detail view of the message monitoring:
- Message Data: Displays all relevant message header information.
- Message Content: Displays envelope and payload of selected message.
- Message Audit: Displays a detailed list of the individual steps carried out during message processing.
- Message Security: Displays the security agreements as well as the certificates used (only when handling message-level security or communication-level security).
- Adapter Details: Displays the RosettaNet transaction trace (only for messages that have been processed by the RNIF adapter).
- End-to-End: Opens the end-to-end monitoring instance view of the selected message (only if respective data exists).

2.3 End-to-End Monitoring

End-to-end monitoring allows you to trace the complete message flow, from start to end. It displays the status of each message processing step within the individual components that the message went through. It is based on the Process Monitoring Infrastructure (PMI) shipped by the SAP Web Application Server.

For the RNIF adapters, a set of agents is invoked, for example adapter inbound agent, adapter outbound agent, ID mapping agent, status agent. These agents pass the relevant monitoring data to PMI.

2.4 Alerting

Alerts are used to notify users about critical situations, so that immediate and timely action can be taken. Message-based alerting is embedded within the RWB, and is based on the Alert Framework that is shipped by the SAP Web Application Server. By defining alerting rules, you can restrict the alerts to be triggered depending on message header properties, or the component where the error occurs. For example, you can define a specific alert category for errors that occur during processing within RNIF adapters only. By default, the alerts are routed to the alert inbox. In addition, they can be sent to various other delivery channels, such as e-mail or cell phone.

With respect to industry standard adapters, alerts are triggered for various scenarios, which are discussed here. In general, whenever a business transaction dialog fails, an alert is raised. The following use cases exist:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Comments</th>
<th>Supported By</th>
</tr>
</thead>
<tbody>
<tr>
<td>System receives exception</td>
<td>System receives an exception for an action message that is sent to its partner. On the partner side, the processing of the action message fails, and the partner system sends an exception instead of a receipt acknowledgment to the initiating system. Possible reason for failure: Validation fails.</td>
<td>RNIF/CIDX</td>
</tr>
<tr>
<td>System sends exception</td>
<td>System sends an exception for a failed action message that is sent by a partner. Possible reason for failure: Any error in action message, system error or application error</td>
<td>RNIF/CIDX</td>
</tr>
</tbody>
</table>
System receives NOF

System receives a notification of failure (NOF) due to a failure in message processing on the partner side. After the system sent an action message to its partner, a receipt acknowledgment was received, but followed by an NOF. Possible reason: Action or response message processing failed.

Time to acknowledge fails

The time to acknowledge receipt criterion has not been met. Partner system fails to send a receipt acknowledgment for the action message sent by the system. The specified number of retries is exceeded, so the BTD fails. Applicable for single-action notification, and two-action request and confirmation.

Time to perform fails (Two-action only)

The time to perform criterion has not been met. System receives a receipt acknowledgment, but no response message. Partner system fails to send a confirmation/response. The specified time to wait for a response is exceeded, so the BTD fails, and an exception is raised.

Security failure

Possible reason:
System tries to send an action message, but the necessary certificates for signing could not be found in key store.
System sends signed action message, but receipt acknowledgment has no signature.
System sends signed action message, but certificate is invalid.

Correlation (Two-action only)

Response could not be correlated to action message.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SXMS_TO_ADAPTER_TYPE</td>
<td>Adapter type (here: RNIF)</td>
</tr>
<tr>
<td>SXMS_TO_ADAPTER_ERRTXT</td>
<td>Adapter error text</td>
</tr>
<tr>
<td>SXMS_AF_ERRVAL1</td>
<td>Message ID of initiating action message</td>
</tr>
<tr>
<td>SXMS_AF_ERRVAL2</td>
<td>Message tracking ID</td>
</tr>
<tr>
<td>SXMS_AF_ERRVAL3</td>
<td>Document ID of action message</td>
</tr>
<tr>
<td>SXMS_AF_ERRVAL4</td>
<td>Time stamp of action message</td>
</tr>
<tr>
<td>SXMS_AF_ERRVAL5</td>
<td>Process instance ID of action message</td>
</tr>
</tbody>
</table>

The information that is included with the alert enables easy identification of the message and the type of error. In addition to the standard parameters like message GUID and header information, the following industry-speak-specific information is provided:
### 2.5 Acknowledgments

An acknowledgment replies to an asynchronous request message in order to inform the sender about the status of the message processing. There are four different types of acknowledgments:

- **System acknowledgment**: Sent back when the request message arrives at the final receiver.
- **System error acknowledgment**: Sent back when a system error occurs during message processing within SAP XI.
- **Application acknowledgment**: Sent back when the request message is successfully processed within the receiver application.
- **Application error acknowledgment**: Sent back when an error occurs during message processing within the receiver application.

In RosettaNet notation, acknowledgments are called RosettaNet signal messages. The following signal types exist:

- **Positive signal message**:
  - Receipt acknowledgment: Partner considers action to be valid, both structurally and syntactically. Also, to track reliability of delivery, and for non-repudiation purposes.
  - Acceptance acknowledgment: Sent when partner accepts message to be processed in his backend. However, this does not indicate success or failure of message processing (supported by RNIF 1.1 only)

- **Negative signal message**:
  - Receipt acknowledgment exception: Partner considers action to be invalid either structurally or syntactically (supported by RNIF 1.1 only).
  - Acceptance acknowledgment exception: Partner does not accept action for processing in backend (supported by RNIF 1.1 only).
  - General exception: Any other error not mentioned above.

In general, the sender of the request message has to explicitly specify which type of acknowledgment is requested. For the industry standard adapters, you have to configure the receipt acknowledgment mode in the sender communication channel. The following types of acknowledgments are requested depending on the mode:

- **Strong mode**:
  - System acknowledgment
  - System error acknowledgment
  - Application error acknowledgment

- **Weak mode**:
  - System error acknowledgment
  - Application error acknowledgment

### 3 Prerequisites

The RNIF 1.1 adapter is shipped with SAP XI 3.0 SP13. The alerting functionality in conjunction with the industry standard adapters has been supported since SAP XI 3.0 SP16.
4 Test Landscape

For the test runs, two Adapter Engines communicate with each other using the RosettaNet protocol, hence simulating B2B transaction between two RosettaNet-compliant trading partners. The central Adapter Engine acts as the initiator, a non-central Adapter Engine as the responder.

Two scenarios are considered:
- PIP0C1: Asynchronous Test Notification
- PIP0C2: Asynchronous Test Request/Confirmation

4.1 Single-Action PIP: PIP0C1 Asynchronous Test Notification

* Initiator: Central AE
* Responder: Non-Central AE
4.2 Two-Action PIP: PIP0C2 Asynchronous Test Request/Confirmation

* Initiator: Central AE
  Responder: Non-Central AE
5 Best Practices

5.1 Industry-Standard-Specific Configuration Steps

The following examples demonstrate some industry-standard-specific configuration steps based on the single-action PIP PIP0C1. The partner roles are initiator and responder.

1. Start the Integration Builder (Configuration).

Create new communication parties (shortened to: parties) for the trading partners involved in the collaboration process.

For each party, maintain Alternative Identifiers to uniquely identify the party across company boundaries. Here, Dun & Bradstreet Corporation is used as the agency, and DUNS number as the scheme.

Create a new service for the party. The service name has to comply with the following notation:

:\text{PIP}<\text{PIP Code}>_<\text{PIP Version}>_<\text{Partner Role}>

Example:

\text{PIP0C1_R0102_Responder}

2. Create a communication channel by importing a communication channel template. It is part of the business package for RosettaNet.
3. For the receiver communication channel, select template PIP0C1_R0102_Responder_Receiver_AsyncNotificationAction_11

4. The message-protocol-specific information and PIP information is specified automatically according to the template chosen. Because of this, you only have to maintain the transport parameters and authentication. Specify the following parameters:
   - **URL (under Transport Parameters)**
     Specify the URL that points to the responder service that the action message is sent to.
   - **User Name/Password (under Authentication)**
     Specify the corresponding user name and password. Here, the non-central Adapter Engine is addressed.

5. For the sender communication channel, select template PIP0C1_R0102_Initiator_Send_AsyncNotificationAction_11
6. The message-protocol-specific information and PIP information is specified automatically according to the template chosen.

Because of this, you only have to maintain the transport parameters and authentication. Specify the following parameters:

- **URL (under Transport Parameters)**
  Specify the URL that points to the initiator service.

- **User Name/Password (under Authentication)**
  The settings are required for sending the signal message to the sender service. Here, the central Adapter Engine is addressed.
5.2 Good Day Scenario 1: Strong Receipt Acknowledgment (Single-Action PIP)

Upon successful delivery of XI message, IS sends Sys Ack to adapter.

7. In the Integration Builder (Configuration), maintain the sender communication channel. Set the Receipt Acknowledgment mode to Strong.
8. During runtime, the RNIF Adapter determines the partner's service name for an incoming action message based on the corresponding header fields of the service header. The name is built according to the naming convention mentioned above (see step 1).

9. Start Message Monitoring (transaction SXMB_MONI), and display the request message.

For the incoming action message, the globally unique identifier (here the DUNS number) is mapped to the internal party name using the Alternative Identifiers (normalization).

The Reliable Messaging header segment shows which acknowledgment types are requested.

For strong receipt acknowledgment, these are:

- System ack
- System error ack
- Application error ack

10. Launch the RWB, and go to Message Monitoring for the non-central Adapter Engine.

The messages are exchanged in the following sequence:

- Inbound action message
- Outbound XI message
- Inbound XI acknowledgment
- Outbound signal message (receipt acknowledgment)
11. Choose Details to display the Audit Log of the action message.

12. Switch to the Adapter Details tab page to display the RosettaNet transaction details, a list of all processed messages involved in the BTD, and the RosettaNet transaction trace.
5.3 Good Day Scenario 2: Weak Receipt Acknowledgment (Single-Action PIP)

-Initiator (RNIF)
-Responder (RNIF Adapter)
-XI IS
-Business System

RNIF::Request
XI::Request
RNIF::ReceiptAck
 XI Reliable Messaging Header contains request for Sys Error Ack, and App Error Ack

13. In the Integration Builder (Configuration), maintain the sender communication channel.

Set the Receipt Acknowledgment mode to Weak.

14. Start Message Monitoring (transaction SXMB_MONI), and display the request message.

According to the Reliable Messaging header segment, the following acknowledgments are requested for weak receipt acknowledgment:

- System error ack
- Application error ack
15. Start the RWB, and go to *Message Monitoring* for the non-central Adapter Engine.

The messages are exchanged in the following sequence:

- Inbound action message
- Outbound XI message
- Outbound signal message (receipt acknowledgment)
5.4 Good Day Scenario 3: Secure Communication (Single-Action PIP)

16. Start the Integration Builder (Configuration).
    Maintain the message security policy parameters in the receiver communication channel (under Security Policy). You can specify the following security policies:
    - Sign the action message
    - Sign the signal message
    - Non-repudiation of receipt acknowledgment, and of origin and content

17. Maintain the message security policy parameters in the sender communication channel.

18. In the receiver agreement, specify the security settings.
    Maintain the trust model. For Trust Model, select direct. In this case, the partner’s certificate is directly validated against the certificate in the J2EE key store.

    Under Current Certificate for Signing, maintain the following parameters:
    - Algorithm
      Only algorithm SHA-1 is supported.
    - Keystore View
    - Keystore Entry
Enter the name of the initiator's private key.

Under **Partner Certificate for Signing**, maintain the following parameters:

- Keystore View
- Keystore Entry
  - Enter the name of the partner's public key.

19. In the sender agreement, specify the security settings.

Maintain the trust model (see step 18).

Under **Current Certificate for Signing**, maintain the following parameters:

- Algorithm
  - Only algorithm SHA-1 is supported.
- Keystore View
- Keystore Entry
  - Enter the name of the responder's private key.

Under **Partner Certificate for Signing**, maintain the following parameters:

- Keystore View
- Keystore Entry
  - Enter the name of the initiator's public key.

20. Start the RWB, and go to **Message Monitoring** for the central Adapter Engine.

Select the action message, and choose **Details**.

The **Audit Log** indicates that the action message was signed using the private key of the initiator.

The Message Security Monitor shows the details about the RNIF security agreements, and the certificate used.

22. Go to Message Monitoring for the non-central Adapter Engine, select the action message, and choose Details.

The Audit Log indicates that the action message was verified using the public key of the initiator.

23. Analogously to the action message, you can monitor the security settings of the signal message.

The signal message is signed using the responder’s private key.

24. The signal message is verified using the responder’s public key.

25. The Message Security Monitor shows the details about the certificate used.
5.5 Good Day Scenario 4: End-to-End Monitoring (Single-Action PIP)

To describe end-to-end monitoring, the figure depicts a message that is sent from SAP ERP via SAP XI and the RNIF adapter of the central Adapter Engine, to the RNIF adapter of the non-central Adapter Engine.

26. Start the RWB, and go to End-to-End Monitoring.

Select the respective message. This takes you to the Instance View where detailed information about an instance (here a message) is provided both in table form and graphically.

The request message is sent from the SAP ERP system to SAP XI using the ABAP proxy runtime. The PMI inbound agent tracks the message coming into the local Integration Engine of SAP ERP. It is called immediately after a message is received. Thereafter, the message is sent to the Integration Server.
27. After the request message comes into the Integration Server, the receiver is determined, and the message is transferred to the central Adapter Engine for further processing.

28. In the central Adapter Engine, the incoming message is tracked, followed by a channel determination, and an ID mapping.

The ID mapping agent tracks any change of the message ID. It is called immediately after the message ID is changed, in this case after the conversion from an XI message to an RNIF message.

Finally, the status agent tracks the status of the message processing. In this case, it is stated that the message was successfully delivered.

29. Select a process step. This opens the attribute display, where detailed information about the selected process step is displayed.

Here, the details for the channel determination step are displayed. To access further analysis tools, choose the tool icon next to the message ID. This starts Message Monitoring.
30. The **outbound agent** tracks the sending of a message. It is called before a message is sent out of the adapter. In the example, it is stated that the action message has been sent out of the RNIF adapter.

31. In the RNIF adapter of the non-central Adapter Engine, the **inbound agent** is invoked to track the incoming of the action message.

32. The ID mapping is tracked while the RNIF message is converted to an XI message, and the XI message is sent to the XI resource adapter.
33. In the RNIF adapter of the central Adapter Engine, the *inbound agent* is invoked to track the incoming of the signal message.
5.6 Bad Day Scenario 1: System Error in Integration Server (Single-Action PIP)

An error occurs in the Integration Server (for example, no receiver could be determined), so a transient system error acknowledgment is sent back. After the message has been canceled, a permanent system error acknowledgment is sent back to the initiator of the action message.

34. Start Message Monitoring for the non-central Adapter Engine in the RWB, and display the adapter details.

The RosettaNet transaction trace indicates that two XI system error acknowledgments were sent from the Integration Server to the non-central Adapter Engine. When the permanent system error acknowledgment arrives, an RNIF exception signal is sent back to the initiator.

35. Go to Message Monitoring for the central Adapter Engine in the RWB, and display the adapter details.

A general exception signal was sent from the responder to the initiator, and a corresponding alert was raised.
36. In RWB, start your Alert Inbox.

An alert was raised by the sender of the general exception, that is, the RNIF adapter of the non-central Adapter Engine.

37. An alert was raised by the receiver of the general exception, that is, the RNIF adapter of the central Adapter Engine.
38. The RNIF adapter forwards the RNIF exception as an XI system error acknowledgment, as can be seen in Message Monitoring (transaction SXMB_MONI).
5.7 Bad Day Scenario 2: Time to Acknowledge Fails (Single-Action PIP)

The initiator sends an action message to the trading partner, but the delivery of the corresponding receipt acknowledgment fails.

39. Start the **Integration Builder** (Configuration), and maintain the **Number of Retries**, and the **Time to Acknowledge Receipt**

In the receiver communication channel, maintain the following parameters.

Under **Message Exchange Controls**, maintain the following parameters:

- **Time to Acknowledge Receipt**: Indicates the time by which the acknowledgment of receipt signal must be returned
- **Number of Retries**: Indicates how often the action message is retransmitted before the adapter receives a signal from the partner.

In this example, for test purposes the action message should be resent every 2 minutes as long as a receipt acknowledgment has not been received, up to maximum of 3 times.
40. Go to **Message Monitoring** for the central Adapter Engine in the RWB, and display the adapter details.

The RosettaNet transaction trace indicates that the acknowledgment period expired, and that the action message was resent to the partner. Finally, the maximum number of retries exceeded, and a corresponding alert was raised.

41. In RWB, start your **Alert Inbox**.

An alert was raised by the initiator of the action message, that is, the RNIF adapter of the central Adapter Engine.
5.8 Bad Day Scenario 3: Validation Fails Due to Mismatch in Partner Agreement (Single-Action PIP)

The initiator sends an action message to the trading partner, but the validation of the message against the sender agreement of the partner fails.

42. Go to Message Monitoring for the central Adapter Engine in the RWB, and display the adapter details.

The RosettaNet transaction trace indicates that a general exception signal was sent from the responder to the initiator, and that a corresponding alert was raised.

43. Enter Message Monitoring (transaction SXMB_MONI), and display the details of the XI system error acknowledgment.

The Error header segment indicates that an error occurred during reading or validation of an RNIF action message.
44. In RWB, start your Alert Inbox.

An alert was raised by the sender of the general exception, that is, the RNIF adapter of the non-central Adapter Engine.

<table>
<thead>
<tr>
<th>Category</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
</tbody>
</table>

Alert Box of XIIG User

<table>
<thead>
<tr>
<th>Short Text</th>
<th>Long Text</th>
<th>Recipient</th>
<th>Follow-On Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message GUID: 56a81230b97211de6b0d000c296baf1c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Party: RNIF1_PARTNER_SA01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Service: PPPOC1_R0102_Responder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Interface: GeneralException</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver Party: RNIF1_II_SA01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver Service: PPPOC1_R0102_Initiator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver Interface: GeneralException</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adapter: RNIF1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adapter Error: RNIF1蹇VCSP161</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

45. An alert was raised by the receiver of the general exception, that is, the RNIF adapter of the central Adapter Engine.

<table>
<thead>
<tr>
<th>Category</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
<tr>
<td>Message-Based Alerts</td>
<td></td>
<td>Message-Based Alerting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Short Text</th>
<th>Long Text</th>
<th>Recipient</th>
<th>Follow-On Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message GUID: ca76880b97811de6e43000c296be504</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Party: RNIF1_PARTNER_SA01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Service: PPPOC1_R0102_Responder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Interface: GeneralException</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver Party: RNIF1_II_SA01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver Service: PPPOC1_R0102_Initiator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver Interface: GeneralException</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adapter: RNIF1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adapter Error: RNIF1蹇RCOP16</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Roundtrip specific:
- Message ID of initiating action: c93540d16797711de6d873000c296be504
- Message Tracking ID: Sa6f1200097211da8d0d000c296be504
- Document ID of action: 901
- Timestamp of action: 20081211183030.005Z
- Process Instance ID of action: c08ba100697811de6b0d000c296be504
- Message ID of Exception signal: 56a81230b97211de6b0d000c296baf1c
46. The general exception contains details about the reason for the validation failure.

In general, the incoming action message is validated against the following parameters in the sender communication channel:

- Process name
- Transaction name
- Requesting action
- Code
- Version
- Current role
- Partner role
5.9 Bad Day Scenario 4: Security Verification Fails (Single-Action PIP)

The initiator sends a signed action message to the trading partner, but the signature verification fails on the partner side.

47. Launch the RWB, and go to **Message Monitoring** for the non-central Adapter Engine. 

Select the action message, and choose **Details**.

The Audit Log indicates that the signature verification failed because the action message was signed with a different key.

48. Go to **Message Monitoring** for the central Adapter Engine, and display the adapter details.

The RosettaNet transaction trace indicates that a general exception signal was sent to the initiator, and that a corresponding alert was raised.

49. The general exception contains details about the reason for failure.
50. In RWB, start your Alert Inbox.

An alert was raised by the sender of the general exception, that is, the RNIF adapter of the non-central Adapter Engine.

51. An alert was raised by the receiver of the general exception, that is, the RNIF adapter of the central Adapter Engine.
5.10 Bad Day Scenario 5: Time to Perform Fails (Two-Action PIP)

The initiator sends an action message to the trading partner who fails to return a confirmation in time.

52. Start the Integration Builder (Configuration).

In the receiver communication channel, maintain the following parameters.

Under Message Exchange Controls, maintain the following parameters:

- Number of Retries
- Time to Acknowledge Receipt
- Time to Perform

Indicates the time by which the response message in a two-action PIP must be returned.

In this example, for test purposes the partner that received the action message has to send a confirmation within 5 minutes. Otherwise, the BTD fails.

53. Go to Message Monitoring for the central Adapter Engine in the RWB, and display the adapter details.

The RosettaNet transaction trace indicates that the time to perform expired while waiting for a response action message, and that a
corresponding alert was raised.