Sun B2B Suite HIPAA Protocol Manager User's Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820–1277–10
December 2007

071212@19028

Contents

Preface

Sun B2B Suite HIPAA Protocol ManagerUser's Guide explains how to install, configure, deploy, and use the Sun Java™ Composite Application Platform Suite (Java CAPS) Sun B2B Suite HIPAA Protocol Manager (PM). This product is part of the Sun B2B Suite.

Who Should Use This Book

This book is intended for computer users who have the ability and responsibility of setting up and maintaining a fully functioning Java CAPS system.

These persons must also understand any operating systems on which Java CAPS is installed, for example, and must be thoroughly familiar with Windows-style user interface operations, as well as having a familiarity with the HIPAA protocol.

Before You Read This Book

Before you try to understand the concepts presented in this book and begin using the tutorial and reference materials it presents, make sure you read or are familiar with the references listed under Related Books. You must be especially proficient in the basic use of eGate™ Integrator, eWay™ Adapters, eInsight™ Business Process Manager, and eXchange™ Integrator.

How This Book Is Organized

This book contains the following chapters:

- Chapter 1, "Introduction," provides a brief summary of HIPAA PM and its operation, as well as an overview of this document.
- Chapter 2, "Overview of HIPAA PM," gives an overview of HIPAA PM, HIPAA, and eXchange.
- Chapter 3, "Installing HIPAA PM," explains installation procedures, before and after installation, as well as system requirements.
- Chapter 4, "Configuring HIPAA PM," explains the eXchange ePartner Manager (ePM) configuration steps necessary to allow HIPAA PM to operate in your environment.

- Chapter 5, "Quick Start for HIPAA PM," provides a brief overview of how to set up and run the HIPAA PM Project sample scenario provided with the product.
- Chapter 6, "HIPAA PM Sample Scenario Tutorial," explains in detail, how to implement and use the HIPAA PM sample Project scenario.
- Appendix A, "Externally Assigned Unique IDs" explains how HIPAA PM handles this type of unique ID.

Related Books

The following books provide additional related information about topics in this book:

The following books provide additional related information about topics in this book:

- *Java Composite Application Platform Suite Installation Guide*
- *Java Composite Application Platform Suite Deployment Guide*
- *Sun SeeBeyond eGate Integrator User's Guide*
- *Sun SeeBeyond eGate Integrator System Administration Guide*
- *Sun SeeBeyond eGate Integrator JMS Reference Guide*
- *Sun SeeBeyond File eWay Adapter User's Guide*
- *Sun SeeBeyond Batch eWay Adapter User's Guide*
- *Sun SeeBeyond Oracle eWay Adapter User's Guide*
- *Sun SeeBeyond LDAP eWay Adapter User's Guide*
- *Sun SeeBeyond HTTP(S) eWay Adapter User's Guide*
- *Sun SeeBeyond eInsight Business Process Manager User's Guide*
- *Sun SeeBeyond HIPAA OTD Library User's Guide*
- *Sun B2B Suite eXchange Integrator User's Guide*
- *Sun B2B Suite eXchange Developer's Guide*
- B2B Suite Readme file for HIPAA PM information

Screen Captures

Depending on what products you have installed, and how they are configured, the screen captures in this book may differ from what you see on your system.

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.

TABLE P–1 Typographic Conventions *(Continued)*

Typeface	Meaning	Example
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell	`machine_name%`
C shell for superuser	`machine_name#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell for superuser	`#`

◆ ◆ ◆ CHAPTER 1

Introduction

This document provides instructions and background information for all users of HIPAA PM.

This chapter contains the following sections:

About HIPAA Protocol Manager

This document provides instructions and background information for all users of HIPAA PM.

The purpose of this document is to help you with the following information:

- The nature and function of HIPAA (Health Insurance Portability and Accountability Act) and HIPAA PM.
- The relationship of HIPAA PM to other components of Java CAPS, including eXchange™ Integrator and eGate™ Integrator, as well as the appropriate eWay™ Adapters.
- The HIPAA PM components and editors and how to use them in your environment.
- Importing and implementing a HIPAA PM sample Project scenario provided with the product.

Additional HIPAA References

For more information on HIPAA, see the following Web sites:

- `http://www.cms.hhs.gov`
- `http://www.hipaa-dsmo.org`
- `http://www.wedi.org/`
- `http://www.claredi.com/`

- http://aspe.os.dhhs.gov/admnsimp/

For more information on the National Council for Prescription Drug Programs, Inc. (NCPDP), visit the official NCPDP Web site at this address:http://www.ncpdp.org/

◆ ◆ ◆ CHAPTER 2

Overview of HIPAA PM

This chapter provides a general overview of HIPAA data structuring, as well as HIPAA PM and its place in Java CAPS, including system descriptions, general operations, and basic features.

This chapter contains the following topics:

About the HIPAA Protocol

The acronym HIPAA stands for the Health Insurance Portability and Accountability Act (of 1996). This law is designed to protect health care patients and ensure the fast, easy exchange of patient-related data. Among other things, the act makes specifications affecting standards of treatment and privacy rights.

The act provides a number of standardized transactions that can be used for such things as a health-care eligibility inquiry or a health care claim. The HIPAA protocol realizes these legal mandates in the form of a standardized, universal data-messaging format and structure.

HIPAA Message Structure

HIPAA messages have a message structure that indicates how data elements are organized and related to each other for a particular electronic data interchange (EDI) transaction.

Java CAPS Object Type Definitions

In the Java CAPS, message structures are defined as Object Type Definitions (OTDs).

Each OTD consists of the following elements:

- **Physical Hierarchy** – The predefined way in which envelopes, segments, and data elements are organized to describe a particular HIPAA EDI transaction.
- **Delimiters** – The specific predefined characters used to mark the beginning and end of envelopes, segments, and data elements.
- **Properties** – The characteristics of a data element, such as the length of each element, default values, and indicators that specify attributes of a data part, for example, whether it is required, optional, or repeating.

Note – Included with the HIPAA PM product is the HIPAA OTD Library. See the *HIPAA OTD Library User's Guide* for details.

HIPAA OTD Usage

The Transaction Set structure of an invoice sent from one trading partner (TP) to another defines the header, trailer, segments, and data elements required by invoice transactions. The HIPAA OTD for a specific version includes Transaction Set structures for each of the transactions available in that version.

You can use these structures as provided, or customize them to suit your business needs. There is an OTD message structure for each HIPAA transaction.

Structure of HIPAA Envelopes

The rules for HIPAA envelope structure ensure the integrity of the data and the efficiency of the information exchange. The actual HIPAA message structure has primary levels that are hierarchical.

From highest to the lowest, they are:

- Interchange envelope
- Functional Group
- Transaction Set

A schematic structure of HIPAA envelopes is shown in Figure 2–1. Each of these levels is explained in more detail in the remainder of this section.

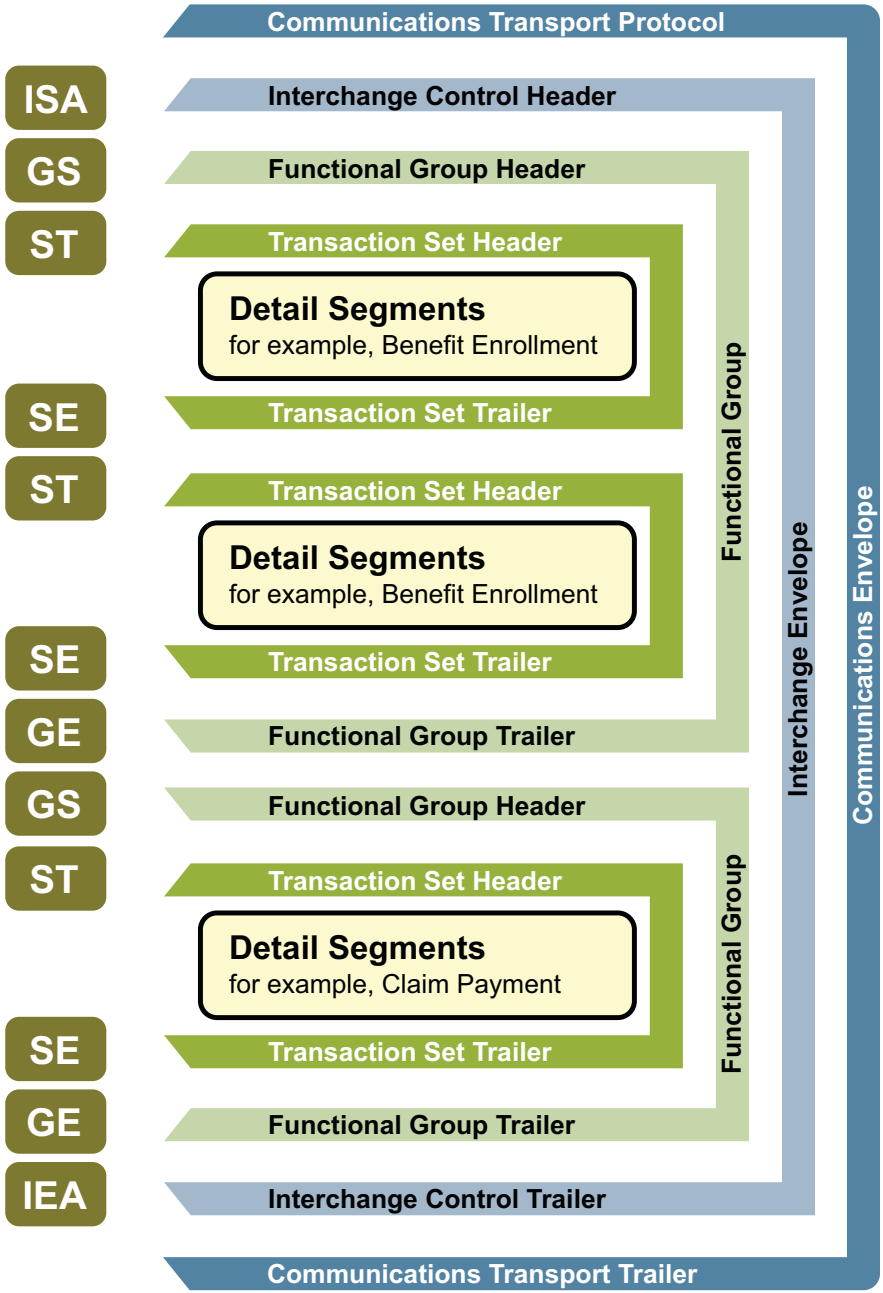

FIGURE 2–1 HIPAA Envelope Schematic Diagram

Table 1 - Header

POS #	SEG. ID	Name	REQ. DES.	MAX USE	LOOP REPEAT
010	ST	Tranasctional Set Header	M	1	
020	AK1	Functional Group Response Header	M	1	
		LOOP ID - AK2			**999999**
030	AK2	Transactional Set Response Header	O	1	
		LOOP ID - AK2/AK3			**999999**
040	AK3	Data Segment Note	O	1	
050	AK4	Data Element Note	O	99	
060	AK5	Transaction Set Response Trailer	M	1	
070	AK9	Functional Group Response Trailer	M	1	
080	SE	Transaction Set Trailer	M	1	

FIGURE 2–2 HIPAA 997 (Functional Acknowledgment) Segment Table

Figure 2–2 shows the standard segment table for an HIPAA 997 (Functional Acknowledgment) as it appears in the HIPAA standard and in most industry-specific implementation guides.

Functional Groups (GS/GE)

Functional Groups, often referred to as the "inner envelope," are made up of one or more Transaction Sets, all of the same type, which can be batched together into one transmission. The Functional Group is defined by the header and trailer segments.

The Functional Group Header (GS) segment appears at the beginning (the Functional Group Trailer, designated GE, segment appears at the end). Many Transaction Sets can be included in the Functional Group, but all transactions must be of the same type.

Within the Functional Group, each Transaction Set is assigned a functional identifier code, which is the first data element of the header segment. The Transaction Sets that constitute a specific Functional Group are identified by this functional ID code.

The GS segment contains:

- Functional ID code (the two-letter transaction code; for example, PO for an 850 Purchase Order, HS for a 270 Eligibility, Coverage, or Benefit Inquiry) to indicate the type of transaction in the Functional Group
- Identification of sender and receiver
- Control information (the Functional Group control numbers in the header and trailer segments must be identical)
- Date and time

The GE segment contains:

- Number of Transaction Sets included
- Group control number (originated and maintained by the sender)

See Figure 2–3 and Figure 2–4.

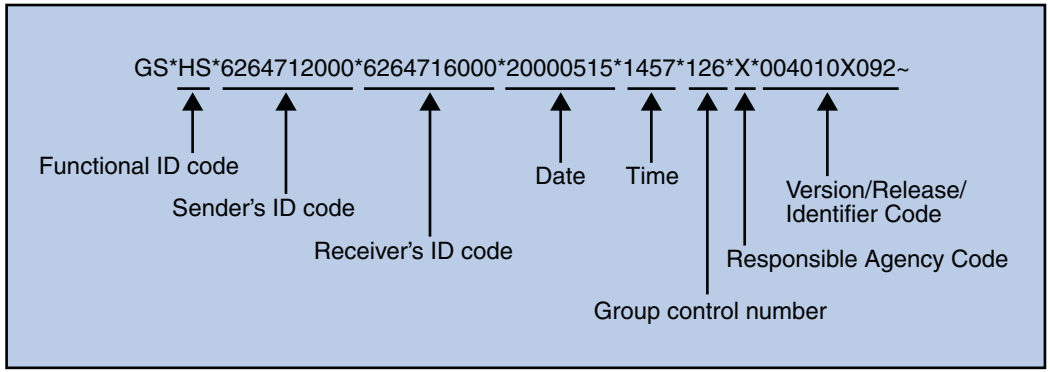

FIGURE 2–3 Example of a Functional Group Header (GS)

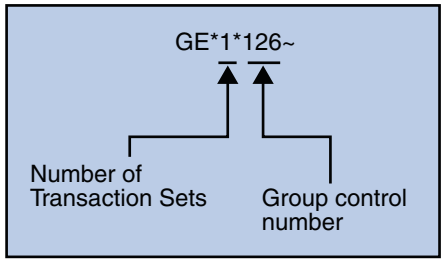

FIGURE 2–4 Example of a Functional Group Trailer (GE)

Interchange Envelopes (ISA/IEA)

The Interchange Envelope, often referred to as the "outer envelope," is the wrapper for all the data to be sent in one transmission. It can contain multiple Functional Groups. This characteristic means that transactions of different types can be included in the interchange envelope, with each type of transaction stored in a separate Functional Group.

The Interchange Envelope is defined by the header and trailer. The Interchange Control Header (ISA) appears at the beginning (the Interchange Control Trailer, designated IEA appears at the end).

As well as enveloping one or more Functional Groups, the ISA (and IEA) segments include:

- Data element separators and data segment terminator
- Identification of sender and receiver
- Control information (used to verify message was correctly received)
- Authorization and security information, if applicable

The sequence of information transmitted is:

- ISA
- Optional interchange-related control segments
- Actual message information, grouped by transaction type into Functional Groups
- IEA

See Figure 2–5 and Figure 2–6.

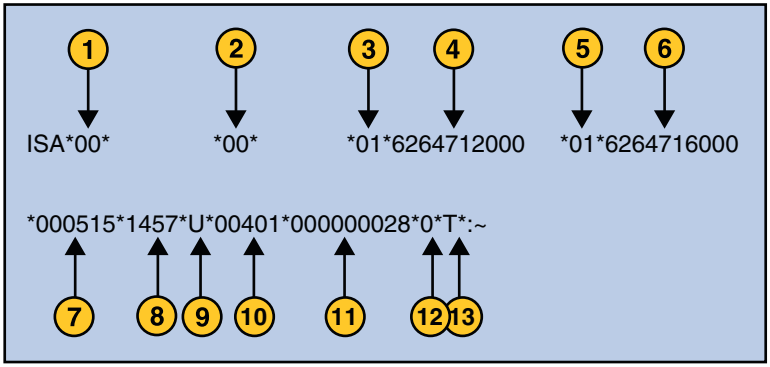

FIGURE 2–5 Example of an Interchange Header (ISA)

The following list describes the ISA segments shown in Figure 2–5:

1. Authorization Information Qualifier
2. Security Information Qualifier
3. Interchange ID Qualifier
4. Interchange Sender ID
5. Interchange ID Qualifier
6. Interchange Receiver ID
7. Date
8. Time
9. Repetition Separator
10. Interchange Control Version Number
11. Interchange Control Number
12. Acknowledgment Requested
13. Usage Indicator

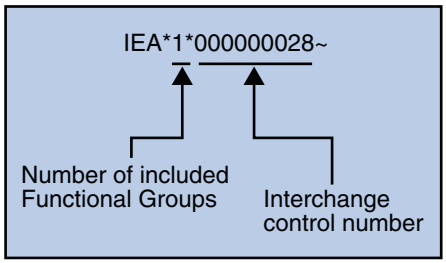

FIGURE 2–6 Example of an Interchange Trailer (IEA)

Transaction Sets (ST/SE)

Each Transaction Set also known as a transaction) contains:

- Transaction Set header (designated ST)
- Transaction Set trailer (designated SE)
- Single message, enveloped within the header and footer

A Transaction Set has a three-digit code, a text title, and a two-letter code, for example, **997, Functional Acknowledgment (FA)**.

The Transaction Set is composed of logically related pieces of information grouped into units called segments. For example, one segment used in the Transaction Set might convey the address: city, state, postal code, and other geographical information. A Transaction Set may contain multiple segments. For example, the address segment might be used repeatedly to convey multiple sets of address information.

The HIPAA standard defines the sequence of segments in the Transaction Set and also the sequence of elements within each segment. The relationship between segments and elements can be compared to the relationship between records and fields in a database environment. See Figure 2–7 and Figure 2–8.

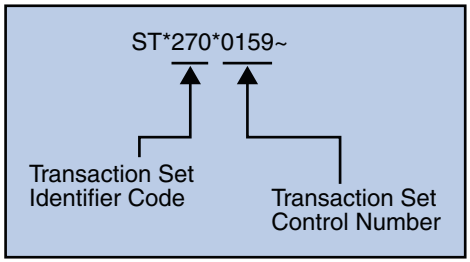

FIGURE 2–7 Example of a Transaction Set Header (ST)

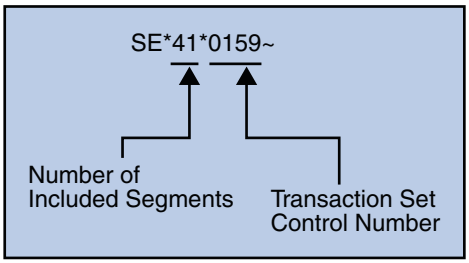

FIGURE 2–8 Example of a Transaction Set Trailer (SE)

Elements of HIPAA Envelopes

HIPAA messages are all in ASCII text, with the single exception that the BIN segment is binary.

Each HIPAA message is made up of a combination of the following elements:

- Data
- Segments
- Loops

Elements are separated by delimiters. The remainder of this section explains these elements.

Data Elements

The data element is the smallest named unit of information in the HIPAA standard. Data elements can be broken down into types. The distinction between the types is strictly a matter of how they are used.

The types are:

- **Simple**: If a data element occurs in a segment outside the defined boundaries of a composite data structure, it is called a simple data element.
- **Composite**: If a data element occurs as an ordinally positioned member of a composite data structure, it is called a composite data element. A telephone number is a simple example of a composite. It has a three-digit area code, which must precede the three-digit central office code, which must precede the final four digits.

Each data element has a unique reference number, and it also has a name, description, data type, and minimum and maximum length.

Segments

A segment is a logical grouping of data elements. In HIPAA, the same segment can be used for different purposes.

This means that a field's meaning can change based on the segment, for example:

- The NM1 segment is for *any* name (patient, provider, organization, doctor)
- The DTP segment is for *any* date (date of birth, discharge date, coverage period)

For more information on the HIPAA enveloping segments, refer to the Web sites provided under "Additional HIPAA References" on page 13.

Loops

Loops are sets of repeating ordered segments.

In HIPAA you can locate elements by specifying:

- Transaction Set ,for example, 270 or 271
- Loop, for example, "info. receiver loop"
- Occurrence of the loop
- Segment, for example, BGN
- Field number, for example, 01
- Occurrence of the segment if it is a repeating segment

Delimiters

In an HIPAA message, the various delimiters are part of the syntax, dividing up the different elements of a message. The delimiters used in a message are defined in the interchange control header, the outermost layer enveloping the message.

For this reason, there is flexibility in the delimiters that are used. No suggested delimiters are recommended as part of the HIPAA standards, but the industry-specific implementation guides do have recommended delimiters.

The default delimiters used by the HIPAA OTD Library are the same as those recommended by the industry-specific implementation guides. These delimiters are shown in Table 2–1.

TABLE 2–1 Default Delimiters in the HIPAA OTD Library

Type of Delimiter	Default Value
Segment terminator	~ (tilde)
Data element separator	* (asterisk)
Subelement (component) separator	: (colon)

Within eXchange, delimiters are specified at the enveloping level. The delimiters defined for an envelope apply to all transactions in the same business service (a predefined dialog between the two parties).

If you do not specify delimiters and do not override them in the payload transactions fed into FROMINTERNAL, eXchange expects the default delimiters shown in Table 2–1.

Note – It is important to note that errors could result if the transmitted data includes any of the characters that have been defined as delimiters. Specifically, the existence of asterisks within transmitted third-party validation data is a known issue in HIPAA and can cause problems with translation.

See "Element Separator" on page 51 for information on the ePM delimiter parameter.

Acknowledgment Types

The HIPAA protocol includes the following types of acknowledgments:

- TA1 Interchange Acknowledgment
- 997 Functional Acknowledgment

Note – See "Sample Scenario Business Description" on page 61.

TA1, Interchange Acknowledgment

The TA1 Interchange Acknowledgment verifies the interchange envelopes only. The TA1 is a single segment and is unique in the sense that this single segment is transmitted without the GS/GE envelope structures. A TA1 acknowledgment can be included in an interchange with other Functional Groups and transactions.

997, Functional Acknowledgment

The Transaction Set 997 Functional Acknowledgment includes much more information than the TA1. This Transaction Set was designed to allow TPs to establish a comprehensive control function as part of the business exchange process.

There is a one-to-one correspondence between Transaction Set 997 and a Functional Group. Segments within this Transaction Set identify whether the Functional Group was accepted or rejected. Data elements that are incorrect can also be identified.

Many EDI implementations have incorporated the acknowledgment process into all of their electronic communications. Typically, Transaction Set 997 is used as a functional acknowledgment to a Functional Group that was transmitted previously.

Note – Transaction Set 997 is the acknowledgment transaction recommended by HIPAA.

The acknowledgment of the receipt of a payment order is an important issue. Most corporate originators want to receive at least a Functional Acknowledgment (Transaction Set 997) from the beneficiary of the payment. Transaction Set 997 is created using the data about the identity and address of the originator found in the ISA and/or GS segments.

Formats: ANSI ASC X12 and XML

The HIPAA messages accept either the standard ANSI ASC X12 or XML formats as input, by default. You do not need to change the existing Business Protocols (BPs) or eGate Java Collaboration Definitions (JCDs) to specify the input format (standard data is ANSI X12 or XML).

For more information about HIPAA, see the Web sites listed under "Additional HIPAA References" on page 13.

For more information on the ASC X12 protocol, see the following Web site:
`http://www.x12.org/`

For more information on the XML messaging, see the following Web site:
`http://www.xml.com/`

HIPAA PM Overview

Because HIPAA PM integrates with eGate, eInsight, eXchange, and the HIPAA OTD Library, the product enables you to design Java CAPS Projects that process HIPAA messages. Message validation is handled through a third-party service.

For more information about eGate, eXchange, and the HIPAA OTD Library, see the corresponding user's guides.

Note – As you use this document, refer to the *eXchange Integrator User's Guide* for information relating directly to eXchange operation.

Basic Operation

HIPAA PM allows you to test and validate your HIPAA transactions by performing calls to a third-party validation service. The HIPAA PM's validation features allow you to do this operation. HIPAA PM validation supports HIPAA validation, which may consist of any certified HIPAA validation solution.

HIPAA PM and eXchange

eGate and eXchange enable you to build Java CAPS Projects that process standard B2B business protocols and enveloping protocols, such as HIPAA.

HIPAA PM works with eXchange to provide the following features during message processing:

- Message transport
- Message tracking
- Error handling

HIPAA PM and the HIPAA OTD Library

HIPAA messages within eGate are called HIPAA OTDs. The Java CAPS provides packaged HIPAA OTDs for eGate as part of the HIPAA OTD Library.

Note – For more information on these OTDs, see the *HIPAA OTD Library User's Guide*.

You can also build your own OTDs using the SEF OTD wizard supplied with Java CAPS. HIPAA PM provides packaged BP rules to handle HIPAA OTDs.

Third-party Validation

HIPAA PM allows your system to validate data using third-party services such as EDIFECS and Foresight.

When you import the `xengine.jar` and `xe_extensions.jar` files (see "Initializing and Running Enterprise Designer" on page 78) into your Logical Host directories, you enable validation through the EDIFECS XEngine.

For complete instructions on how to set up EDIFECS to validate HIPAA data, as well as how to use the EDIFECS XEngine, see the following Web site:

`http://www.edifecs.com`

From this Web site, search under EDIFECS XEngine for information on how to enable and use this feature to validate HIPAA data.

You need to create an environment variable `XEROOT`that will contain the installation path of the EDIFECS XEngine.

Note – HIPAA PM allows you to set outbound messages to be sent without Business Message Syntax validation, to speed up message processing. However, inbound message validation is always required.

To Set Up Foresight to Validate HIPAA Data

For complete instructions on how to set up Foresight to validate HIPAA data, see the following Web site:

`http://www.foresightcorp.com`

After you have installed the Foresight engine, do the following:

1. **Create a new file,`TI.csv` using the `SamplePartnerAutomation.csv` file.**

   For more information about the `SamplePartnerAutomation.csv` file, refer to the Foresight documentation.

2. **Copy the `TI.csv` file to the `HIPAAValidatorInstream/Bin` directory.**

3. **Open the `fsdir.ini` file in an editor and modify the parameter `PARTNERAUTOMATION`.**

   a. **Remove the colon that is present before the parameter `PARTNERAUTOMATION`.**

   b. **Replace the `SamplePartnerAutomation.csv` file with the `TI.csv` file.**

      ```
      PARTNERAUTOMATION="C:\ProgramFiles\HIPAA Validator Instream\Bin\TI.csv"
      ```

4. **To start the application server on UNIX, you need to set the following Environment variables:**

   a. **Add the following path to the environment variable `FSINSTREAMINI`.**

      `...`*`ForesightInstallDir`*`/Bin`

   b. **The `LIBPATH(AIX)`, `LD_LIBRARY_PATH(Sun OS)`, or `SHLIB_PATH(HP-UX)` needs to contain the value of the `FSINSTREAMINI` variable.**

How HIPAA PM Messaging Works

HIPAA PM operates using the following basic functional layers:

- **View**: eInsight provides the ability to create and view the structure of HIPAA eXchange Projects, and the eXchange Message Tracking feature allows the searching and viewing of sent and received HIPAA messages. HIPAA PM Message Tracking includes interleaved error reports to allow pinpoint tracking of system messaging errors.
- **Services Orchestration**: You use the eXchange Partner Manager (ePM) to design HIPAA Transaction Sets; then the appropriate HIPAA Projects prepare and return the interchange and functional acknowledgments (TA1 and 997) to the TP. HIPAA Projects also perform message correlation to associate business responses to the related requests. A HIPAA B2B Host Project manages and coordinates the HIPAA messaging operations.
- **Integration Services**: The HIPAA Project handles Interchange Envelope (ISA) and Functional Group (GS) enveloping from incoming messages, prepares these envelopes for outgoing messages, batches together documents to be delivered as a single transaction (ISA), and records the activity in Message Tracking. You may configure these enveloping parameters using ePM.

Key Parts of EDI Processing Logic

The key parts of EDI processing logic are listed in Table 2–2.

TABLE 2–2 Key Parts of EDI Processing

Term	Description	Language Analogy	Java CAPS Component
Structures	Format, segments, loops	Syntax rules	OTD elements and fields
Validations	Data contents “edit” rules	Semantic rules	Not supported by HIPAA PM; handled by a third-party service
Translations (also called mappings)	Reformatting or conversion	Translation	Collaborations, Java Collaboration Definitions (JCDs)
Enveloping	Header and trailer segments	Envelope for a written letter	Special “envelope” OTDs: FunctionalGroupEnv and InterchangeEnv
Acks	Acknowledgments	Return receipt	Specific acknowledgment elements in the OTD

Java CAPS uses structures, translations, enveloping, and acknowledgments, as listed in Table 2–2 to support the HIPAA standard. The remainder of this section explains these terms in greater detail.

OTD Message Structures

The HIPAA OTD Library includes pre-built OTDs for messaging in all supported HIPAA versions. These OTDs can be viewed in the eGate OTD Editor but cannot be modified.

To customize an OTD structure , for example, in order to add a segment or loop , you must first create a `.sef` file (generally using a third-party application). You then use the SEF OTD wizard to generate the appropriate OTD from a given `.sef` file.

Translations, Enveloping, and Acknowledgments

Within each HIPAA OTD are Java methods and Java bean nodes for handling translations, enveloping, and acknowledgments. The marshal and unmarshal methods of the two *envelope* OTDs handle enveloping and de-enveloping.

No prebuilt translations are supplied with the HIPAA OTD Library. You build data translations with an eGate Enterprise Designer user interface called the Java Collaboration Editor (JCE).

Note – In eGate, HIPAA translations are called Java Collaboration Definitions (JCDs).

You may also construct eGate XSLT Collaborations and/or eInsight BPs to perform translations.

Message Information Levels

The levels of information that guide the final format of a specific transaction are:

- **HIPAA Protocol** : The HIPAA Act mandates a standard structure for each HIPAA TP transaction. Specifically, since HIPAA regulations are law, it is important to follow the guidelines for these transactions as strictly as possible.
- **TP Agreements** : It is normal for TPs to have individual agreements that supplement the standard guidelines. The specific processing of the transactions in each TP's individual system can vary from one site to another. As a result, additional documentation providing information about the differences is helpful to the site's TPs and simplifies implementation. For example, although a certain code might be valid in an implementation guide, a specific TP might not use that code in transactions. In such a case, it is important to include that information in the TP agreement.

Using the SEF Wizard

You can use this product with custom SEF OTDs built with the SEF OTD wizard. The wizard supports the most current SEF versions.

The SEF OTD wizard does *not* handle the following information and sections:

- In the .SEMREFS section, semantic rules with its type of the "exit routine" are ignored as per SEF specification. An exit routine specifies an external routine (such as a COM-enabled server program supporting OLE automation) to run for translators or EDI data analyzers.
- The .TEXT sections (including subsections such as .TEXT,SETS, .TEXT,SEGS, .TEXT,COMS, and .TEXT,ELMS) are ignored, because these sections store information about changes in a standard's text, such as notes, comments, names, purposes, descriptions, titles, semantic notes, explanations, and definitions.

About eXchange Integrator

eXchange Integrator provides an open Business Protocol framework to support standard EDI and B2B protocols, as well as packaging protocols. The eXchange product supports existing standard protocols, using an extensive set of prebuilt eInsight Business Processes (BPs). It also provides the tools and framework to create and adopt new protocols and to build custom BPs.

B2B modeling semantics are exposed so that eInsight Business Rules can be added and tailored to address the particular needs of providing eBusiness solutions. The tight integration with the rest of Java CAPS provides validation, logging, and reporting capabilities. Because each logical step within any Business Rule is accessible anywhere along the entire eInsight BP, the design tools provide complete end-to-end visibility.

Note – For a complete explanation of eXchange and eInsight, as well as their operation, see the *eXchange Integrator User's Guide* and *eInsight Business Process Manager User's Guide*.

Understanding BPs

An eInsight BP is a collection of actions or operations that take place in your company, revolving around a specific business practice. These processes can involve a variety of participants and may include internal and external computer systems or employees.

In eXchange, you create a graphical representation of a business process called a BP model. When you are using the sample for a PM's implementation scenario, the system uses the BPs necessary for scenario's operation. The BPs specific to the sample scenario provided with the product have already been created for this scenario.

Trading Partner Overview

The architecture of eXchange centers around the concept of sending and receiving messages relative to one or more TPs. Each TP that you import or create and then configure corresponds to one of your business trading partners.

These TPs contain configurable transaction profiles for each individual TP relationship. You can configure TPs with Transaction Profiles and Schedules, within ePM, for use by run-time components.

Each Transaction Profile specifies which one or more BPs to use for the current transaction, where and how to receive inbound messages, how to configure and secure messages in their channels, and how and where to deliver outbound messages.

Process Overview

Using eXchange to create a business solution consists of the following phases:

- Design phase within Enterprise Designer
- Configuration/design phase within ePM
- Run-time phase

eXchange Partner Manager

ePM is a feature of eXchange you can use as a tool that allows you to configure eXchange for use with any of your PMs. You must set specific parameter values within ePM to ensure the correct operation of your Projects, for each protocol. This guide explains how to use and configure ePM, to set parameters relevant to this guide's PM.

For more information on how to use ePM, see the *eXchange Integrator User's Guide*.

B2B Suite, eXchange, and Java CAPS

eXchange is one of the products that make up the B2B Suite within Java CAPS. The B2B Suite products, including eXchange, provide a Web-based TP configuration and management solution for automating and securely managing business partner relationships. The products also facilitate real-time interaction between the enterprise and its TPs, suppliers, and customers.

As a part of Java CAPS, the B2B Suite provides the following benefits and features:

- B2B services using eXchange
- Protocol managing, specifically by the PMs
- Protocol formats contained in the OTD Libraries
- Trading partner management facility, that is, the ePM interface
- Archiving tool, the Message Tracking feature

The B2B Suite is tightly integrated with Java CAPS and runs as a group of components within Java CAPS environment. Figure 2–9 illustrates how the B2B Suite, eXchange, and other Java CAPS components work together, including eInsight.

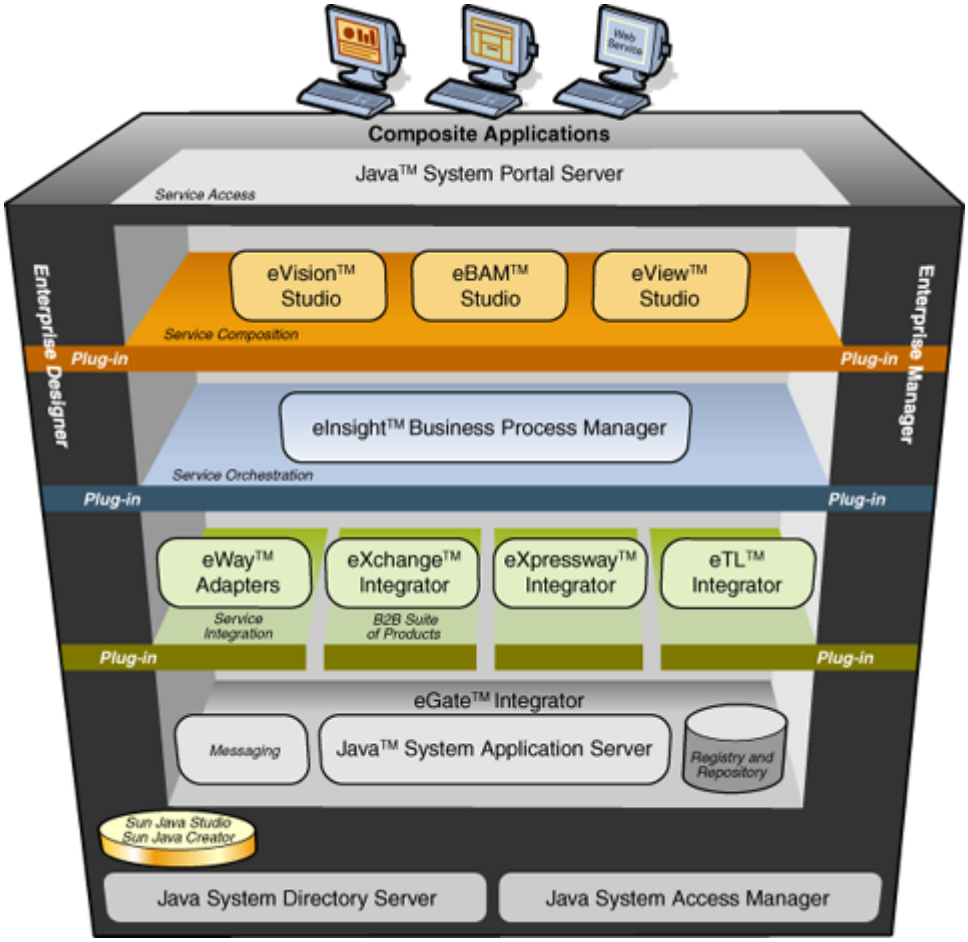

FIGURE 2–9 Architecture of Java CAPS product stack

◆ ◆ ◆ CHAPTER 3

Installing HIPAA PM

This chapter explains how to install HIPAA PM, as well as pre- and post-installation procedures and contains the following sections:

Supported Operating Systems and Prerequisites

This section describes the HIPAA PM supported operating systems and the prerequisites you need for its use.

Supported Operating Systems

HIPAA PM supports all operating systems supported by eGate and eXchange versions compliant with this release. See the *eXchange Integrator User's Guide* for a complete list.

System Prerequisites

HIPAA PM requires the following Sun SeeBeyond products (compliant with this release) for its correct operation:

- Core Products
  - eGate
  - eXchange
  - eInsight
  - SEF OTD Wizard
- eWays
  - Batch eWay

- File eWay
- HTTP eWay
- LDAP eWay
- Oracle eWay

- OTD Library
  - HIPAA OTD Library

See the eXchange Readme file for a list of the Sun SeeBeyond products compliant with this release.

Third-party Service Requirements

HIPAA PM requires the EDIFECS third-party service to perform required message validations. Contact EDIFECS for instructions on how to interface with their service. For more information, see "Third-party Validation" on page 26.

Getting Started With Installation

Open and review the Readme file for Java CAPS to gain current information you may need, for example for eGate or eInsight, before installing HIPAA PM. You can find this file in the root directory of Java CAPS installation's Repository CD-ROM.

Also, HIPAA PM has its own **HIPAA_Manager_Readme.txt** file that contains additional information specific to this application, including required ESRs.

Note – See the *SeeBeyond Java CAPS Installation Guide* for details on how to obtain the Readme and documentation files.

This version of HIPAA PM is compatible with Java CAPS version 5.1.2 (eGate and eInsight).

Configuring eGate Projects for Large Messages

If an eGate Project uses Sun SeeBeyond JMS (Java Messaging Service) IQ Manager and is estimated to process messages or transactions over 8 MB for Windows, or 16 MB for UNIX, you must increase the **Segment Size** property of JMS IQ Manager as explained in the *eGate Integrator JMS Reference Guide*.

Installing HIPAA PM Product Files

During the Java CAPS installation operation, use Enterprise Manager, a Web-based application, to select and upload HIPAA PM and add-on application `.sar` files from the Java CAPS installation CD-ROM to the Repository.

When the Repository is running on a UNIX operating system, you must still install HIPAA PM using Enterprise Manager and Microsoft Internet Explorer on a Windows computer connected to the Repository server.

Basic Installation Procedures

Follow the general instructions for installing Java CAPS, which you can find in the *Java CAPS Installation Guide*. You must begin by installing eGate. For more information, see the *eGate Integrator System Administration Guide*.

In this document, the examples and illustrations show a Repository named **repB2B**, installed under the base installation directory and using the default ports (12000-12009).

▼ To Create HIPAA Tables

1. **In Enterprise Explorer, in the project tree, expand the following folders: Sun SeeBeyond ⇒ eXchange ⇒ Protocol Manager ⇒ HIPAA Manager ⇒ Download Database Scripts**

2. **Right-click `hipaa_oracle510.zip` and, on the popup context menu, click Export; then use the Save dialog box to save the file to a local directory.**

3. **Extract the files in `hipaa_oracle510.zip` into this local directory, yielding:**

   - `create_hipaa_tables.cmd`
   - `create_hipaa_tables.sql`
   - `setenv.cmd`

4. **To edit the `setenv.cmd`, open a command prompt and change directories to the local directory where you saved the scripts .**

5. **Use a text editor to edit the as-supplied version of `setenv.cmd`:**

```
@REM SET YOUR DATABASE CONNECTION INFORMATION HERE
*
echo * This file should be edited to use appropriate
echo * database connection settings. *
echo * SETENV.CMD
@REM TNS_NAME
@set TNS_NAME=< TNS NAME >
```

```
@REM ORACLE_SID
@set ORACLE_SID=< SID >
@REM Oracle system login password
@set SYSTEMPWD=< PWD >
@set USERID=ex_admin
@set USERPWD=ex_admin
```

6 **Supply the appropriate values for** `TNS_NAME`**,** `ORACLE_SID`**, and** `SYSTEMPWD`**. For example:**

```
@set TNS_NAME=eXchange_myOracleHostname
@set ORACLE_SID=ORCL
@set SYSTEMPWD=manager
@set USERID=ex_admin
@set USERPWD=ex_admin
```

7 **Open a command prompt and change directories to the local directory where you saved the .cmd scripts in the previous procedure.**

8 **Enter the following command:**

```
create_hipaa_tables.cmd
```

The script starts SQL*Plus, invokes an SQL script to create HIPAA tables.

Note – Create and configure the eXchange database using the `Oracle510.zip` file. For complete information on how to perform this and other eXchange setup operations, see the *eXchange Integrator User's Guide*. You need to create HIPAA specific database tables after the eXchange database is created.

▼ To Install the Repository and Product `.sar` files

1 **Install the Repository by running either of the following scripts:**

- **(for Windows)**

```
... \Repository\install.bat
```

- **(for UNIX)**

```
sh ... /Repository/install.sh
```

2 **Upon completion of the installation, start the Repository by running the following script:**

```
C:\ ... repository\startserver.bat
```

3 **Start a new browser session and point your browser at this URL:**

```
http://localhost:12000
```

4 **In the Java CAPS Login window of the Java CAPS Installer, supply the following values:**

- **username**: Administrator
- **password**: STC

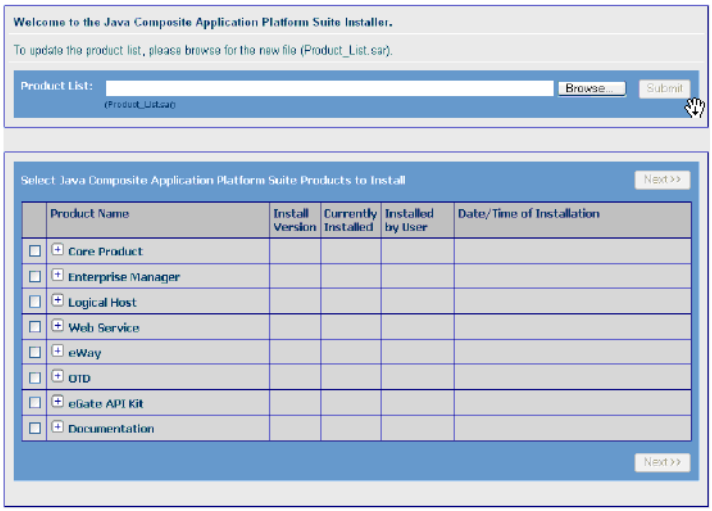

FIGURE 3–1 Java Caps Installer

5 **Use the Java CAPS Installer's Administration tab to install the following file:** `eGate.sar`

This installation may require approximately 15 minutes.

Note – Ensure that, to duplicate the sample shown in this document, you have named your Repository `repB2B`.

---

6 **Click the link to install additional products, and then browse to the current product list and submit it:**

`Product_List.sar`

7 **Stage and install the following files:**

- From the Core Product category:

  `eInsight.sar`

- From the Enterprise Manager category:

  `...` *yourOS-type*`\Enterprise_Manager-`*yourOS-Platform*`.sar`

8 **Stage and install the following product file, from the Logical Host category:**

`...` *yourOS-type*`\logicalhost-`*yourOS-platform*`.sar`

9 **Stage and install the following product files, from the eWay category:**

- `BatcheWay.sar`
- `FileeWay.sar`
- `HTTPeWay.sar`
- `LDAPeWay.sar`
- `OracleeWay.sar`

10 **Stage and install the following product files from the Core Product category:**

- `eXchange.sar`
- `SEF_OTD_Wizard.sar`

Note – You must finish installing `eXchange.sar` before you start to install `HIPAA_Manager.sar`.

---

11 **Stage and install the following product file, from the OTD category:**

`HIPAA_2000_Addenda_OTD.sar`

Note – You must finish installing this file before you start to install `HIPAA_Manager.sar`.

---

12 **Stage and install the following product file, from the Core Product category:**

`HIPAA_Manager.sar`

13 **Finally, stage and install the following product file, from the OTD category:**

`HIPAA_2000_Addenda_OTD_ExternalUniqueID_BP.sar`

After You Install

Once HIPAA PM is installed and configured, it must then operate in conjunction with an eGate Project before it can perform its intended functions. You must create these Projects specifically for HIPAA PM or import one or more HIPAA PM Projects.

See the *eXchange Integrator User's Guide* and *eGate Integrator User's Guide* for detailed information on incorporating these types of Projects into eGate. See Chapter 5, "Quick Start for HIPAA PM," and Chapter 6, "HIPAA PM Sample Scenario Tutorial," for information on a sample business scenario with Projects already created, using eXchange and HIPAA PM.

◆ ◆ ◆ CHAPTER 4

Configuring HIPAA PM

This chapter explains how to configure eXchange Partner Manager (ePM) parameters for use with HIPAA PM and HIPAA and contains the following topics:

Configuring eXchange Partner Manager: Overview

This chapter explains the configuration parameters required for HIPAA PM Projects and their operation with HIPAA and other Java CAPS applications. You can configure these parameter values for HIPAA PM using the eXchange ePM user interface.

Note – For more information on how to do these operations in ePM, including default values for general eXchange parameters and how to override them, see the *eXchange Integrator User's Guide*.

---

ePM, B2B Hosts, and Trading Partners

You may use ePM to set up and configure HIPAA PM parameters at the B2B Host configuration level for the Projects in a business scenario. In ePM, B2B Host components can be created from scratch or imported. These components derive their default parameter properties from the B2B Host you built in Enterprise Designer, which contains HIPAA PM configuration parameters.

eXchange ePM

The eXchange ePM interface allows you to set essential parameter properties for your HIPAA PM eXchange Projects. This tool also allows you to configure the specific business and messaging functions you want implemented by your B2B Hosts and Trading Partners (TPs).

Ensuring that you have configured the appropriate values in ePM allows the B2B Hosts and TPs you configure to operate seamlessly with eXchange, HIPAA PM, and HIPAA within your B2B scenario. Also, TPs in ePM can be either created from scratch or imported.

For more information on B2B Hosts and TPs, see "Constructing the B2B Host Project" on page 93 and "Importing and Configuring Components in ePM" on page 102.

Using ePM: Overview

In eXchange, each TP contains information identifying the values for using HIPAA PM with eXchange, as well as communication with the HIPAA B2B Host and TP delivery and transport information used for sending and receiving B2B information.

Categories of Configurable Properties

There are three categories of configurable parameter properties in ePM, as follows:

- Business Protocols
- Delivery Protocols
- Transports

In general, you may use parameters under Business Protocols to configure data payload-related operations within your business. Also generally, parameters under Delivery Protocols determine data payload-unrelated messaging operations. Parameters under Transports are directly related to eXchange and remain the same regardless of which PM you are using.

Note – See the *eXchange Integrator User's Guide* for more information.

You may locate the current B2B Host or TP in **ePM Explorer**, by clicking the **B2B Host Configuration** or **Trading Partner Configuration** tab. The B2B Host acts as a top-level "parent" component that supplies all default parameter properties to the components under it, including the TP. These components include Action Groups and Transaction Profiles.

Business Actions

You define Business Actions within the B2B Host, as constructed in Enterprise Designer. Business Actions are already a part of the B2B Host in ePM when you begin to configure in ePM. They are the message type, inbound or outbound, for example, **270 FromPartner**.

Action Groups

Under B2B Hosts, you may create Action Groups. They function as "child" components that inherit parameter properties from their "parent" B2B Host. By associating one or more Action Groups with a TP, you define the TP's general operation.

In terms of usage, for example, you might want to place all of your Transaction Profiles for purchase order requests and responses in one Action Group and give it a name that represents its function.

Note – You cannot create an Action Group within a TP.

Transaction Profiles

Each Transaction Profile enables a specific messaging function and is associated with a B2B Host. For example, you may create Transaction Profiles at the B2B Host level (in the **B2B Host Configuration** tab in ePM), whose parameter values are inherited at the TP level (in the **Trading Partner Configuration** tab in ePM).

A Transaction Profile consists of a Business Protocol Action Group, a Delivery Protocol Action Group (if necessary), and a Transport. Therefore, a given Transaction Profile inherits parameter values from each of its constituent Action Group and Transport components.

At the TP level, a B2B Host Transaction Profile may be used as a part of the configuration of a TP component, that is, one of the TP's Transaction Profiles. In these cases, the TP is said to "inherit" the configuration values of the B2B Host Transaction Profile it is using.

Defaults and Overrides

ePM allows you to override the default parameter properties at any "parent" or "child" component level. Overrides inherit from "parent" to "child" components. Default overrides cascade from B2B Hosts to TPs. You can also configure specific overrides for individual TPs.

Note – For information on Lookup parameters and how they operate in ePM, including how they are inherited and overridden, see the *eXchange Integrator User's Guide*.

The current TP configuration inherits the current B2B Host configuration. Additionally, ePM allows you to override any inherited parameter values at this level or at any lower level in the TP, if necessary (see Table 4–1). For example, a TP's Action Group's overrides are inherited from the current B2B Host's Action Groups.

Review the previous example of the B2B Host Transaction Profile used as a part of the TP configuration. Since this Transaction Profile also belongs to the current TP, the inherited parameter values may be overridden at this level, effectively "customizing" the Transaction Profile for the TP.

Inheritance and Override Hierarchy

Table 4–1 illustrates this ePM hierarchy of default override inheritance. Keep in mind that parameter categories only inherit from the same categories, for example, B2B Host Action Group Business Protocols from TP Action Group Business Protocols, and so on.

TABLE 4–1 ePM Override Inheritance Hierarchy

Major Component Being Configured	Row in This Table	Selected in ePM Explorer	Parameter Categories in ePM Canvas	Parameter Values Inherit Overrides
B2B Host component: May have one or more Action Groups, which in turn may have one or more Transaction Profiles.	**Row 1**	B2B Host under B2B Host Configuration tab	Business Protocols	Top level; no inheritance
			Delivery Protocols	
			Transports	
	Row 2	Action Group; "child" component relation to "parent" B2B Host above	Business Protocols	From B2B Host Configuration tab values set on ePM canvas
			Delivery Protocols	
	Row 3	Transaction Profile; "child" component relation to "parent" Action Group (and "grandparent" B2B Host) above	Business Protocols	From B2B Host ⇒ Action Group configuration values set on ePM canvas
			Delivery Protocols	
			Transports	
Trading Partner (TP) component: May have one or more Action Groups, which in turn may have one or more Transaction Profiles.	**Row 4**	TP under Trading Partner Configuration tab	Business Protocols	This Row 4 inherits from Row 1 above
			Delivery Protocols	
			Transports	
	Row 5	TP Action Group; same as Row 2 above (cannot be created at this level)	Business Protocols	This Row 5 inherits from Row 2 above
			Delivery Protocols	

TABLE 4–1 ePM Override Inheritance Hierarchy *(Continued)*

Major Component Being Configured	Row in This Table	Selected in ePM Explorer	Parameter Categories in ePM Canvas	Parameter Values Inherit Overrides
	Row 6	Transaction Profile	Business Protocols	This Row 6 inherits from Row 3 above
			Delivery Protocols	
			Transports	

It is recommended that you set your necessary configurations at the "highest" level possible, according to the hierarchy shown in the previous table. For example at the B2B Host Business Protocol level or at the TP Business Protocol level. See the sample scenario ePM configuration for an example of these recommended configuration practices.

Note – For more information about parameter override inheritance in ePM, see the *eXchange Integrator User's Guide*.

Configuring B2B Hosts and TPs in ePM

Before you can use a TP, you must configure its associated parameters specifically for eXchange, HIPAA PM, and your B2B operation.

Tabs on ePM Canvas

You can set certain parameters in the following tabs in ePM that will be used by the HIPAA PM Projects at runtime:

- **B2B Host Configuration**
- **Trading Partner Configuration**

These tabs offer you the following sets of properties in the Host Explorer tree in the left column:

- **Business Protocols**
- **Delivery Protocols**
- **Transports**
- **Transaction Profiles**
- **Private Keys**
- **Contacts**
- **Schedules**

Configuration parameters for your HIPAA PM Projects are located under the **Business Protocols**, **Delivery Protocols**, and **Transports** categories of properties. See "Categories of Configurable Properties" on page 40 for a description of these categories.

Parameter Types

Each set of ePM parameters contains the following parameter types:

- General eXchange parameters common to all PMs, for example, Transports
- HIPAA PM-specific parameters present only for this PM

Additional Information

This document contains a sample implementation scenario with specific ePM settings configured. You may refer to this sample scenario for ePM implementation examples.

The rest of this chapter explains the available parameters for HIPAA PM configuration and how to set them.

Configuring HIPAA PM ePM Parameters

This section explains how to configure HIPAA PM-specific parameter values in ePM.

Configuring ePM: ToPartner and FromPartner Messaging Model

The following list explains the outbound and inbound messaging model used for Environments and TPs during ePM configuration:

- When you are configuring ePM for a component related to the current TP's Environment, you must take the viewpoint of that Environment.

  For example, Company A is the current TP with its own Environment. You are configuring a component related to Company A's Environment **envA**. Therefore, in terms of the companies, **ToPartner** means from Company A (outbound from **envA**) and **FromPartner**, to Company A (inbound to **envA**).
- Following the same model, when you are configuring ePM for a component related to a *different* TP's Environment, you must take the viewpoint of *that* Environment.

  For example, Company B is a TP with an Environment outside of Company B. You are configuring a component related to Company B's Environment **envB**. Therefore, in terms of the companies, **ToPartner** means from Company B (outbound from **envB**) and **FromPartner**, to Company B (inbound to **envB**).
- Therefore, if TPs in the previous examples are named as follows:
  - **tpB** is Company A's TP.
  - **tpA** is Company B's TP.

  The following relationship holds true:

- **tpA** is the TP for **envB**.
- **tpB** is the TP for **envA**.

HIPAA PM-specific Parameter Types

HIPAA PM-specific parameters are of two basic types as explained under:

- "Interchange Envelope Parameters" on page 45
- "Functional Group Parameters" on page 51

Note – When ePM displays both sets of parameters in the previous list, parameters appear, which are generic to eXchange and are not explained in this chapter. See the *eXchange Integrator User's Guide* for details on these parameters.

For additional information on how to configure ePM parameters, see "Importing and Configuring Components in ePM" on page 102, as well as the *eXchange Integrator User's Guide*.

Interchange Envelope Parameters

This section explains how to configure Interchange Envelope (outer envelope or ISA) ePM parameters for HIPAA PM. Figure 6–12 shows an ePM example with these parameters displayed.

This section describes the following parameters:

ISA01 Author Info Qual

Description

Allows you to enter a value representing the code used to identify the type of information in the Authorization Information; required.

Required Values

The appropriate valid integer that represents the Authorization Information.

Default

None

ISA02 Author Information

Description

Allows you to enter a value representing the information used for additional identification or authorization of the interchange sender or the data in the interchange. The type of information is set by the Authorization Information Qualifier (ISA01).

Required Values

The appropriate valid integer that represents the Author Information.

Default

None

ISA03 Sec Info Qual

Description

Allows you to enter a value representing the code used to identify the type of information in the Security Information; required.

Required Values

The appropriate valid integer that represents the Security Information type.

Default

None

ISA04 Security Information

Description

Allows you to enter a value representing security information about the interchange sender or the data in the interchange. The type of information is set by the Security Information Qualifier (ISA03) value.

Required Values

The appropriate valid integer that represents the Security Information.

Default

None

ISA05 IC Sender ID Qual

Description

Allows you to enter a value representing the qualifier used to designate the system/method of information code (IC) structure employed to designate the sender ID element being qualified; required

Required Values

The appropriate valid integer that represents the IC sender ID qualifier.

Default

None

ISA06 Interchange Sender ID

Description

Allows you to enter a value representing the IC published by the sender for other parties to use as the receiver ID to route data to them. The sender always codes this value for the sender ID element; required.

Required Values

The appropriate valid integer that represents the interchange sender ID.

Default

None

ISA07 IC Rcvr ID Qual

Description

Allows you to enter a value representing the qualifier used to designate the system/method of IC structure used to designate the receiver ID element being qualified; required.

Required Values

The appropriate valid integer that represents the IC receiver ID qualifier.

Default

None

ISA08 Interchange Rcvr ID

Description

Allows you to enter a value representing the IC published by the receiver of the data. When you are sending, this value is used by the sender as their sending ID, thus other parties sending to them use this as a receiving ID to route data to them; required.

Required Values

The appropriate valid integer that represents the interchange receiver ID.

Default

None

ISA11 IC Control Standard Identifier

Description

Allows you to enter a value representing the IC used to identify the agency responsible for the control standard used by the message that is enclosed by the current interchange header and trailer; required.

Required Values

The appropriate valid integer that represents the IC control standard identifier.

Default

U

ISA12 IC Version Number

Description

Allows you to enter a value representing the current IC version number. This number covers all the current interchange control segments; required.

Required Values

The appropriate valid integer that represents the current IC version number.

Default

00401

ISA13 IC Control Number

Description

Allows you to enter a value representing the data interchange IC control number. This value is a setting that starts calculating the unique identifier for outbound messages. The identifier increments by 1 from this number, for each additional message; required.

Required Values

The appropriate valid integer that represents the IC control number.

Default

0

ISA14 Acknowledgment Requested

Description

Allows you to enter a value representing the code sent by the sender to request an interchange acknowledgment (TA1); required.

Required Values

The appropriate valid integer that represents the acknowledgment code.

Default

1

ISA15 Usage Indicator

Description

Allows you to enter a value representing the code used to indicate whether data enclosed by the current interchange envelope is for testing, production, or information only; required.

Required Values

P, **T**, or **I**.

Default

P

ISA16 Comp Elem Sep

Description

Allows you to enter a value that changes the component element default delimiter.

The data element type is not applicable. The component element separator is a delimiter and not a data element. This field provides the delimiter used to separate component data elements within a composite data structure. This value must be different from the data element separator and the segment terminator.

Required Values

Enter the appropriate delimiter override character.

If you use nondefault delimiters (for example, if you use "!" for segment terminator in v4060), you must ensure that your business rules manually pass the nondefault delimiters into the ExStdEvent/PayloadSection/Envelopes/BusinessProtocol/ location, that is, pass the ISA into .../Batch/Header, the IEA into .../Batch/Trailer, the GS into .../Group/Header, and the GE into .../Group/Trailer.

To use a control character as a delimiter, pass the escaped Unicode UTF-16 representation of the character (**\uXXXX**). For example, if you wanted to use a carriage return (ASCII **0x0d**) as a delimiter, you would pass the string \u000d.

Default

Colon (:) character

Segment Terminator

Description

Allows you to change the segment terminator default delimiter. See "ISA16 Comp Elem Sep" on page 50 for more details.

Required Values

Enter the delimiter override character.

Default

Tilde (~) character

Element Separator

Description

Allows you to change the element separator default delimiter. See "ISA16 Comp Elem Sep" on page 50 for more details.

Note – XML reserved characters, for example &, <, or >, cannot be used as delimiters. See the appropriate XML information source for a complete list of these characters.

Required Values

Enter the delimiter override character.

Default

Asterisk (*) character

Functional Group Parameters

This section explains how to configure Functional Group (inner envelope or GS) ePM parameters for HIPAA PM. Figure 6–13 shows an ePM example with these parameters displayed. This section contains the following parameters:

GS01 Functional ID Code

Description

Allows you to set a value to match the Group Name attribute of this business action, set in the B2B Host's Business Service; required.

Required Values

For example, a Group Name of "HS" is for a 270 action and "HB" for a 271 action.

Default

None (depends on the current business action)

GS02 Application Sender Code

Description

Allows you to enter a value representing the code identifying the party sending a message transmission. These codes are predefined and agreed upon by the TPs; required

Required Values

The appropriate valid integer that represents the application sender code.

Default

None

GS03 Application Rcvr Code

Description

Allows you to enter a value representing the code identifying the party receiving a message transmission. These codes are predefined and agreed upon by the TPs; required.

Required Values

The appropriate valid integer that represents the application sender code.

Default

None

GS04 Date Format

Description

Allows you to set the date structure for this transaction set, in a format specified under "Required Values;" required.

Required Values

CCYYMMDD or **CCYYYYMMDD**; choose from the list to use a four-digit or two-digit year format, for example:

- 20041201 = December 1, 2004
- 050112 = January 12, 2004

Default

CCYYMMDD

GS05 Time Format

Description

Allows you to set the time structure for this transaction set, in a format specified under "Required Values;" required.

Required Values

HHMM, **HHMMSS**, **HHMMSSD**, or **HHMMSSDD**.

Choose from the list to specify seconds and degrees of accuracy, for example:

- 2359 = 11:59PM
- 235959 = 11:59:59PM
- 23595999 = 11:59:59.99PM

The time is expressed in 24-hour (military) clock time as follows: HHMM, or HHMMSS, or HHMMSSD, or HHMMSSDD, where H = hours (00-23), M = minutes (00-59), S = integer seconds (00-59); and DD = decimal seconds; decimal seconds are expressed as follows: D = tenths (0-9) and DD = hundredths (00-99).

Default

HHMM

GS06 Group Control Num

Description

Allows you to enter the group control number assigned and maintained by the sender.

Required Values

The appropriate valid integer that represents the group control number.

Default

0

GS07 Resp Agency Code

Description

Allows you to enter a value representing the code used in conjunction with data element (DE) 480 used to identify the issuer of the current HIPAA standard; required.

Required Values

The appropriate correct transaction set code (X is recommended, but you may have to use others, for example, T, as required by the current HIPAA standard being used.

Default

X

GS08 Vers/Rel/Indust ID Code

Description

Allows you to enter a value representing the code indicating the HIPAA version, release, subrelease, and industry identifier of the EDI standard being used, including the GS and GE segments; required.

Required Values

If the responsible agency code under the GS07 segment is X (recommended), enter values as follows in the appropriate DE 480 positions:

- 1 through 3 = the current version number
- 4 through 6 = the release and subrelease levels of the current version
- 7 through 12 = the current industry or trade association identifiers (optionally assigned by the user)

If code entered for the GS07 segment is different, for example, T, then other formats are allowed, as required by the current HIPAA standard being used.

Default

00401X091

Starting Control Number

Description

Allows you to set the group control number that starts calculating the unique identifier for groups. The identifier increments by 1 from this number, for each additional group; required.

Required Values

The appropriate integer.

Default

0

Validation URL

Description

Allows you to enter the URL for the external third-party validation server.

Required Values

A valid URL allowing access to the external third-party validation server.

Default

None

Use Functional Ack from Validation Service

Description

Allows you to specify whether to use the functional acknowledgment generated by the external third-party validation server; required.

Required Values

Select **true** or **false**.

Default

false

Save Report to Files

Description

Allows you to specify whether to save interleaved error reports to text files. If you set this parameter to **false**, these error reports persist *only* in Message Tracking; required.

Required Values

Select **true** or **false**.

Default

false

Report File Directory

Description

If you do save interleaved error reports to text files (**Save Report to Files** is set to **true**), allows you to specify the directory path location where you want these error report files to be saved.

Required Values

A valid directory path location accessible to eXchange.

Default

None

Unique ID Source

Description

Allows you to select whether to select third-party message validation is based on algorithms or multiple message responses.

Validation, the default option, assigns unique IDs to incoming transaction sets based on an algorithm embedded in validation routines (externally assigned). **Internal** assignment supports environments where multiple valid responses to a single unique ID are permissible, and an internally assigned ID is necessary; required.

Required Values

Select **Validation** or **Internal**.

Default

Validation

Note – See Appendix A, "Externally Assigned Unique IDs" for more information on externally assigned unique IDs.

◆ ◆ ◆ CHAPTER 5

Quick Start for HIPAA PM

HIPAA PM comes with a sample implementation scenario that includes Projects, B2B Hosts, TPs, and data files. This chapter provides basic overview and "quick-start" procedures. Use this chapter as a HIPAA PM setup overview and/or a quick way to get started, using the sample scenario. This chapter contains the following sections:

Using the Quick Start Procedures

This chapter provides an overview of the HIPAA PM sample implementation scenario and basic procedures that describe how to import the necessary files, then efficiently set up, run, and monitor the business scenario. The remainder of this section explains the purpose and content of this chapter in greater detail.

Quick Start, Tutorial, or Both?

The HIPAA PM product includes a complete sample implementation, included in the **HIPAA_ManagerDocs.sar** file, that allows you to see the end results without having to go through all the design steps.

If you import and set up this sample scenario, as described in this chapter, you can see run-time results quickly without having to read detailed instructions.

The tutorial in Chapter 6, "HIPAA PM Sample Scenario Tutorial," on the other hand, provides a detailed hands-on guide to creating all the sample components, including some procedures that are not specific to HIPAA PM. This chapter gives detailed, instructional procedures and more specific examples.

Table 5–1 compares the purposes and tasks of the two approaches.

TABLE 5–1 Comparing Quick Start and Tutorial

Approach	Purpose	Tasks
Quick Start	This "load and go" method provides the quickest route to seeing HIPAA PM in action with eXchange.	Import the sample Projects; create the DPs and build/deploy the Projects; view initial results; run the sample scenario; experiment with passing and monitoring message data.
Tutorial:	This "up close and detailed" method provides complete steps for creating, configuring, and monitoring the working HIPAA PM business scenario provided in the sample.	Create the necessary Environments and Projects; add and configure all components to be used (for example, OTDs, HIPAA PM components, BPs, and Connectivity Maps), build/deploy the Projects; view initial results; experiment with passing and monitoring message data.

If you use either the quick-start or the tutorial approach, do the procedures contained in this chapter *first*. In this way, you can use this chapter as a general guide and reference to gain essential background knowledge, before you begin the tutorial in Chapter 6, "HIPAA PM Sample Scenario Tutorial."

Overview of Basic Setup Steps

The basic setup steps, after installation, for setting up, running, and monitoring the sample implementation scenario provided in this chapter are:

- "Getting Started" on page 62
- "Constructing the Environments" on page 65
- "Using Deployment Profiles" on page 66
- "Importing Files for ePM" on page 68

For complete information on how to use eXchange, see the *eXchange Integrator User's Guide*.

Atlanta and Berlin: Sample Business Scenario

The sample HIPAA PM implementation scenario demonstrates inbound and outbound message processing between the following parties:

- Atlanta Company
- Berlin Company

In the sample's business scenario, each company has an eXchange installation, and the two companies trade data.

Sample Scenario Business Description

This sample scenario and its Projects demonstrate the configuration of eXchange to support HIPAA. The scenario involves the HIPAA PM and two TPs, an Atlanta healthcare provider company, and a Berlin health insurance company. The current viewpoint is assumed to be Atlanta.

The resulting B2B solution functions as follows:

- HIPAA 270 Health Care Eligibility Benefit Inquiry payloads are read from a local (internal) file.
- The individual payloads are wrapped in the inner and outer HIPAA envelopes and sent to the Berlin TP.
- Berlin replies with a TA1 and 997 Functional Acknowledgments.
- Berlin delivers an 271 Health Care Eligibility Benefit Response eXchange prepares and writes the individual response payloads to an internal file and displays the messages in Message Tracking.

You can change the sample's scenario to reverse the companies' sender and receiver roles, if you want (see Chapter 6, "HIPAA PM Sample Scenario Tutorial," for more details). See "Using Message Tracking" on page 114 for details on this feature.

Figure 5–1 shows a diagram of the HIPAA PM sample's basic operation.

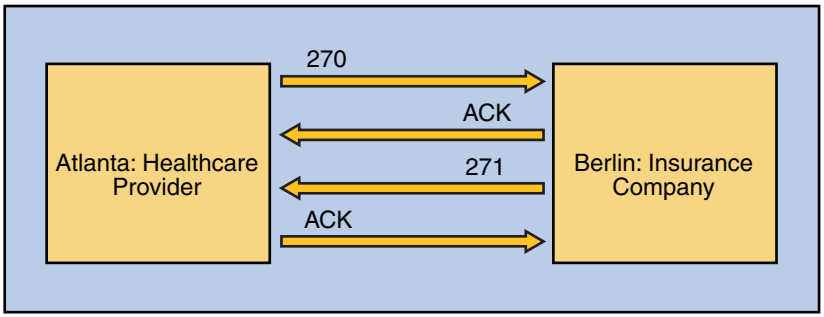

FIGURE 5–1 Sample Scenario Diagram

For a more detailed diagram, see Figure 6–1.

Sample Scenario Projects

The sample scenario is installed with the HIPAA PM product and contains sample Projects, available upon first use of Enterprise Designer. You may locate these components in the Enterprise Designer's **Project Explorer**.

The scenario utilizes the following Projects under **eXchange** in **Project Explorer**:

- **B2BHosts**
- **Deployment**
- **GUI**
- **Error**
- **Samples ⇒ HIPAA**

Note – You must create the Environments to be used by the sample scenario, as explained under "Constructing the Environments" on page 83 .

For a list of files used by these Projects, see "Exporting Sample Files" on page 63.

Getting Started

This section explains basic information you need to begin using the sample implementation scenario.

Note – See the *eXchange User's Guide* for more information on the subject matter covered by this section.

Before You Start

Before you start using the sample Projects, ensure you have completed the following tasks:

- Finish the installation, as explained in Chapter 3, "Installing HIPAA PM."
- Make sure your LDAP and Oracle systems are installed, configured, and operating correctly.
- Your Repository must be running.
- You must have two Domains installed and running, one for Atlanta (**dmnA**) and one for Berlin (**dmnB**).
- Using Enterprise Manager (port 15000), you must add two Integration Servers for the Domains, **dmnA** on 18000 for Atlanta and **dmnB** on 28000 for Berlin (**Host Name**: **localhost**; **User Name**: **Administrator**; **Password**: **STC**).
- Also for **dmnA**, add a user with the following parameters:
  - **username: userA**
  - **password: userA**
  - **Group List: PartnerManager, MessageTracking**
- For **dmnB**, add a user with the following parameters:
  - **username: userB**
  - **password: userB**
  - **Group List: PartnerManager, MessageTracking**
- You must be logged on to Enterprise Designer.

Note – If your Repository already has a Project at the root level whose name is identical to any of the Projects you are importing, you must delete or rename such Projects before you start

Exporting Sample Files

Files are supplied with the sample scenario, which support the general data processing of the sample. These files are for the transport of data and for the operation of ePM. You must export these files using Project Explorer in Enterprise Designer.

Note – For a list of the sample scenario's Projects, see "Sample Scenario Projects" on page 62 .

These files are:

- Data
- ePM

Exporting Data Files

The data files are:

- For Atlanta under **eXchange** ⇒ **Samples** ⇒ **HIPAA** ⇒ **RecvFromInt** ⇒ **Files**:
  - `270-SendingOutbound.dat.~in`
  - `270.dat`.
- For Berlin under **eXchange** ⇒ **Samples** ⇒ **HIPAA** ⇒ **271_FromInt_270** ⇒ **Files**:
  - `HIPAA_4010_271_template.st`
  - `HIPAA_dlg_270_In_Atlanta_270_In.xml`

It is recommended that you set up an export folder structure to contain these files like:

```
C:\temp\eXchange\Sample\HIPAA\Data\Atlanta (or Berlin)
```

Exporting ePM Files

The ePM export files are located in **Project Explorer** under **eXchange**, as follows:

- **ePMImport** ⇒ **HIPAA** ⇒ **Hosts** ⇒ **envA_HIPAA_Host.exp and envB_HIPAA_Host.exp**
- **ePMImport** ⇒ **HIPAA** ⇒ **Schedulers** ⇒ **envA_HIPAA_S1.exp and envB_HIPAA_S1.exp**
- **ePMImport** ⇒ **HIPAA** ⇒ **TP_Profiles** ⇒ **envA_HIPAA_TP_Berlin.exp and envB_HIPAA_TP_Atlanta.exp**

It is recommended that you set up an export folder structure to contain these files like:

```
C:\temp\eXchange\Sample\HIPAA\TP_Profiles (or B2B Hosts or Schedules)
```

The Atlanta ePM files are:

- **envA_HIPAA_Host**: For the B2B Host.
- `envA_HIPAA_S1.exp`: For the Schedule.
- `envA_HIPAA_TP_Berlin.exp`: For the **Berlin** TP.

The Berlin ePM files are:

- **envB_HIPAA_Host**: For the B2B Host.
- `envB_HIPAA_S1.exp`: For the Schedule.
- `envB_HIPAA_TP_Atlanta.exp`: For the **Atlanta** TP.

Editing the Sample Data Files

Files are supplied with the sample scenario, which reference path locations enclosed between the XML tags: `<dir>` … `</dir>`. You must edit these files to reflect the location where the data files are to be used by the Atlanta and Berlin systems.

The files you need to edit are:

- For Atlanta:

  `270-SendingOutbound.dat.~in`

- For Berlin

  `HIPAA_dlg_270_In_Atlanta_270_In.xml`

The previous section lists the locations of where to find these files, if you have not already exported them. If you need information on exactly how to edit these files, see "Editing the Sample Data .xml Files" on page 79.

If you have already run the sample and you want to experiment with other differences from the sample (such as using a payload data file with a different file name, or using a TP with a different name), be sure these differences are also reflected in these files, as necessary.

Constructing the Environments

This section contains Enterprise Designer procedures for constructing the required Environments for the sample scenario. Make sure that properties you configure under these procedures match your system's configuration, including system configurations you must check before you start (see "Getting Started" on page 62).

Before You Begin

- Make sure you have completed all the operations, as explained under "Before You Start" on page 63.

You must create these two Environments:

- For Atlanta: **envA**
- For Berlin: **envB**

Creating External Systems

Create, construct, and if necessary, configure the following external systems for **envA and envB**:

- **esOracle**
- **esBLF**
- **esHTTP**
- **esHTTPserver**
- **esFileA** (for **Atlanta) and esFileB (for Berlin)**
- **esLDAP**
- **esB2BService**

Configuring External Systems

Using their **Properties** dialog boxes, configure the following external systems for **envAtlanta**, as necessary for your setup:

- esOracle
- esLDAP

Make sure to configure the File external systems, as necessary for your system:

- **esFileA**
- **esFileB**

Using their **Properties** dialog boxes, configure the following additional components, as necessary for your setup:

- B2B Configuration Service
- JMS settings
- Sun SeeBeyond Integration Server

For additional information on these and additional necessary setup operations, see "Constructing the Environments" on page 83.

Using Deployment Profiles

This section describes how to build and deploy the Projects' Deployment Profiles in the HIPAA PM sample scenario. Building a Deployment Profile creates the application **.ear** file for the Project. After creating this file, you must deploy it for all Deployment Profiles *except* the B2B Host.

For more information on these operations, see "Constructing the Projects" on page 92.

Locating the Projects

On the **Project Explorer** tree, you may open the sample scenario's Projects to display their components.

Note – Make sure you have all of the Projects, as listed under "Sample Scenario Projects" on page 62 .

Deploying the Deployment Profiles

This section provides a procedure that describes how to construct and deploy the sample scenario's Project Deployment Profiles.

▼ To Construct and Deploy the Deployment Profiles

1. **Open the Project you want to work with, using Project Explorer.**
2. **Create and name one or more Deployment Profiles for each Project, as shown in Table 6–1.**
3. **Automap and deploy each Deployment Profile, except that you do *not* deploy the Deployment Profiles for the Host Project.**

Note – Make sure the B2B Host Deployment Profiles create an instance of the eXchange Service for each current Deployment Profile and Environment (one each for Atlanta and one each for Berlin).

---

4. **Make sure you click Save All after you are finished with each individual operation.**

Special Considerations for Deployment Profiles

Ensure that you take the following necessary considerations into account while constructing your Deployment Profiles:

- Do *not* deploy the B2B Host Deployment Profiles.
- Be sure that you create the validation Connectivity Map for the eXchange Deployment Project's Deployment Profiles; see "Creating the Validation Connectivity Map" on page 96 for details.
- Be sure that you include the correct path location in **bp271**; see "Updating the bp271 Business Process" on page 99 for details.

Importing Files for ePM

This section explains ePM procedures for importing the sample scenario files supplied for the B2B Hosts and Trading Partners.

Note – For a general description of the outbound and inbound messaging `ToPartner` and `FromPartner` model used by ePM, see "Importing and Configuring Components in ePM" on page 102 .

If you need more detailed procedures for any of the operations described under this section, see the *eXchange Integrator User's Guide*.

Running the ePM Interface

Start running ePM as explained under "Running ePM" on page 103.

Importing B2B Hosts

Your next step is importing the following B2B Host files:

- **envAtlanta_HIPAA_Host**: For Atlanta.
- **envBerlin_HIPAA_Host**: For Berlin.

Importing Schedules

Next, you must import the following Schedule files for the B2B Hosts.

- `envA_HIPAA_S1.exp`: For Atlanta.
- `envB_HIPAA_S1.exp`: For Berlin.

Importing Trading Partners

Next, you must import the TPs for the B2B Hosts.

- `envB_HIPAA_TP_Atlanta.exp`: For the **Atlanta** TP (**envB** for Berlin)
- `envA_HIPAA_TP_Berlin.exp`: For the **Berlin** TP (**envA** for Atlanta)

Running the Sample Scenario

This section explains how to run the sample scenario and transport data between the two TPs in the scenario, Atlanta and Berlin.

▼ To Transport Data Between the TPs

1. **Locate the folder on the machine running the domains, where you have stored the data to be transported, for example,** `C:\temp\eXchange\Sample\HIPAA\Data`**.**

2. **Rename file** `270-SendingOutbound.dat.~in` **located in the …** `HIPAA\Data\Atlanta\` **folder to** `270-SendingOutbound.dat`**.**

   The message transport operation occurs.

3. **Check Message Tracking (Figure 6–15) and make sure you see the following messages:**

   - *Transaction IDs* **HIPAA HIPAA_Actions** *Dialog ID* **271 Inbound**
   - *Transaction IDs* **HIPAA HIPAA_Actions** *Dialog ID* **270 Outbound**

   Result: If you are able to view the previous messages in Message Tracking, the sample scenario is running correctly and the data transport operation is successful.

Monitoring Messages

You may monitor overall message activity using the eXchange Message Tracking features. See "Using Message Tracking" on page 114 for information on how to access and begin using this feature.

◆ ◆ ◆ CHAPTER 6

HIPAA PM Sample Scenario Tutorial

This chapter provides a basic HIPAA PM tutorial, explaining how to create and implement a sample scenario, as well as how you can use eXchange to achieve B2B solutions using the HIPAA protocol. This chapter contains the following sections:

Using This Tutorial

This chapter provides detailed procedures that describe how to construct, run, and monitor the HIPAA PM sample implementation scenario.

If you prefer to see runtime results quickly without learning the detailed procedures, use the Quick Start.

Introduction to the Sample Implementation

To perform the sample scenario implementation, you need to set up the sample projects, their environments, and their components using the eGate Enterprise Designer with eInsight and eXchange.

The sample implementation scenario demonstrates inbound and outbound message processing between the Atlanta Company and the Berlin Company. In the sample's business scenario, each company has an eXchange installation, and the two companies trade data. This sample scenario and its Projects demonstrate the configuration of eXchange to support HIPAA. The current viewpoint is assumed to be Atlanta.

The resulting B2B solution functions as follows:

- HIPAA 270 Health Care Eligibility Benefit Inquiry payloads are read from a local (internal) file.
- The individual payloads are wrapped in the inner and outer HIPAA envelopes and sent to the Berlin TP.
- Berlin replies with a TA1 and 997 Functional Acknowledgments.
- Berlin delivers an 271 Health Care Eligibility Benefit Response eXchange prepares and writes the individual response payloads to an internal file and displays the messages in Message Tracking.

For more information solving business problems using eXchange with eInsight and eGate, including additional details on implementation, see the *eXchange Integrator User's Guide, eInsight Business Process Manager User's Guide,* and *eGate Integrator User's Guide.*

Figure 6–1 shows an operational diagram of the sample scenario.

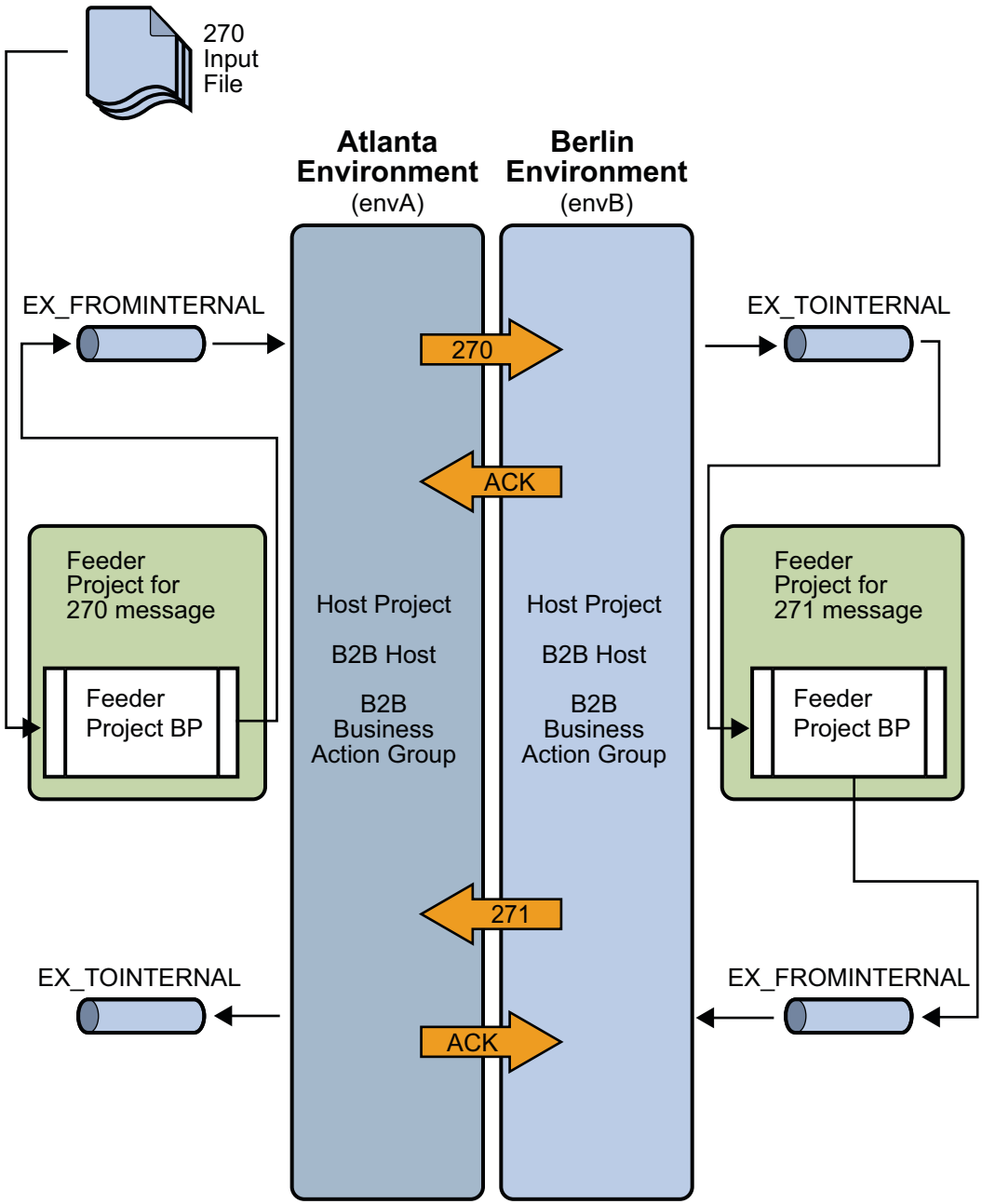

FIGURE 6–1 Sample Scenario Operation

Server Configurations

The sample assumes you use default configurations for all servers, where possible, and that you make any changes in Enterprise Designer, where needed, for example:

- **Oracle** – You must create a new outbound Oracle external system instance for each environment and configure it for your system, even if you imported the sample environments. Sample parameters are for reference only. Any Oracle database used by eXchange must be accessible to eGate. You must know the database's Oracle SID, user name, and password. Create and configure the eXchange database using the `Oracle510.zip` file. For more information see the *Oracle eWay Adapter User's Guide*.
- **LDAP** – You must create a new outbound LDAP external system instance for each Environment and configure it for your system, even if you imported the sample Environments. Sample parameters are for reference only. Any LDAP application used by eXchange must be accessible to eGate. For more information see the *LDAP eWay Adapter User's Guide*.
- **HTTPS** – For information on how to configure your HTTP server or client to use SSL, see the *HTTP(S) eWay Adapter User's Guide*.

Preconfiguration for the Atlanta and Berlin Environments

This section explains the preconfiguration operations you must perform for the Atlanta and Berlin Environments.

Creating and Starting the Domains

This section explains how to create and start the Logical Host Domains for the Atlanta and Berlin Environments.

See the *eGate Integrator User's Guide* for more information about eGate logical hosts, domains, and the Domain Manager feature.

▼ To Create and Start the Sample Domains

1 Create the domains.

- **To create the Atlanta domain, run the following script in the `\logicalhost` directory:**

```
C:\ ...
 logicalhost\createdomain --dname dmnA
```

- **To create the Berlin domain, run the following script in the** `\logicalhost` **directory:**

```
C:\ ...
 logicalhost\createdomain --dname dmnB --startingport 28000
```

This script creates the domain name **dmnB** and designates the default ports 2800x.

2. **If the repository is not already running, start it by running the following script:**

```
C:\ ... repository\startserver.bat
```

3. **Start the domains.**

- **To start the Atlanta domain , type the following command:**

```
C:\ ...
 logicalhost\start_dmnA.bat
```

Note – Starting the first domain can require approximately 7 minutes.

- **To start the Berlin domain , type the following command:**

```
C:\ ...
 logicalhost\start_dmnB.bat
```

4. **Use the Domain Manager interface to make sure the new domains are started and running.**

Adding a New User to ePM and Message Tracking

You must add two new ePM users, one for Atlanta and one for Berlin, using the eGate Integration Server Security Gateway.

▼ To Add a New User To the ePM and Message Tracking Groups

1. **With the Repository running, start a new browser session.**

2. **Access the appropriate URL.**

- **Atlanta:**`http://localhost:18000`

- **Berlin:**`http://localhost:28000`

3. **Log in to Integration Server Security Gateway using with the username** `Administrator` **and the password** `STC`**.**

4. **In the Integration Server Administration window, click the User Management tab.**

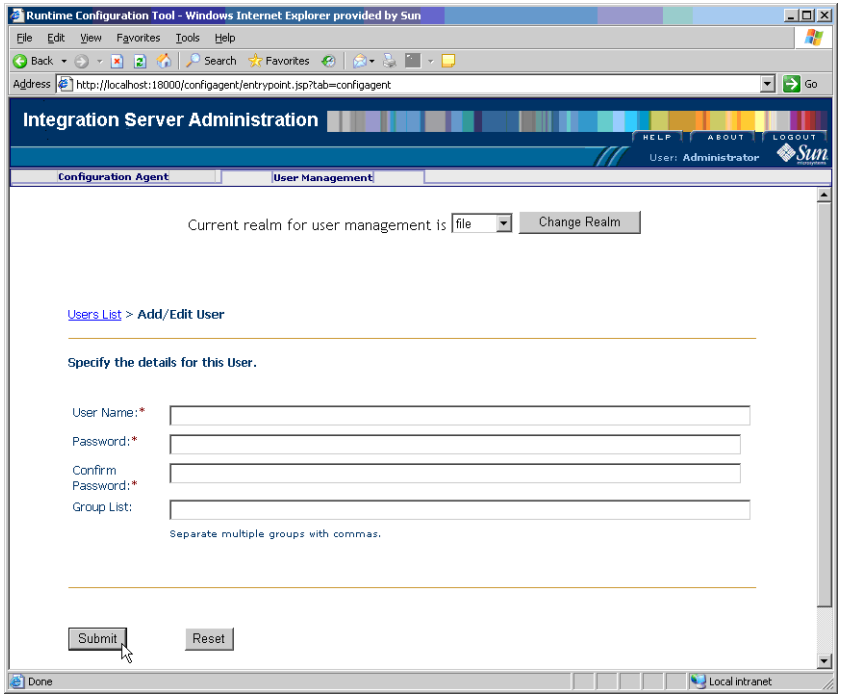

FIGURE 6–2 Screen capture of Integration Server Administration, User Management tab

5 Select Add New User and supply the user name and password for the new user.

- **Atlanta:**
  - Assign the user name `userA`
  - Assign the password `userA`
- **Berlin:**
  - Assign the user name `userB`
  - Assign the password `userB`

6 For Group List, type PartnerManager, MessageTracking

This step provides the following user privileges:

- The `PartnerManager` role allows the specified user to log in to and use ePM.
- The `MessageTracking` role allows the specified user to use the Message Tracking Web client.

7 When you are finished, click Submit.

8 Log out of Integration Server Administration and close the window.

Adding the Application Server Instances

You must add two new instances of the Application Server using the eGate Enterprise Manager, one for Atlanta and one for Berlin. Therefore, perform this procedure twice, once for Atlanta and once for Berlin.

▼ To Add Two New Application Server Instances

1. **With the Repository running, install Enterprise Manager by running the following script:**

   ```
   C:\ ...
    \emanager\install.bat
   ```

2. **In the installation wizard, follow the prompts and accept the license agreement and default port (15000).**

3. **After the installation is complete, start Enterprise Manager server by running the following script:**

   ```
   C:\ ...
    \emanager\startserver.bat
   ```

4. **Start a new browser session and access the appropriate URL:**

   ```
   http://localhost:15000
   ```

5. **Log in to Enterprise Manager with the user name** `Administrator` **and the password** `STC`**.**

6. **Select J2EE.**

7. **Click the Manage Servers tab, and add a new application server.**

   - Server Type:**Sun SeeBeyond Integration Server**
   - Host Name:**localhost**
   - User Name:**Administrator**
   - Password:**STC**

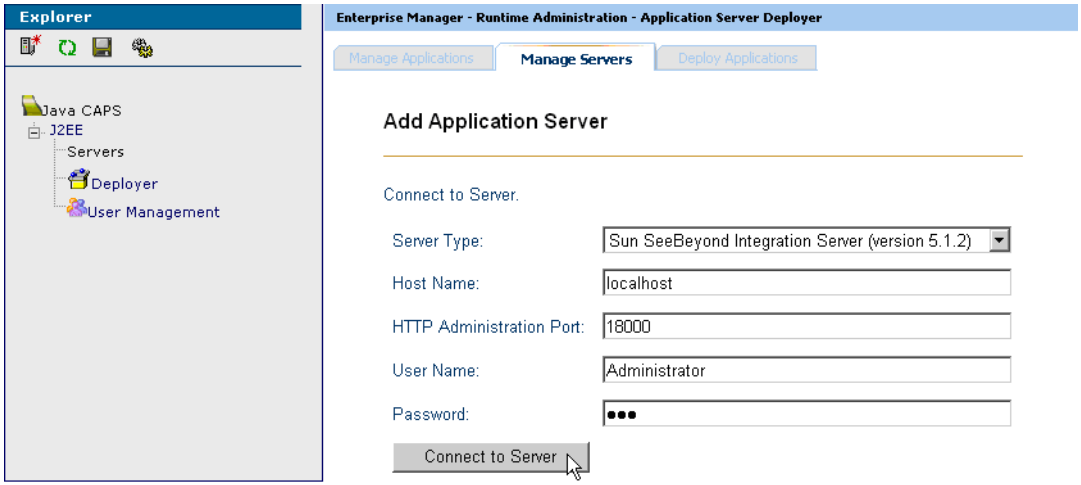

FIGURE 6–3 Enterprise Manager Window

8 **Click Connect to Server.**

9 **Save your changes and exit the window.**

Initializing and Running Enterprise Designer

This section describes operations to perform once you have initialized and run the Enterprise Designer.

Note – Using Enterprise Designer, increase the *eDesigner_heap_size* property to `1024`. For more information, see the *eXchange Integrator User's Guide*.

▼ To Initialize and Run Enterprise Designer

1 **With the Repository running, start Enterprise Designer by running the following script:**

```
C:\ ...
 \edesigner\bin\runed.bat
```

2 **Choose Update Center from the Tools menu.**

3 **In the Update Center wizard, follow the steps to check for updates, and to add all available updates and new modules.**

4 **When you are done, restart Enterprise Designer (referred to as IDE in the user interface).**

Note – For more information, see the *eGate Integrator User's Guide*.

5 **Log in to Enterprise Designer with the user name `Administrator` and the password `STC`.**

Next Steps Patch each Logical Host domain with `.jar` files to ensure message validation using the EDIFECS service.

▼ To Patch the Domains With Files For Validation

1 **To ensure correct third-party validation of messages, you must locate the following files in Enterprise Designer's Project Explorer under Sun SeeBeyond ⇒ eXchange ⇒ Protocol Managers ⇒ HIPAA Manager ⇒ Validations ⇒ EDIFECS ⇒ Files:**

- `xengine.jar`
- `xe_extensions.jar`

2 **Export these files to the following locations in your installation:**

- For Atlanta:

```
C:\ ...
 \logicalhost\is\domains\dmnA\lib\
```

- For Berlin:

```
C:\ ...
 \logicalhost\is\domains\dmnB\lib\
```

Note – For more information, see "Third-party Validation" on page 26.

Editing the Sample Data .xml Files

Data files are supplied with the sample scenario, which reference a path enclosed between the XML tags: `<dir>` … `</dir>`. You must first export these files using Enterprise Designer's **Project Explorer**. Then, edit these files to reflect the path location where you actually export the sample scenario files.

Note – For a list of the sample scenario's files, see "Exporting Sample Files" on page 63.

▼ To Export the Sample Data Files

1 **Locate the export files for the Atlanta sample data in Enterprise Designer's Project Explorer under eXchange ⇒ Samples ⇒ HIPAA ⇒ RecvFromInt ⇒ Files**

These files are:

- `270-SendingOutbound.dat.~in`
- `270.dat`.

2 **Export these files to a folder on your C drive. It is recommended that you set up a folder structure to contain these files, under `C:\temp`, for example:**
`C:\temp\eXchange\Sample\HIPAA\Data\Atlanta`

3 **Locate the export files that ensure Berlin returns the correct messages to Atlanta in Project Explorer, under eXchange ⇒ Samples ⇒ HIPAA ⇒ 271_FromInt_270 ⇒ Files:**

These files are:

- `HIPAA_4010A1_271_template.st`
- `HIPAA_dlg_270_In_Atlanta_270_In.xml`

4 **Export these files to a folder on your C drive. It is recommended that you set up a folder structure to contain these files, under `C:\temp`, for example:**
`C:\temp\eXchange\Sample\HIPAA\Data\Berlin`

You must make sure that the `270-SendingOutbound.dat.~in` file is updated to reflect the appropriate Atlanta data path location. You may do this operation using a text editor.

▼ To Edit the Atlanta `270-SendingOutbound.dat.~in` File

1 **Make sure you have exported the sample data files.**

2 **Use the Enterprise Designer's Export feature to export the sample data files to a specified location, for example:**

```
cd /d C:\temp\eXchange\Sample\HIPAA\Data\Atlanta
```

3 **Change directories to the subdirectory of the location where you exported the sample data files.**

4 **Use a text editor open the following file:**

`270-SendingOutbound.dat.~in`

You see text that resembles the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSPY v2004 rel. 3 U
(http://www.xmlspy.com)--><TestInput xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance" xsi:
noNamespaceSchemaLocation="C:\HIPAASample\xsd\ServiceInput.xsd">
<dir>path</dir>
<filename>270.dat</filename>
<tradingPartner>Berlin</tradingPartner>
<service>Eligibility_AG_Profile</service>
<action>270</action>
<createnumberofmsgs>1</createnumberofmsgs>
</TestInput>
```

The lines preceding the last line `</TestInput>` have the following meaning:

- The `<dir>…</dir>` line supplies the path of the directory that holds the payload data file to be processed.
- The `<filename>…</filename>` line supplies the file name of the payload data file for the current transaction.
- The `<tradingpartner>…</tradingpartner>` line supplies the name of the current TP.
- The `<service>…</service>` line supplies the name of the Transaction Profile Group of the current TP; used in ePM.
- The `<action>…</action>` line supplies the transaction number, in this case, 270.
- The `<createnumberofmsgs>…</ createnumberofmsgs>` line supplies the number of messages to be created, in this case, one.

5 If necessary, in the line `<dir>`*path*`</dir>` (shown in the previous example), change the string represented by `<path>`, to the actual path of the directory that holds your local copy of the `270.dat` file.

For example:

```
<dir>C:\temp\eXchange\Sample\HIPAA\Data\Atlanta</dir>
```

Or:

```
<dir>/~myname/eXchange/Sample/HIPAA/Data/Atlanta</dir>
```

6 If you have already run the sample and you want to experiment with other changes (such as using a payload file with a different file name, or using a TP with a different name), be sure they are also reflected here.

7 **When you are finished, save your changes and exit the text editor.**

You must make sure that the **Berlin** `HIPAA_dlg_270_In_Atlanta_270_In.xml` file is updated to reflect the appropriate Berlin data path location. You may do this operation using a text editor.

▼ To Edit the Berlin `HIPAA_dlg_270_In_Atlanta_270_In.xml` File

1 **Make sure you have exported the sample data files.**

2 **Use the Enterprise Designer's Export feature to export the sample data files to a specified location, for example:**

```
cd /d C:\temp\eXchange\Sample\HIPAA\Data\Berlin
```

3 **Change directories to the subdirectory of the location where you exported the sample data files.**

4 **Use a text editor open the following file:**

`HIPAA_dlg_270_In_Atlanta_270_In.xml`

You see text that resembles the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<FileAndService>
    <TradingPartner>Atlanta</TradingPartner>
    <TPProfileID></TPProfileID>
    <Service>Eligibility_Inb_AG</Service>
    <Action>271</Action>
    <Files Directory="path">
        <Name>HIPAA_4010A1_271_template.st</Name>
    </Files>
</FileAndService>
```

5 **If necessary, in the line <dir>*path*</dir> (shown in the previous example), change the string represented by *path*, to the actual path of the directory that holds your local copy of the `HIPAA_dlg_270_In_Atlanta_270_In.xml` and `HIPAA_4010A1_271_template.st` files.**

For example:

```
<dir>C:\temp\eXchange\Sample\HIPAA\Data\Berlin</dir>
```

Or:

```
<dir>/~myname/eXchange/Sample/HIPAA/Data/Berlin</dir>
```

6 **If you have already run the sample and you want to experiment with other changes (such as using a payload file with a different file name, or using a TP with a different name), be sure they are also reflected here.**

7 **When you are finished, save your changes and exit the text editor.**

Note – For more information, see the *eXchange Integrator User's Guide*.

Constructing the Environments

In implementing HIPAA PM Projects, you must set up at least one Environment for each eXchange installation. The sample scenario is set up to operate on one machine but mimic two TPs.

As a result, for the sample scenario, you need to construct the Environments as explained under the following sections:

- "Using Environment Explorer" on page 83
- "Setting up the Environments" on page 84

Using Environment Explorer

You perform these operations using Enterprise Designer's **Environment Explorer** and its canvas windows.

The sample Environments contain the following types of components:

- Instances for external systems accessed by eWays
- Instance for the B2B Service Configurator external system
- Instance for the Logical Host

For example, the Oracle external system must be configured to reference your Oracle setup. Other external systems (for example, the File and Batch eWays) have configurations that may differ depending on your system setup, and so forth. Also, you may be using nonstandard ports or user name/password combinations.

The remainder of this section describes the procedures to construct the sample scenario's Environments.

Note – Before you begin, make sure you have followed the preliminary instructions provided under "Getting Started" on page 62.

Setting up the Environments

This section explains how to create the sample's Environments for Atlanta and Berlin. Use the procedures to set up Atlanta first, then Berlin.

▼ To Create the Basic Components

1. **On Enterprise Designer, near the lower left of the window, click the Environment Explorer tab.**
2. **On the Environment Explorer tree, right-click the Repository and, on the context menu, click New Environment.**
3. **Name the newly created Environment envA (envB for Berlin).**
4. **Right-click envA (envB for Berlin) and, on the menu, click New Logical Host and name the Logical Host lhA (lhB for Berlin).**
5. **Right-click IntegrationSvr1 and select Properties from the context menu.**

   The **Properties** dialog box for **IntegrationSvr1** appears. See the figure below.

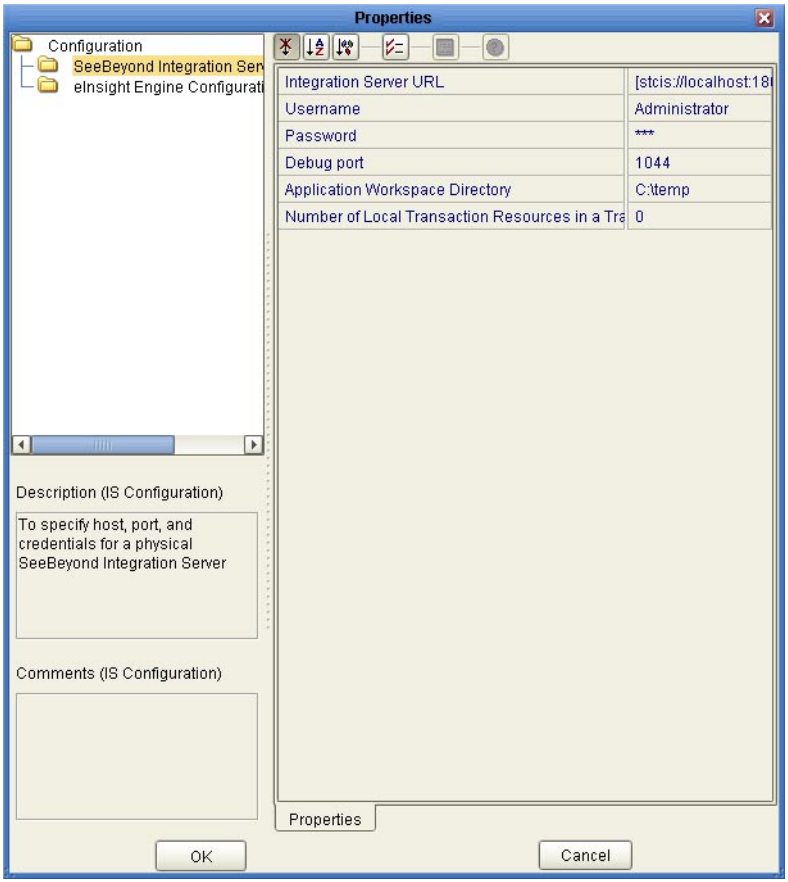

FIGURE 6–4 Integration Server Properties Dialog Box: Environment

6 For lhA ⇒ IntegrationSvr1 on Environment Explorer, set the Configuration ⇒ SeeBeyond Integration Server properties as follows:

- **Integration Server URL**: Points to the Integration Server, for example:
  - `http://localhost:18000` (for **envA**)
  - `http://localhost:28000` (for **envB**)
- **Username: Administrator**
- **Password**: **STC** (masked)
- **Debug port**: **1044**
- **Application Workspace**: Blank, for this sample.
- **Number of Local Transactions**: **0**

7 **For the rest of the IntegrationSvr1 properties settings, accept the defaults.**

8 **Create a Sun SeeBeyond JMS IQ Manager under IntegrationSvr1 and name it SBJMSIQMgr1.**

9 **Right-click SBJMSIQMgr1 and select Properties from the context menu.**

The **Properties** dialog box for **SBJMSIQMgr1** appears.

10 **For lhA ⇒ SBJMSIQMgr1 on Environment Explorer, set the Configuration ⇒ SeeBeyond JMS IQ Manager Configuration property as follows:**

Password: **STC**

▼ To Create and Configure the Oracle External System

1 **On Enterprise Designer, on the Environment Explorer tree, right-click envA (envB for Berlin) and, on the context menu, click New Oracle External System.**

2 **Name the new component esOracleand click OK.**

These actions create, for the current Environment, an external system instance for the Oracle eWay in outbound mode.

Note – The eXchange database uses Oracle. For more information on Oracle requirements for eXchange and HIPAA PM, see the `Readme`file that accompanies HIPAA PM.

---

3 **Right-click esOracle and select Properties from the context menu.**

The **Properties** dialog box for the external system appears. See the figure below.

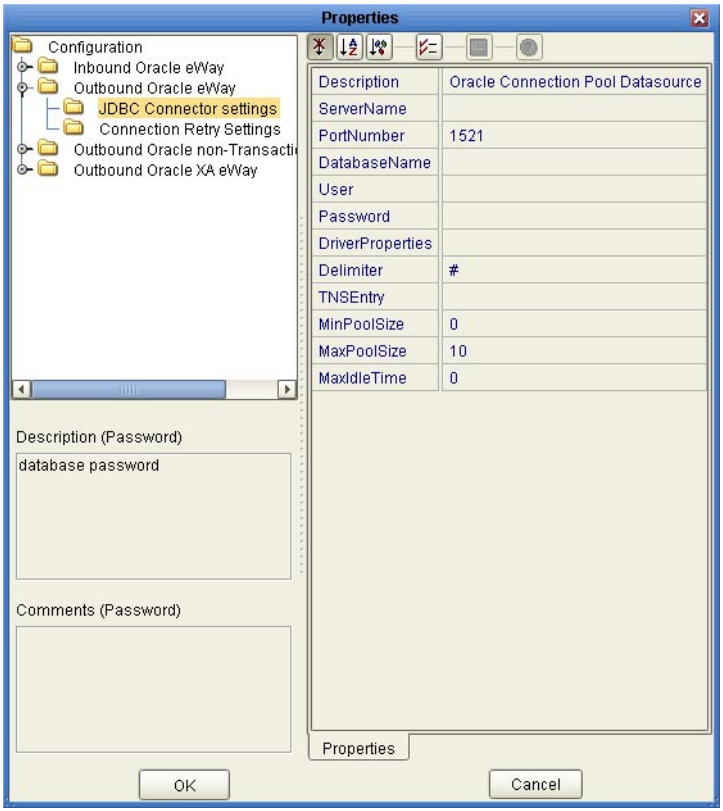

FIGURE 6–5 Oracle External System Properties Dialog Box: Environment

4 Configure the Configuration ⇒ Outbound Oracle eWay ⇒ JDBC Connector settings properties for esOracle as follows:

- **Description**: **Oracle Connection Pool Datasource**
- **ServerName**: Host name of the Oracle server machine
- **PortNumber**: **1521** (change this value only if your Oracle system administrator changed the default)
- **DatabaseName**: SID for your current Oracle system
- **User**: Valid user ID for the current Oracle system
- **Password**: Valid password for the current Oracle system (masked)
- **Driver Properties**: Blank, for this sample
- **Delimiter**: **#**
- **TNS Entry**: Blank, for this sample
- **MinPoolSize**: **0**

- **MaxPoolSize**: **10**
- **MaxIdleTime**: **0**

5 **Configure the Configuration ⇒ Outbound Oracle non-Transactional eWay ⇒ JDBC Connector settings properties for esOracle as follows:**

- **Description**: **Oracle non-Transactional Connection Pool Datasource**
- **ServerName**: Host name of the Oracle server machine
- **PortNumber**: **1521** (change this value only if your Oracle system administrator changed the default)
- **DatabaseName**: SID for your current Oracle system
- **User**: Valid user ID for the current Oracle system
- **Password**: Valid password for the current Oracle system (masked)
- **Driver Properties**: Blank, for this sample
- **Delimiter**: **#**
- **TNS Entry**: Blank, for this sample
- **MinPoolSize**: **0**
- **MaxPoolSize**: **10**
- **MaxIdleTime**: **0**

6 **When all properties have been configured correctly for your site, click OK.**

▼ To Create and Configure the LDAP External System

1 **Create a new LDAP external system (New ⇒LDAP External System) under envA (envB for Berlin) and name it esLDAP.**

2 **Set the Environment Configuration ⇒ Connection properties for esLDAP as follows:**

- **Initial Context Factory**: **com.sun.jndi.ldap.LdapCtxFactory**
- **Provider URL**: **As necessary for your system, according to the provided syntax**. You need to provide one organizational unit for Atlanta(exA) and another one for Berlin (exB), For example, `ldap://mycompany.co.in:1389/ou=exA,dc=co,dc=in`
- **Authentication**: **simple**
- **Principal**: As necessary for your system. For example, `Manager`
- **Credentials**: Password, as necessary for your system. For example, `exchange`

Note – A separate LDAP external system instance is required for each B2B Host.

3 **For all other esLDAPproperties, accept the defaults.**

▼ To Create and Configure the B2B Configurator Service External System

1 **Create a B2B Service Configurator (New ⇒ B2B Configurator Service) external system under envA and name it esB2BService.**

2 **Set the environment-configuration ⇒ Database Settings properties for esB2BService as follows:**

- **Type**: **Oracle**
- **URL**: Points to the eXchange database; an example of the URL syntax is: **jdbc:oracle:thin:@***hostname***:***port***:exchange**
- **UserName**: Valid user ID for the current Oracle system. For example, `ex_admin`
- **Password**: Valid password for the current Oracle system (masked). For example, `ex_admin`

3 **Set the environment-configuration ⇒ JMS Settings properties for esB2BService as follows:**

- Set the **environment-configuration ⇒ JMS Settings** properties for **esB2BService** as follows:
- **JMS Server URL**: Points to the IQ Manager port. The **envA** Logical Host is on 18000 (**envB** on 28000), the IQ Manager port for **envA** is 18007 (28007 for **envB**). This port number is listed in the Domain Manager for the current Logical Host; an example of the URL syntax is: **stcms://***hostname***:***port*
- **Security Principal**: **Administrator**
- **Security Credentials**: **STC** (masked)
- **Connection Factory**: **connectionfactories/topicconnectionfactory**
- **Resend Topic**: **topics/EX_TODELIVERY**
- **Timeout Topic**: **topics/EX_ERROR**
- **Business Protocol Topic for Batching**: **topics/EX_BATCHER**
- **Delivery Protocol Topic for Batching**: **topics/EX_DELIVERYBATCHER**

4 **For the rest of the esB2BService properties settings, accept the defaults.**

▼ To Create and Configure the File External Systems

1 **Create a new File eWay (New ⇒ File External System) in inbound mode under envA and name it esFileA.**

2 **Set the Configuration ⇒ Inbound File eWay ⇒ Parameter Settings property for esFileA as follows:**

Directory:

```
C:/temp/eXchange/Sample/HIPAA/Data/Atlanta
```

Note – Make sure this folder and the folder for envB are correctly configured under the appropriate parameter in ePM. It is recommended that you create an additional folder under HIPAA named Errors.

---

3 **Set the Configuration ⇒ Outbound File eWay ⇒ Parameter Settings property (for DLQ and processing errors) for esFileA as follows:**

Directory:

```
C:/temp/eXchange/Sample/HIPAA/Errors/Atlanta
```

4 **For all other File eWay (esFileA and esFileB) properties, accept the defaults.**

5 **Create a new File eWay (New ⇒ File External System) in inbound mode under envB and name it esFileB.**

6 **Set the Configuration ⇒ Inbound File eWay ⇒ Parameter Settings property for esFileB as follows:**

Directory:

```
C:/temp/eXchange/Sample/HIPAA/Data/Berlin
```

7 **Set the Configuration ⇒ Outbound File eWay ⇒ Parameter Settings property (for DLQ and processing errors) for esFileB as follows:**

Directory:

```
C:/temp/eXchange/Sample/HIPAA/Errors/Berlin
```

▼ To Create and Configure the Additional External Systems

1 **In Enterprise Designer, on the Environment Explorer tree, right-click envA (envB for Berlin) and, on the context menu, click New Batch Local File System.**

2 **Name the new external system esBLF, and click OK.**

These operations create, for the Environment, an external system for the Batch eWay in local file mode.

3 **In the new external systems' Properties dialog boxes and accept the defaults.**

Note – When you are finished with each *Properties* dialog box, click OK.

---

4 **Create an HTTP eWay (client mode) external system under envA (envB for Berlin) and name it esHTTP.**

5 **Open the Properties dialog boxes for esHTTP and accept the defaults.**

Note – You must create HTTP(S) external systems if you want to use the sample scenario with HTTP(S).

---

6 **Create an HTTP eWay (server mode) external system under envA (envB for Berlin) and name it esHTTPserver.**

7 **Open the Properties dialog boxes for esHTTPserver and accept the defaults.**

Note – When you build a B2B Host Deployment Profile, eXchange automatically creates another external system on the chosen Environment. This external system is called an eXchange service. For more information on this service, see the *eXchange Integrator User's Guide*. Also, see "Constructing the B2B Host Project" on page 93.

When You Are Finished for Atlanta

Result: You have set up the Environment for Atlanta, **envA**. See Figure 6–6.

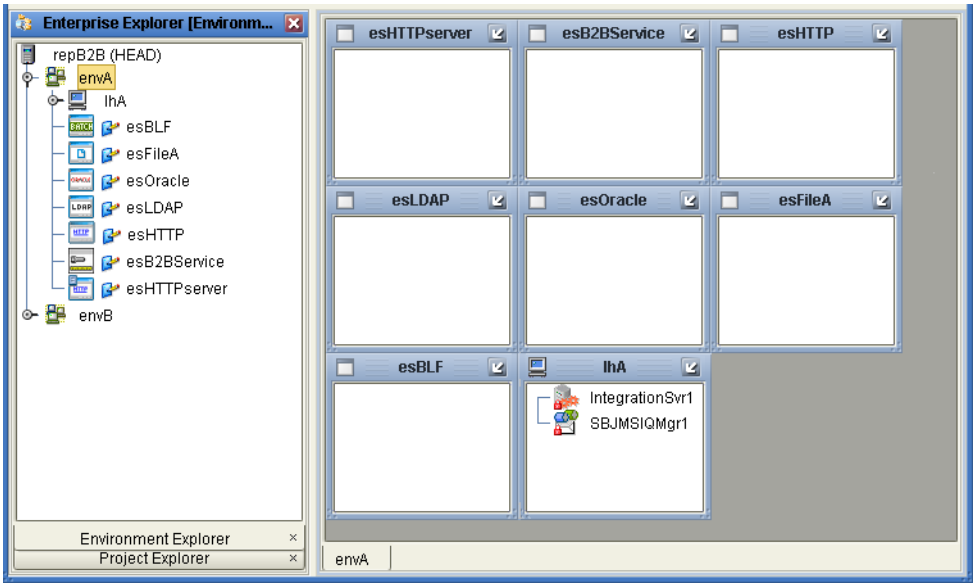

FIGURE 6–6 Sample Scenario Atlanta Environment

Collapse the **envA Environment Explorer** tree, click Save All, and close all canvases.

When You Are Finished for Berlin

Result: You have set up the Environment for Berlin, **envB**, which appears directly under **envA** on the **Environment Explorer** tree. See Figure 6–6.

Collapse the **envB Environment Explorer** tree, click Save All, and close all canvases.

Final Result: You have now finished setting up the Environments for Atlanta and Berlin, including the external system components to be used by both.

Constructing the Projects

This section explains how to construct the Projects in the HIPAA PM in order to run the sample scenario.

This operation includes:

- Using installed Projects (in **Project Explorer**) for the sample scenario
- Setting up and configuring Project components
- Associating each Project with the appropriate Environment(s)
- Mapping and building the Project's Deployment Profile
- Deploying the Deployment Profile, if necessary

Building a Deployment Profile creates the application .ear file for the Project. After creating this file, you must deploy it for all Deployment Profiles except the B2B Host.

You perform these operations using Enterprise Designer's **Project Explorer** and its canvas windows.

The remainder of this section describes the necessary procedures under the following sections:

Constructing the B2B Host Project

This section explains how to set up, and configure the HIPAA PM sample scenario's B2B Host Project, **HipaaHost**. Constructing the B2B Host Project creates an eXchange service that acts as a channel manager and provides a connection to the eXchange database. You must build two Deployment Profiles, one for each company, Atlanta and Berlin. However, you do *not* deploy these Deployment Profiles.

▼ To Build the B2B Host's Deployment Profile for Atlanta

1 **On Enterprise Designer's Project Explorer tree, right-click HipaaHost under eXchange ⇒ B2BHosts and, on the context menu, choose New and click Deployment Profile.**

2 **In the resulting dialog box, name the new Deployment Profile dpHost_A, point it at envA, make sure it is using only the cmHIPAA Connectivity Map, and click OK.**

Deployment Editor opens. Its left pane shows the HIPAA B2B Host instance, the **Oracle1** external application, and the **LDAP1** external application. These are the components created in the Connectivity Map **cmHIPAA**.

The Deployment Editor right pane contains windows representing the Logical Host and external systems created in **envA**.

3 **Click Automap to map the components.**

The components in the left pane automatically map to the appropriate windows on the right pane of Deployment Editor for **dpHost_A**. .

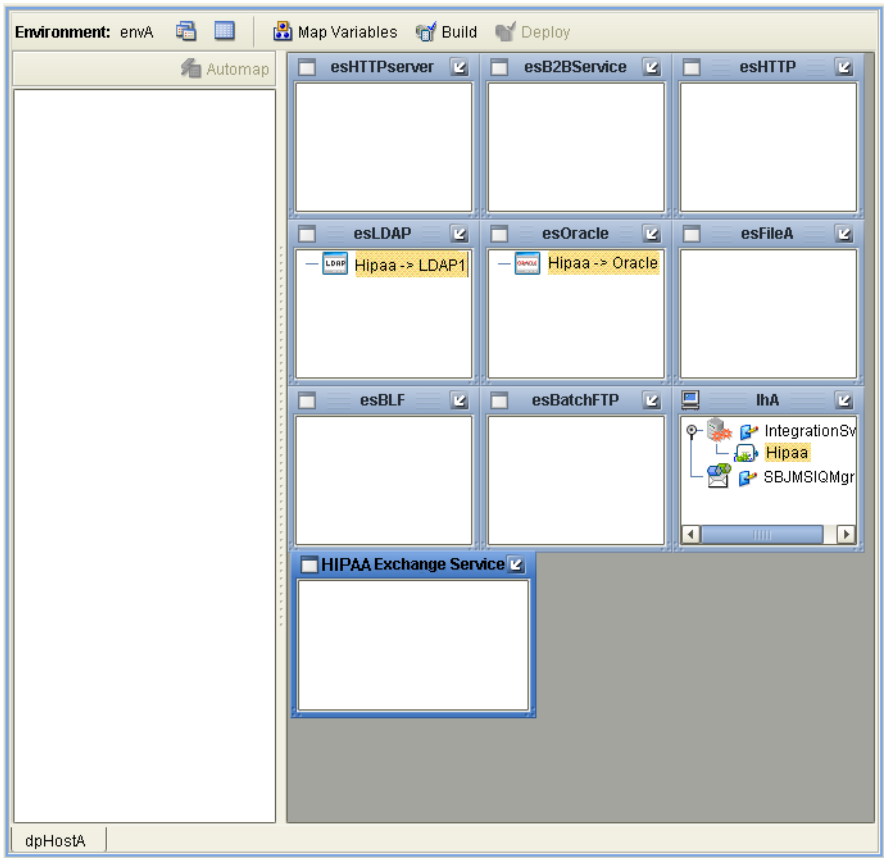

FIGURE 6–7 Deployment of dpHost A

4 **Click Save.**

5 **Click Build to build the Deployment Profile.**

A dialog box appears, indicating the status of the build operation. A new service, the HIPAA eXchange Service, is created and assigned to the current Deployment Profile and Environment.

You may view this HIPAA eXchange Service on **envA**, in the Environment Explorer tree, as well as in the right pane of Deployment Editor for **dpHost_A**.

Note – Do not deploy the B2B Host Project.

If the build operation is not successful, repeat the steps in this procedure, carefully rechecking every action. When the build is successful, go to the next step.

Note – Building Deployment Profiles for large Projects may take approximately 10 to 15 minutes or more.

6 **When you are finished, click Save All and close all canvases.**

▼ To Build the B2B Host's Deployment Profile for Berlin

1 **On Enterprise Designer's Project Explorer tree, right-click HipaaHost under eXchange ⇒ B2BHosts and, on the context menu, point at New and click Deployment Profile.**

2 **In the resulting dialog box, name the new Deployment Profile dpHost_B, point it at envB, make sure it is using cmHIPAA, and click OK.**

3 **In Deployment Editor, click Automap to map the components.**

4 **Click Save.**

5 **Build the Deployment Profile for Berlin in the same way as you did for Atlanta, except make sure to use envB and cmHostB.**

The HIPAA eXchange Service is created and assigned to the current Deployment Profile and Environment. Do not deploy the B2B Host Project. Once more, if there are any errors, troubleshoot until you are ready to go to the next step.

6 **When you are finished, click Save All and close all canvases.**

Result: You have now finished constructing the B2B Host Project, including creating, mapping, and building Deployment Profiles for Atlanta and Berlin.

eXchange Deployment Project

This section explains how to set up, build, and deploy Atlanta and Berlin Deployment Profiles in the eXchange **Deployment** Project. This Project makes all of the core B2B services and processing available to the application `.ear` files built from the Deployment Profiles.

To complete this operation, you must set up a Connectivity Map for HIPAA OTD validation and Deployment Profiles for both Atlanta and Berlin. You must map, build, and deploy both Deployment Profiles.

Creating the Validation Connectivity Map

To complete this operation, you must deploy OTD validation BPs using a Connectivity Map, to allow you to configure the Trading Partner Profiles to specify the custom validation handlers. You must then map, build, *and deploy* two Deployment Profiles, one each for Atlanta and Berlin.

▼ To Create the OTD Validations Connectivity Map

1. **Create a Connectivity Map using Project Explorer, under eXchange ⇒ Deployment, named, for example, cmHIPAAValidation (or a convenient name for your system, with fewer characters).**
2. **From Project Explorer, drag Sun SeeBeyond ⇒ eXchange ⇒ User Components ⇒ OTD Validations ⇒ HIPAA ⇒ 2000_Addenda ⇒ addenda_hipaa_270_Full_UniqueIDHandler onto the Connectivity Map canvas.**
3. **From the same Project Explorer location, drag the addenda_hipaa_271_Full_UniqueIDHandler component onto the Connectivity Map canvas.**
4. **Drag one eXchangeService from the eXchange ⇒ Deployment folder onto the canvas.**
5. **Connect eXchangeService to each of the other components.**
6. **Locate the files in the Project Explorer based on the validation service you want to use and drag it onto the Connectivity Map.**
   - **Sun SeeBeyond ⇒ eXchange ⇒ Protocol Managers ⇒ HIPAA Manager ⇒ Validations ⇒ EDIFECS ⇒ BPs ⇒ bp_HIPAA_ValidationService**
   - **Sun SeeBeyond ⇒ eXchange ⇒ Protocol Managers ⇒ HIPAA Manager ⇒ Validations ⇒ FORESIGHT ⇒ BPs ⇒ bp_EX_Foresight_HIPAA**
7. **Drag the respective JCD file onto the Connectivity Map.**
   - **EDIFECS ⇒ JCDs⇒jcdEX_HIPAA_ValidationService**
   - **FORESIGHT ⇒ JCDs⇒jcdEX_Foresight_HIPAA as shown in Figure 6–8**
8. **Rename the respective JCD component in the Connectivity Map by removing the `cmHIPAAValidation` prefix.**
9. **Connect all of the components as shown in Figure 6–8.**

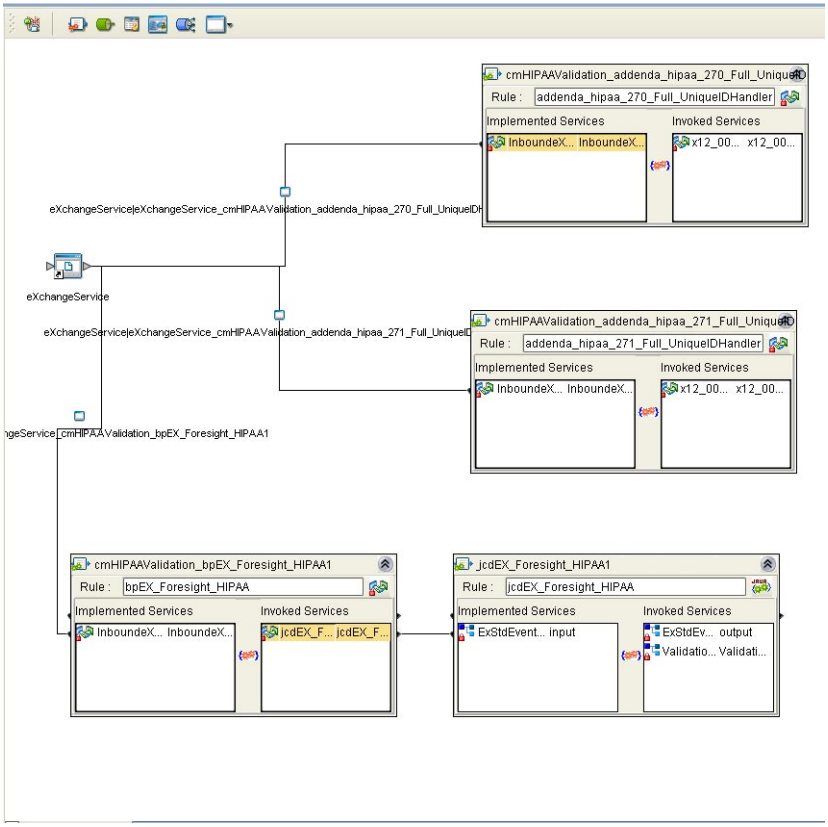

FIGURE 6–8 OTD Validation Connectivity Map Linking

10 **Open and save all the default properties for the eWays on the Connectivity Map.**

11 **Update the `instreamapi.jar` file with the correct version of the jar file from the Foresight engine.**

12 **Click Save All then close the Connectivity Map.**

Building and Deploying the Deployment Profiles

When you are finished, you must create Deployment Profiles for both Atlanta and Berlin. These Deployment Profiles are for the eXchange Deployment Project.

▼ To Build and Deploy the eXchange Deployment Project's Deployment Profile for Atlanta

1. **On Enterprise Designer's Project Explorer tree, right-click Deployment and, on the context menu, point at New and click Deployment Profile.**
2. **In the resulting dialog box, name the new Deployment Profile dpA, point it at envA, make sure it is using all the checked Connectivity Maps, and click OK.**
3. **On Deployment Editor, click Automap to map the components.**
4. **Click Build to build the Deployment Profile for Atlanta.**
5. **Click Deploy to deploy the Deployment Profile.**

Note – After each of the operations, map, build, and deploy, you receive a status message. If you receive any errors, troubleshoot your previous procedures, as necessary. Deploying Deployment Profiles may take as long or longer than building them.

---

6. **When you are finished, click Save All and close all canvases.**

▼ To Build and Deploy the eXchange Deployment Project's Deployment Profiles for Berlin

1. **On Enterprise Designer's Project Explorer tree, right-click Deployment and, on the context menu, point at New and click Deployment Profile.**
2. **In the resulting dialog box, name the new Deployment Profile dpB, point it at envB, make sure it is using all the checked Connectivity Maps, and click OK.**
3. **On Deployment Editor, click Automap to map the components.**
4. **Click Build to build the Deployment Profile for Berlin.**
5. **Click Deploy to deploy the Deployment Profile.**
6. **When you are finished, click Save All and close all canvases.**

   Result: You have now finished constructing the eXchange Deployment Project, including creating, mapping, building, and deploying Deployment Profiles for Atlanta and Berlin.

Constructing the 271_FromInt_270 Project

This section describes how to set up, build, and deploy the Berlin Deployment Profile for the **271_FromInt_270** Project. This Project operates with **envB** and makes sure the HIPAA 271 message is returned from Berlin to Atlanta.

Updating the bp271 Business Process

You must make sure the Berlin system is using the data file path listed under "Editing the Sample Data .xml Files" on page 79 by checking the **bp271** BP in **271_FromInt_270**. To do this action, open **eXchange** ⇒ **Samples** ⇒ **HIPAA** ⇒ **271_FromInt_270** ⇒ **BPs** ⇒ **bp271** in **Project Explorer**.

The BP structure appears in Business Process Editor, in Enterprise Designer's right pane. See Figure 6–9.

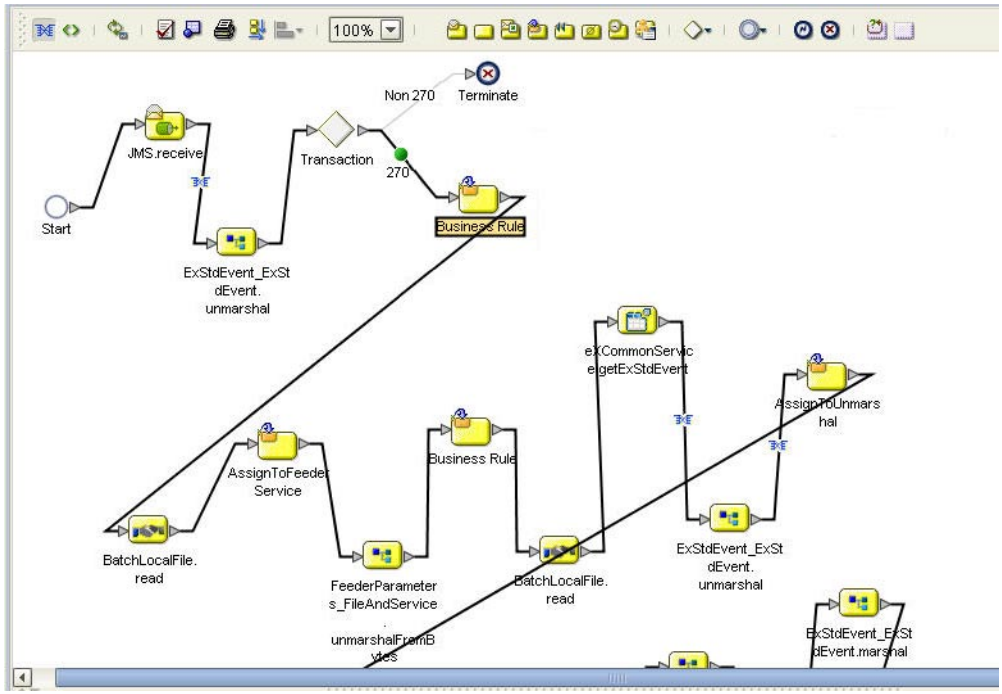

FIGURE 6–9 Business Process Editor: bp271

Make sure that the path given in the indicated component, in the previous figure, reflects your Berlin data path, for example:

```
C:\temp\eXchange\Sample\HIPAA\Data\Berlin
```

This is also the path location of the `HIPAA_dlg_270_In_Atlanta_270_In.xml` and `HIPAA_4010A1_271_template.st` files.

Note – This setup has been created for the purpose of the sample scenario only. It is recommended that, when creating your own inbound BPs, you configure the BP to read this type of path information from the inbound eWay.

Building and Deploying the Deployment Profile

This section describes how to build and deploy the **271_FromInt_270** Project's Deployment Profile for Berlin.

▼ To Build and Deploy the 271_FromInt_270 Project's Deployment Profile for Berlin

1. **On Enterprise Designer's Project Explorer tree, right-click Deployment and, on the context menu, point at New and click Deployment Profile.**
2. **In the resulting dialog box, name the new Deployment Profile dp271_B, point it at envB, make sure it is using all the checked Connectivity Maps, and click OK.**
3. **On Deployment Editor, click Automap to map the components.**
4. **Click Build to build the Deployment Profile for Berlin.**
5. **Click Deploy to deploy the Deployment Profile.**
6. **When you are finished, click Save All and close all canvases.**

   Result: You have now finished setting up the **271_FromInt_270** Project, including creating, mapping, building, and deploying Deployment Profile for Berlin only (there is no Atlanta Deployment Profile for this Project).

Constructing the Remaining Projects' Deployment Profiles

Construct the following Projects's Deployment Profiles, as shown under **eXchange** in **Project Explorer**, in the same way you have done for the previous Projects in the sample scenario:

- **ePM**
- **Tracker**
- **Sub_DLQ**
- **Sub_ProcErrors**

- **RecvFromInt**
- **RecvFromTP**; use only the **BatchLocalFile** sub-Project.
- **SendToInt**

To construct the remaining Projects' Deployment Profiles

Locate, name, and deploy Deployment Profiles for the Projects shown in the previous list, as depicted in Table 6–1.

Final Result: You have constructed, built, and deployed (if necessary) all the Projects' Deployment Profiles for the sample scenario.

Summary of Sample Scenario Projects

Table 6–1 provides a summary list of the sample scenario's Projects, their Deployment Profiles, and corresponding Environments. It is recommended that you construct the Projects and their Deployment Profiles in the order shown in the table.

TABLE 6–1 Sample Scenario Projects Summary

Location Under eXchange	Projects	Deployment Profiles	Environments
B2BHosts	HipaaHost	dpHost_A; not deployed	envA
		dpHost_B; not deployed	envB
Deployment	eXchange Deployment	dpA	envA
		dpB	envB
Samples ⇒ HIPAA	271_FromInt_270	dp271_B	envB
GUI	ePM	dpePM_A	envA
		dpePM_B	envB
	Tracker	dpTrack_A	envA
		dpTrack_B	envB
Error	Sub_DLQ	dpSDLQ_A	envA
		dpSDLQ_B	envB
	Sub_ProcErrors	dpSPErrors_A	envA
		dpSPErrors_B	envB

TABLE 6–1 Sample Scenario Projects Summary *(Continued)*

Location Under eXchange	Projects	Deployment Profiles	Environments
Samples ⇒ HIPAA	RecvFromInt	dpRecvInt_A	envA
	RecvFromTP	dpRecvTP_A	envA
		dpRecvTP_B	envB
	SendToInt	dpSendInt_B	envB

Importing and Configuring Components in ePM

This section explains how import, create, and configure TPs, Action Groups, Transaction Profiles, and Schedules in the HIPAA PM sample scenario, using the eXchange ePM. Additionally, the section describes how to use ePM to set the configuration parameter values for the Transaction Profiles and their related components.

Note – For detailed procedures on how to use TPs, Action Groups, Transaction Profiles, and Schedules, see the *eXchange Integrator User's Guide*.

Getting Started

Before you begin, it is recommended that you do all the procedures given in the previous sections of this chapter. Also, your Integration Server must be running. Also, your LDAP system and eXchange database (Oracle) must be running and accessible. However, Enterprise Designer does not need to be running.

Note – For a general description of the outbound and inbound messaging `ToPartner` and `FromPartner` model used by ePM, see "Configuring ePM: ToPartner and FromPartner Messaging Model" on page 44.

You *must* do the procedures given under "Running ePM" on page 103 to run ePM. In addition, after you run ePM, it is recommended that you do the procedures given under "Importing B2B Hosts" on page 104 and "Importing TPs" on page 106.

Note – If you want, you can create your own B2B Hosts and TPs using the procedures given in this section and using the sample scenario B2B Hosts and TPs as models. For more details, see the *eXchange Integrator User's Guide*.

The remainder of this section explains these operations.

Note – For detailed information on configuring ePM, see Chapter 4, "Configuring HIPAA PM."

Exporting the necessary ePM Files

The ePM export files for the B2B Hosts, TPs, and Schedules are located in **Project Explorer** under **eXchange**, as follows:

- **ePMImport ⇒ HIPAA ⇒ Hosts ⇒ envA_HIPAA_Host.exp and envB_HIPAA_Host.exp**
- **ePMImport ⇒ HIPAA ⇒ Schedulers ⇒ envA_HIPAA_S1.exp and envB_HIPAA_S1.exp**
- **ePMImport ⇒ HIPAA ⇒ TP_Profiles ⇒ envA_HIPAA_TP_Berlin.exp and envB_HIPAA_TP_Atlanta.exp**

For more information, see "Exporting ePM Files" on page 64. It is recommended that you set up a folder structure to contain these files, which reflects this organization, for example:

```
C:\temp\eXchange\Sample\HIPAA\TP_Profiles
```

Note – For more information on how to use ePM, see the *eXchange Integrator User's Guide*.

Running ePM

This section explains how to start running eXchange ePM.

▼ To Run ePM

1. **Start a browser session.**
2. **Enter the Logical Host name and ePM port number with epm appended, as follows:**

   `http://`*logicalhost*`:`*port+1*`/epm`

   For example:

   ```
   http://localhost:18001/epm
   ```

3 **When the sign-in window appears, enter your Enterprise Manager user name (or the new user described under "Adding a New User to ePM and Message Tracking" on page 75), as well as the appropriate password, and click Sign In.**

The initial ePM window appears. See Figure 6–10.

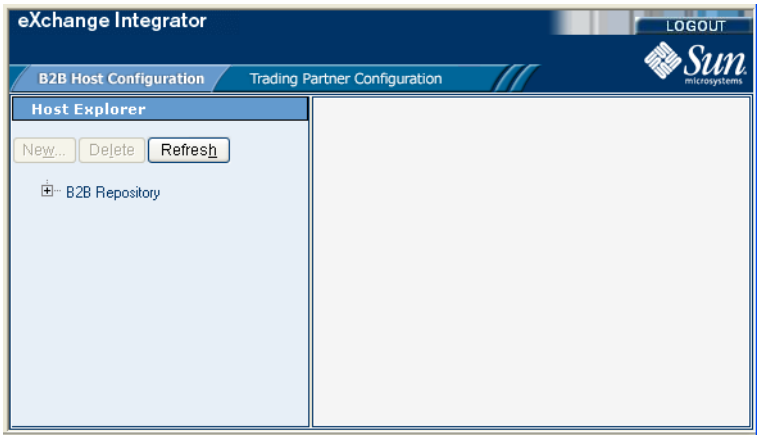

FIGURE 6–10 ePM Window

The ePM window has the following sections:

- **ePM Explorer**
  - **B2B Host Configuration** tab
  - **Trading Partner Configuration** tab
- **ePM Canvas**

Note – For complete instructions on how to use ePM, see the *eXchange Integrator User's Guide*.

Importing B2B Hosts

Your next step is importing the Atlanta and Berlin B2B Host files, as explained under this section.

This sample scenario has the following B2B Hosts:

- **envA_HIPAA_Host**: For Atlanta.
- **envB_HIPAA_Host**: For Berlin.

To Import the envA B2B Host

1. Log in to ePM for envA (dmnA).
2. Click the B2B Host Configuration tab, if Host Explorer is not already displayed.
3. In Host Explorer, click and expand B2B Repository.
4. Select the B2B Host envA_HIPAA_Host.
5. At the bottom of ePM Canvas, click Import.
6. When you are finished, click Save.

To Import the envB B2B Host

1. Log in to ePM for envB (dmnB).
2. Click the B2B Host Configuration tab, if Host Explorer is not already displayed.
3. In Host Explorer, click and expand B2B Repository.
4. Select the B2B Host envB_HIPAA_Host.
5. At the bottom of ePM Canvas, click Import.
6. When you are finished, click Save.

Using Schedules

Next, you must import the Schedules for the B2B Hosts.

To Import a Schedule

1. Log in to ePM for envA (dmnA) for Atlanta; use envB (dmnB) for Berlin.
2. Click the B2B Host Configuration tab.
3. ePM Explorer with this tab selected appears.
4. Click the Schedule icon in ePM Explorer.

5 **Select the Schedule file you want to import (envA_HIPAA_S1.exp for envA and envB_HIPAA_S1.exp for envB).**

6 **Click Import.**

7 **When you are finished, click Save.**

▼ To Modify an Existing Schedule

1 **Log in to ePM for envA (dmnA) for Atlanta; use envB (dmnB) for Berlin.**

2 **Click the B2B Host Configuration tab.**
ePM Canvas with this tab selected appears.

3 **Click the Settings tab.**

4 **In ePM Canvas, modify the scheduling information for the current Schedule, as necessary. This information is for inbound only.**

5 **When you are finished, click Save.**

Importing TPs

Your next step is importing or creating the Atlanta and Berlin TP files, as explained under this section. Keeping track of the TPs, where they are sent from, and where they are received depends on which company you consider to be your current company. See "Configuring ePM: ToPartner and FromPartner Messaging Model" on page 44.

This sample scenario has the following TPs:

- **Berlin**: For Atlanta.
- **Atlanta**: For Berlin.

Note – Also, you may create and construct these TPs yourself, using the sample TPs as models.

This sample scenario has the following TP files (under TP_Profiles):

- `envA_HIPAA_TP_Berlin.exp`: For Atlanta.
- `envA_HIPAA_TP_Atlanta.exp`: For Berlin.

To Import the Berlin TP to EnvA

1. **Click the Trading Partner Configuration tab.**

   The ePM window with this tab selected appears. See Figure 6–11.

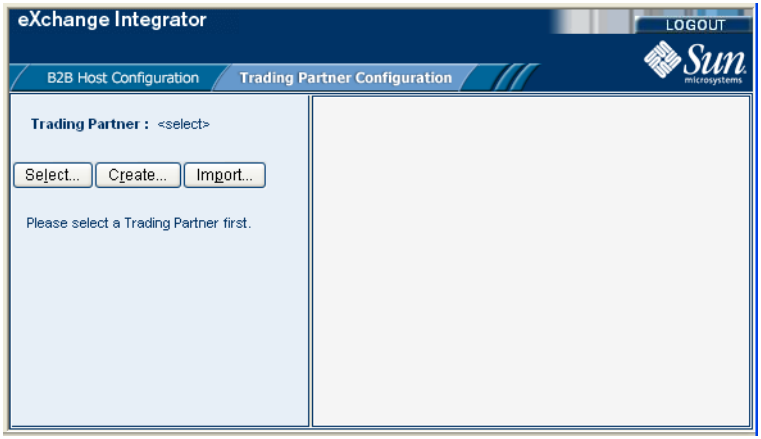

FIGURE 6–11 ePM Window With Trading Partner Configuration Tab Selected

2. **From this window, click Import.**

   The **Import a Trading Partner - Step 1 of 2** window appears in **ePM Canvas**.

3. **Name the TP Berlin.**

4. **Browse to the folder where you have stored your TP files and select envA_HIPAA_TP_Berlin.exp, then click Next.**

   The **Import a Trading Partner - Step 2 of 2** window appears.

5. **Choose envA_HIPAA, from the pull-down menu.**

6. **Click Finish.**

To Locate the Berlin TP in the ePM Window

1. **In the upper left side of the ePM window, click Select.**

   The **Select the Trading Partner to Configure** window appears in **ePM Canvas**.

2. **Click Search on the canvas.**

   Any available TPs appear directly below.

3. **In this case, you are looking for Berlin, which appears.**
4. **Click the TP name, in this case Berlin, to configure the TP.**

▼ To Import the Atlanta TP to envB

1. **Click the Trading Partner Configuration tab.**
   The ePM window with this tab selected appears.
2. **From this window, click Import.**
   The **Import a Trading Partner - Step 1 of 2** window appears in **ePM Canvas**.
3. **Name the TP Atlanta.**
4. **Browse to the folder where you have stored your TP files and select** `envB_HIPAA_TP_Atlanta.exp`**, then click Next.**
   The **Import a Trading Partner - Step 2 of 2** window appears.
5. **Choose envB_HIPAA, from the pull-down menu.**
6. **Click Finish.**

▼ To Locate the Atlanta TP in the ePM Window

- **Use the same procedure as explained for Berlin TP.**

Using Action Groups and Transaction Profiles

You do the actual configuration of Action Groups and Transaction Profiles using parameters available using the following levels of the **ePM Explorer** tree:

- **Business Protocols**
- **Delivery Protocols**
- **Transports**

More information on how to configure **Transport** parameters is available in the *eXchange Integrator User's Guide*. For information on how to configure these parameters in the sample scenario, see "Configuring Transports" on page 113.

Configuring the Sample Scenario

You may use the ePM for the Projects in the sample scenario as a model to complete the configuration of ePM. Enter information in ePM as shown in the sample. For more information, see Chapter 4, "Configuring HIPAA PM," and the *eXchange Integrator User's Guide*.

Using Parameters in ePM

Many of the Business and Delivery Protocol parameters are the same, regardless of the PM and business communication protocol you are using. However, some of them are HIPAA PM-specific and are only present for HIPAA.

This section describes these parameters under:

- "Interchange Envelope Parameters" on page 110
- "Functional Group Parameters" on page 111

For more information on these parameters, see "Configuring HIPAA PM ePM Parameters" on page 44.

Note – For more information on parameters not described under this section, see the *eXchange Integrator User's Guide*.

▼ To Enter an Override Value for a Parameter

1. **Click the check box next to the parameter you want to override, under the Override column (see Figure 6–12 for an example).**
2. **Enter the appropriate override in the text box for the parameter.**
3. **Click Save.**

ePM Configuration General Operation

In the sample scenario, you import preconfigured B2B Hosts and TPs.

When you are configuring your own (for example, if you are creating B2B Hosts and TPs from scratch), it is recommended that you use the following general order of configuration operations when setting values in ePM:

- On the **B2B Host Configuration** tab, create a new B2B Host Transaction Profile.
- Create a new Action Group (ePM here calls this a Business Action Group) for the B2B Host. Be sure to choose the correct Delivery Action and External Transport for the Action Group's Business Actions.

- On the **Trading Partner Configuration** tab, create a new TP.
- For the new TP, select the Transaction Profile from the B2B Host.
- Choose the necessary settings (**Settings** tab) for the current TP Transaction Profile.
- Open any applicable Business Actions and set appropriate overrides, as necessary.

Interchange Envelope Parameters

The HIPAA PM-specific Interchange Envelope (outer envelope or ISA) parameters appear in **ePM Canvas** as shown in Figure 6–12. The example shown is for the **Berlin** TP's **270 ToPartner** Transaction Profile.

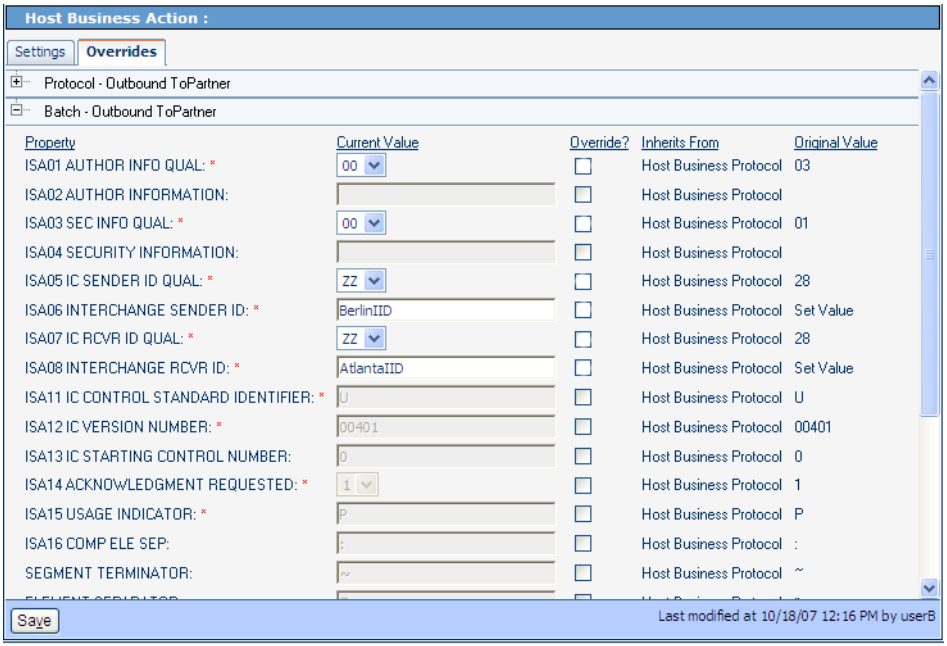

FIGURE 6–12 HIPAA PM-specific Interchange Envelope Parameters: Example

You may display the example in Figure 6–12 by using **ePM Explorer**, under **B2B Repository** ⇒ **envA_HIPAA** ⇒ **Business Protocols** ⇒ **HIPAA**.

As you can see, there are no override values entered in Figure 6–12, and the configuration accepts all the defaults. You may override the defaults for any parameter by clicking a check box under **Override** and entering a different value, as necessary.

You may, of course, do the same override operation with other ePM parameters, as described under "Configuring eXchange Partner Manager: Overview" on page 39.

Functional Group Parameters

The HIPAA PM-specific Functional Group (inner envelope or GS) parameters appear in **ePM Canvas** as shown in Figure 6–13. The example shown is for the **Atlanta** TP's **270 FromPartner** Transaction Profile.

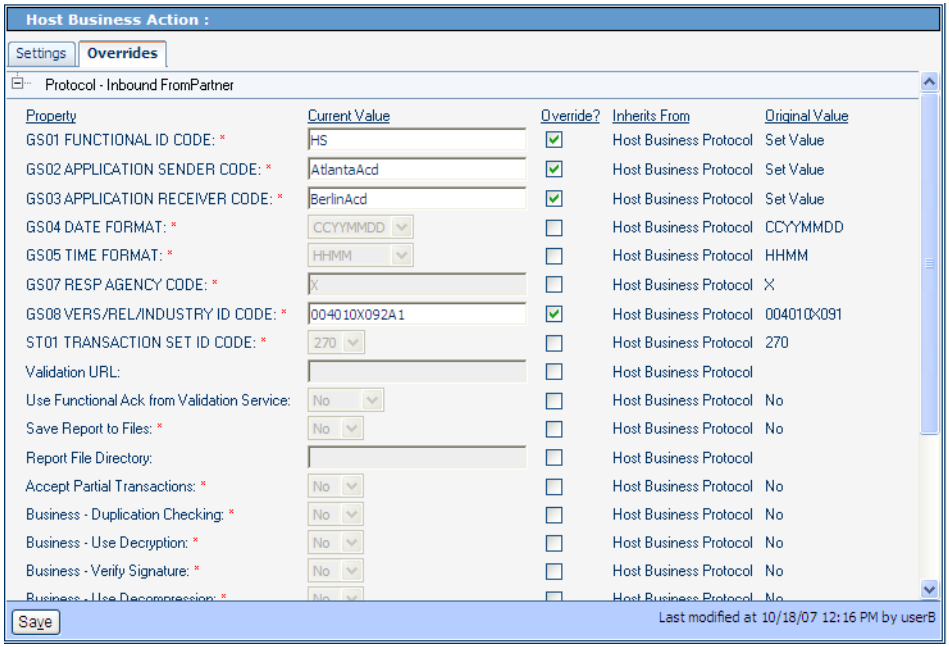

FIGURE 6–13 HIPAA PM-specific Functional Group Parameters: Example

You may display the example in Figure 6–12 by using **ePM Explorer**, under **B2B Repository** ⇒ **envA_HIPAA** ⇒ **Business Protocols** ⇒ **HIPAA**.

As you can see, four overrides value has been entered in Figure 6–13, and the configuration uses the defaults for all other displayed parameters. As explained previously, you may override the default values, as necessary.

Necessary Overrides

The configured overrides in the imported ePM files may not be appropriate to your system. You may need to configure additional overrides, as necessary, depending on your own system setup. It is recommended that you check the ePM interface for the Projects in the sample scenario as a model to ensure the correct configuration of ePM.

You must configure overrides for the following Business Protocol ePM values, as appropriate to your system:

- **Business Message Syntax Validation Handler**: Allows you to specify the third-party validation service for HIPAA PM .
- **Custom External Unique ID Handler**: Allows you to select the external unique ID handlers, and which ones take priority. This parameter also allows you to set up eXchange to use the appropriate messaging unique IDs.
- **Save Report to Files and Report File Directory**: Allows you to save interleaved error reports to text files and send copies of these files to a predefined directory.

Default for ePM Parameter GS08

The current default value for the **GS08** parameter is **00401X091**. You must change this default so that it matches the version for each of the HIPAA transactions defined in ePM. For example, you must enter **00401X092A1** for the HIPAA 270 Addenda.

For more information on this parameter, see "GS08 Vers/Rel/Indust ID Code" on page 55. Figure 6–13 shows the parameter in ePM, reflecting an inherited override setting.

Handler Settings

The **Custom External Unique ID Handler** and **Business Message Syntax Validation Handler** parameters are located in ePM's TP Transaction Profile's **Settings** tab. Make sure both of these parameters are set correctly, according to their usage in your system. See Figure 6–14, from the sample scenario's **Berlin** TP for **envA** (Atlanta).

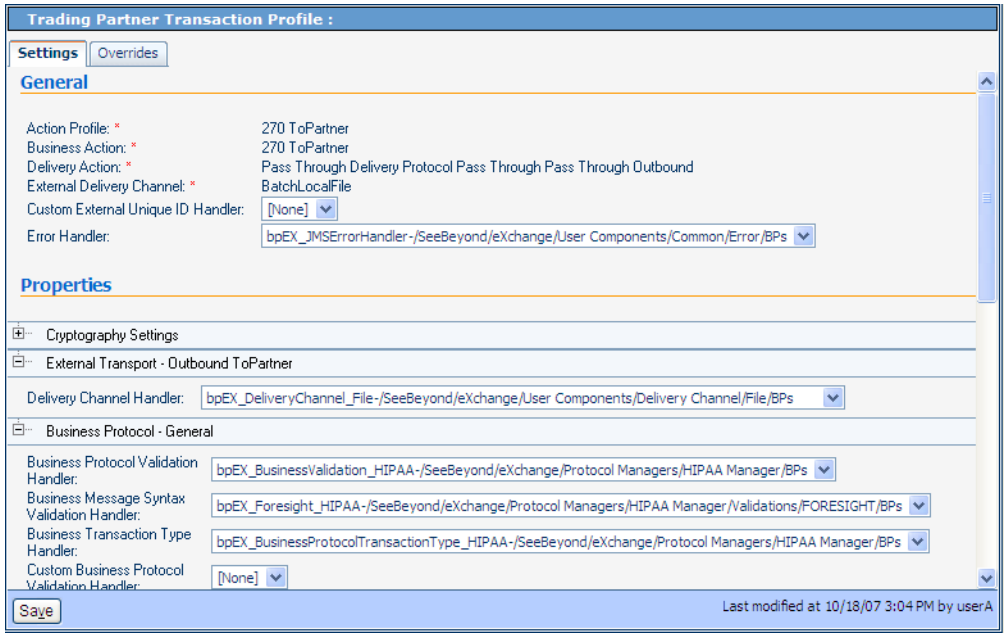

FIGURE 6–14 ePM Handler Settings

Note – If the Unique ID handler is not selected, or if the message itself does not contain the Unique ID field (it is an optional field), random numbers are generated for the message Unique IDs. Third-party defined Unique IDs are not supported.

Configuring Transports

Table 6–2 lists the **Transports** parameter override values you must enter to configure **B2B Host Configuration ⇒ envA_HIPAA ⇒ Transports ⇒ BatchLocalFile**.

TABLE 6–2 Overrides for Atlanta B2B Host Configuration ⇒ … ⇒ BatchLocalFile

Category	Parameter	Override Value
Outbound ToPartner	TargetDirectoryName	`C:\temp\eXchange\Sample\HIPAA\Data\Atlanta`
Inbound FromPartner	TargetFileName	`ToAtlanta_[a-zA-Z0-9_]*\.msg`
ACK - Outbound ToPartner	TargetDirectoryName	`C:\temp\eXchange\Sample\HIPAA\Data\Atlanta`
ACK - Inbound FromPartner	TargetFileName	`ToAtlanta_[a-zA-Z0-9_]*\.msg`

Table 6–3 lists the **Transport** parameter override values you must enter to configure **B2b Host Configuration ⇒ envB_HIPAA ⇒ Transports ⇒ BatchLocalFile**.

TABLE 6–3 Overrides for Berlin B2B Host Configuration ⇒ … ⇒ BatchLocalFile

Category	Parameter	Override Value
Outbound ToPartner	TargetDirectoryName	`C:\temp\eXchange\Sample\HIPAA\Data\Berlin`
Inbound FromPartner	TargetFileName	`ToBerlin_[a-zA-Z0-9_]*\.msg`
ACK - Outbound ToPartner	TargetDirectoryName	`C:\temp\eXchange\Sample\HIPAA\Data\Berlin`
ACK - Inbound FromPartner	TargetFileName	`ToBerlin_[a-zA-Z0-9_]*\.msg`

Running the Sample

See "Running the Sample Scenario" on page 69 for information on how to complete the passing of data between the two TPs.

The results after running the sample scenario:

- `...\HIPAA\Data\Atlanta` folder contains
  - one 270 message
  - one 997 message
  - two TA1 messages
- `...\HIPAA\Data\Berlin` folder contains
  - one 271 message
  - one 997 message
  - two TA1 messages

Using Message Tracking

eXchange provides a special feature, Message Tracking, allowing you to monitor the status of messages as they are received and processed through eXchange and HIPAA PM.

Before You Begin

- You must already have deployed the appropriate Projects' Deployment Profiles for the sample scenario.

  Note – The B2B Host Project is not deployed.

- Your Oracle and LDAP systems for eXchange must already be running, and you must already have begun running both Logical Hosts before you can run Message Tracking.
- The inbound and outbound scenarios for the sample must be running.

- For Message Tracking to be useful, there must be one or more messages that have already been picked up by the current Logical Host's Integration Server.

Accessing Message Tracking

This section explains how to access Message Tracking.

▼ To Access Message Tracking

1 Start a browser session.

2 Point your browser at the following URL:

`http://`*logicalhost*`:`*port+1*`/`*objname*

Where:

- *logicalhost*: The host name or IP address of a Logical Host running your Project, that is, the current Logical Host.
- *port*: The Web server connector port configured in your Integration Server. To discover this information, use **Environment Explorer** to open the current Logical Host. Right-click the Integration Server and select **Properties**. Open **IS Configuration ⇒ Sections ⇒ Web Container ⇒ Web Server ⇒ Default Web Server**; *port* is the value set for **Connector Port**. If you have several Web server configurations, check them also.

  The default port-number value is 18001 for the first Integration Server in the first-created Logical Host. (or **28001** for the first Integration Server in the second-created Logical Host, and so on). For the sample scenario, use 18001 for Atlanta (**envA**) and 28001 for Berlin (**envB**).
- *objname*: The name of the Message Tracking instance as it appears on the current Connectivity Map. For the sample scenario, this name is tracker.

Example: To access Message Tracking for the sample scenario, use the following URLs:

```
http://localhost:18001/tracker
```

Note – You can only use the same port number for different Message Tracking instances if they reside on different machines.

As stated previously, the sample must be running before you access Message Tracking, and messages must have been transported before any become accessible.

Message Tracking Window

When you first run Message Tracking, the **Message Tracking** window appears. After you perform a search, as necessary, in the window's left pane, message information results appear in the right pane. See Figure 6–15.

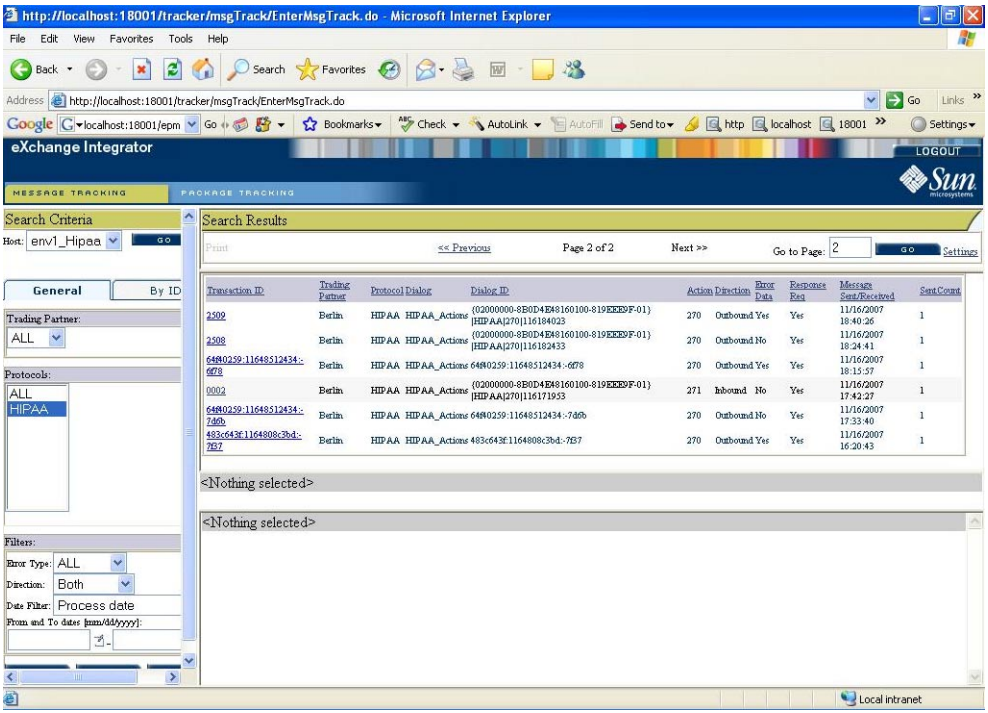

FIGURE 6–15 Atlanta: Example Message Tracking Window

See the *eXchange Integrator User's Guide* for information on how to use Message Tracking.

Interleaved Error Reports

The HIPAA PM Message Tracking feature also allows you to view interleaved error reports, that is, reports that show any error you wish to view, in its messaging context.

▼ To View Interleaved Reports

1 **In the Message Tracking window, select a message with one or more errors..**

2 **Next to Interleaved Report, click Open.**

The interleaved error report appears. See Figure 6–16.

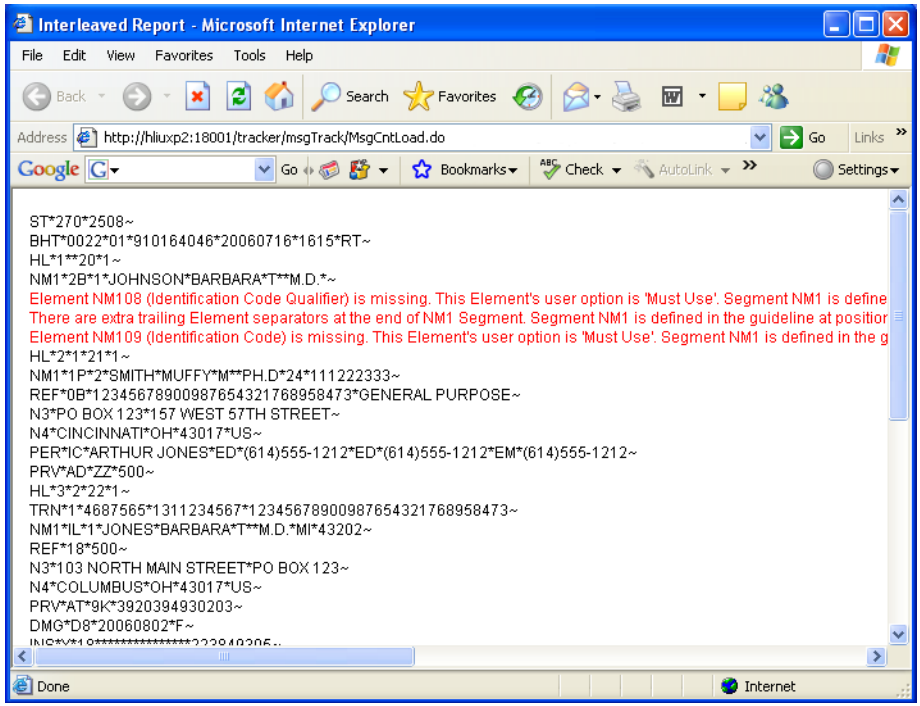

FIGURE 6–16 Atlanta: Interleaved Error Report

Any error appears in context, in red type. You may view interleaved error reports for inbound and outbound messages.

Note – Invalid messages may not be correlated.

◆ ◆ ◆ APPENDIX A

Externally Assigned Unique IDs

This appendix explains how the externally assigned unique IDs are generated in the HIPAA PM. This appendix contains the following topics:

Transaction Set and Unique Source IDs

By default, an externally assigned unique ID of the **BizResponseCorrelationKey** generated from the **UniqueIDHandler** Business Process (BP) is now composed of (ends with) a value from the **Unique ID Source** field for the corresponding HIPAA transaction set (2000 Addenda or Standard), as listed in Table A–1.

TABLE A–1 Unique ID Source Field for Corresponding HIPAA Transaction Set

HIPAA Transaction Set ID	Unique ID Source
837	BHT03
835	TRN02
834	BGN02
820	TRN02
278	BHT03
277	2000E.2200E.TRN02
276	2000E.2200E.TRN02
271	BHT03
270	BHT03

Additional Information

The following list provides additional important information about using the externally assigned unique IDs:

- You may change an externally assigned ID's composition by opening the **UniqueIDHandler** BPEL and modifying the assignment to

  ```
  /ExStdEvent/Container[1]/KeysSection/CorrelationKeys/BizResponseCorrelationKey
  ```
  .
- The full composition of **BizResponseCorrelationKey** in the **UniqueIDHandler** is:
- For a request message:

  ```
  <ExTradingPartnerGUID>|<BusinessProtocolName>|
  <BusinessTransactionIdentifier>|<UniqueID Source>
  ```
- For a response message:

  ```
  <ExTradingPartnerGUID>|<BusinessProtocolName>|
  <ProtocolRespondToMessageID>|<UniqueID Source>
  ```

◆ ◆ ◆ APPENDIX B

Configuration Worksheets

This appendix provides a task list and a data sheet that you could use to create, run and monitor a project that uses the HIPAA PM.

Task list and Data Sheet

Task list

This is list of all the tasks that needs to be performed to create, run and monitor a project.

- Prerequisite setup tasks:
  - Ensure external systems are installed and available.
  - Install the product `.sar` files (if not already done)
  - Create and start logical host domains (if not already done)
  - Download and run Oracle scripts (if not already done)
- Enterprise Designer tasks:
  - Create (or import) environments, and then configure them
  - Create and build B2B Host projects
  - Start logical hosts (if not already done)
  - Build and deploy GUI and Error projects
  - Create validation Connectivity Map, and then build and deploy eXchange deployment
  - Customize sample project components, and then build and deploy samples
- ePM tasks:
  - Start ePM
  - Import (or create) hosts and TPs
  - Configure or customize hosts and TPs as needed

- Run-time tasks:
  - Feed input data (i.e., run the projects)
  - Verify output data
  - Track messages

Data Sheet

Fill in the data sheet and use the completed data sheet when you start working on the project.

TABLE B–1 Configuration Parameters for Oracle Database and Connections

Parameter	Value
Server Name:	
Port Number:	
Database Name:	
User:	
Password:	

TABLE B–2 Configuration Parameters for LDAP Connection

Server Name:	
User ID:	
Password:	
Port Number:	
Base DN:	
Provider URL:	

TABLE B–3 Port Numbers

Repository	
Enterprise Manager	
Integration Server	
IQ Manager	

TABLE B–4 Paths and Filenames of Data Files That Are Read

Path	
Filenames	

TABLE B–5 Paths and Filenames of Data Files That Are Written

Path	
Filenames	

Glossary

AD, *AD, xAD In eXchange an Attributes Definition defines the metadata attributes of parameters used in a business protocol, delivery protocol, or transport. Examples of xADs include: BPAD=BAD+EAD; DPAD=MAD+PAD; and TAD.

AS2 Applicability Statement 2 (AS2) is an Internet Draft security standard defined by the IETF (Internet Engineering Task Force), designed to allow business transactions to move securely over the Internet.

B2B Business-to-business (B2B) interactions are those that occur between business partners in the context of e-commerce.

BAD In eXchange, Business Attribute Definitions (BADs) define the metadata attributes of message payload parameters used in business protocols such as X12, HIPAA, EDIFACT, or CIDX. Each BAD combines with one EAD to constitute a BPAD.

BPAD In eXchange, Business Protocol Attribute Definitions (BPADs) define metadata for business protocols such as X12, HIPAA, EDIFACT, or CIDX. A BPAD consists of one Business Attributes Definition (BAD) and one Enveloping Attributes Definition (EAD).

CAPS The Sun Java Composite Application Platform Suite (Java CAPS) includes eGate Integrator, eInsight Business Process Manager eXchange Integrator, eWay Intelligent Adapters, OTD Libraries, and Protocol Managers, as well as many other products.

CIDX The Chemical Industry Data Exchange (CIDX) is a non-profit organization dedicated to improving the ease, speed and cost of securely conducting business electronically in the chemical industry. CIDX focuses on the development of eBusiness standards, called Chem eStandards.

DPAD In eXchange, Delivery Protocol Attribute Definitions (DPADs) define metadata for delivery protocols such as AS2, ebXML, or RNIF. A DPAD consists of one Messaging Attributes Definition (MAD) and one Packaging Attributes Definition (PAD).

EAD In eXchange, Enveloping Attribute Definitions (EADs) define the metadata attributes of message envelope parameters used in business protocols such as X12, HIPAA, EDIFACT, or CIDX. Each EAD combines with one BAD to constitute a BPAD.

ebXML A well-recognized e-business XML (extensible markup language; see "XML") whose implementation includes specifications for messaging, collaboration profiles, business processes, and metadata registry.

ePM eXchange Partner Manager (ePM) is a Web-based GUI for defining and managing Trading Partner (TP) information.

FTP	File Transport Protocol (FTP) is a transport protocol for sending and receiving files. Specifications for FTP include RFCs 959, 1635, 2228, and 2577.
HTTP	Hypertext Transport Protocol (HTTP) is a transport protocol for transmitting information referenced in a URL of the form http://<hostname>:<port>/.../.... Specifications for HTTP include RFCs 2068, 2616, 2617, 2660, and 3310.
ICAN	Before Java CAPS 5.1.x, SeeBeyond offered an Integrated Composite Application Network (ICAN) Suite that included eGate Integrator, eXchange Integrator, various eWay Intelligent Adapters, OTD Libraries, and Protocol Manager Composite Applications, as well as many other products.
LDAP	The Lightweight Directory Access Protocol is a standard networking protocol for querying and modifying information stored as a distributed nonrelational database in directory servers (informally called "LDAP servers") accessed through TCP/IP. Specifications for LDAP include RFCs 1777-1779 and 2251-2255.
MAD	In eXchange, Messaging Attribute Definitions (MADs) define the metadata attributes of messaging parameters used in delivery protocols such as AS2, ebXML, or RNIF. Each MAD combines with one PAD to constitute a DPAD.
MIME	Multipurpose Internet Mail Extensions (MIME) extends the format of basic Internet mail to allow non-textual messages, multipart message bodies, and so forth. Specifications for MIME include RFCs 2045–2049.
OTD	In Java CAPS, an Object Type Definition (OTD) contains the data structure and rules that define an object. OTDs are used in Java collaborations to transform data interface with external systems.
PAD	In eXchange, Packaging Attribute Definitions (PADs) define the metadata attributes of packaging parameters used in delivery protocols such as AS2, ebXML, or RNIF. Each PAD combines with one MAD to constitute a DPAD.
RNIF	The purpose of the RosettaNet Implementation Framework (RNIF) is to allow trading partners to configure their business processes in such a way as to operate with other trading partners adhering to the same framework, allowing electronic business transactions to be conducted securely over the Internet.
S/MIME	Secure/Multipurpose Internet Mail Extensions (S/MIME) provides a consistent way to send and receive secure MIME data, using digital signatures for authentication, message integrity and non-repudiation and encryption for privacy and data security. Specifications for S/MIME version 2 include RFCs 2311–2315.
SME	In Java CAPS, Secure Messaging Exchange (SME) uses advanced cryptographic techniques to ensure security, verifiability, and nonrepudiation of messages exchanged electronically.
SMTP	Simple Mail Transfer Protocol (SMTP) is a transport protocol for transmitting e-mail messages between servers or from client to server. Specifications for SMTP include RFCs 1651, 2821, and 3461.
TAD	In eXchange, Transport Attribute Definitions (TADs) define the metadata attributes of parameters used in transport protocols such as FTP or HTTP.
TCP/IP	The Transmission Control Protocol/Internet Protocol is a standard suite of communication protocols for connecting hosts and transmitting data over the Internet.

TP, TPP	In eXchange, a Trading Partner (TP) has one or more Trading Partner Profiles (TPPs) that contain information identifying the values of messaging, enveloping, and/or transport parameters to be used for sending and receiving B2B information.
URL	A Uniform Resource Locator (URL) is a string that identifies information, such as a particular piece of information shared by a particular host.
XML	An Extensible Markup Language (XML) is a language whose syntax obeys an official schema, called “the XML schema”, but whose semantics (“vocabulary”) are open.

Index

F

G

H

I

J

L

M

O

P

Q

R

S

T

U

V

X