# Installation Guide

*iPlanet Trustbase Payment Services*

**Version 2.0 Beta**

# List of Figures

# Contents

# Introduction

The following chapter discusses all related documents to this guide.

# Overall Layout

The complete documentation set for iPlanet Trustbase Payment Services comprises of:

Installation Guide (This document) that explains how to install iPlanet Trustbase Payment Services and all its associated components.

System Administration Guide that explains how to configure and run iPlanet Trustbase Payment Services. It further illustrates how to make payments.

Developer and Integration Guide that provides a comprehensive example of how to deploy your own CPI application and how to integrate with your existing back end banking system.

The manual Covers:

- Introduction to Payment Initiation

- Installing iPlanet Trustbase Payment Services

- Installing The Reference Tools: Bank in a Box, Tooled Up, Buyers Bank, Condition Management, Obligation Management and CPI

- Detailed documentation can also be found on the iPlanet Trustbase Payment Services Website at

```
http://docs.sun.com/?p=prod/s1.iptbpayment
```

```
http://docs.iplanet.com/docs/manuals/itps.html
```

# Related Documents

The following documents are considered pre-requisites to installing iPlanet Trustbase Payment Services (iTPS)

- Eleanor . iTPS is based on the Eleanor Technical Specification and as such you need to have familiarised yourself with this document.

  `http://www.identrus.com`

  Eleanor Scheme Technical Specification Version 1.0b

  Eleanor Scheme Operating Rules

  Eleanor Scheme Product Guide

  Note This Website requires a Username and password that should have been given to you when you joined the Identrus Scheme

- Identrus Message Specifications. iTPS is based on the IDentrus four corner model and as such four servers configures as identrus Transaction Coordinators (TC) using iPlanet Trustbase Transaction manager (iTTM) are assumed to be up and running. See `http://www.identrus.com`

  Identrus PKI Compliance (IT-PKI)

  Transaction Coordinator requirements (IT-TCFUNC)

  Identrus Smart Card Signing Interface Requirements (IT-SIR, ver 1.7)

  Core messaging specification (IT-TCMPD)

  Certificate Status Check Messaging specification (IT-TCCSC)

  Identrus Digital Signature Messaging System Specification (IT-DSMSSP, ver 2.0).

  Transaction Coordinator Certificate Status Check (CSC) Protocol Definition (IT-TCCSC, ver 2.0b)

  Note In order to access the documents within this website you need a Username and password that should have been given to you when you joined the Identrus Scheme.

- iPlanet Trustbase Transaction Manager (iTTM) documentation itself can be found below:

  http://docs.sun.com/?p=prod/s1.iptbtranm

  http://docs.iplanet.com/docs/manuals/trustbase.html

  or in /cdrom/cdrom0

# Software Requirements

Solaris(TM) 8 for SPARC(TM)

JDK 1.3.1

iPlanet Web Server 6.0 SP2

iPlanet Application Server 6.5

iPlanet Trustbase(TM) Transaction Manager 3.0.1

iMQ for Java 2.0

Oracle 8.1.7

Certificate Authority [e.g. iPlanet Certificate Management System 4.2]

Optional Hardware Security Module (HSM) on server [mandatory for Identrus participation - nCipher nShield 300 SCSI]

GemSAFE IS 1.1 for Identrus System 16000 Smartcards are configured on Buyer PC for use with Tooledup Seller Website.

# Hardware requirements

## Memory

Recommended single machine setup 512 MB

## Disk Space

Recommended single machine setup 1 GB

# Target Audience

System Administrators and Application Developers within the banking profession.

# Recommended Installation Template

Before attempting an installation you should prepare a template outlining all your proposed settings. The following table provides the setting used throughout the documentation

# iTTM 3.0.1

Do you agree to the license terms? [No]: Yes

Install location [/opt/ittm]: /opt/ittm

The user that will start iTTM ? tbase

The group that this user belongs to ? iplanet

The root location of iPlanet Application Server ? /opt/ias6

The root location of iPlanet Web Server documents directory? /opt/iws6/docs

What is the database user name that is used by iTTM? tbase

What is the database password that is used by iTTM? tbase

On what host is your database stored? mydatabase.mycompany.com

On what port is your database running? 1521

On what SID is your database? orcl

On what URL is your local OCSP responder?
http://myresponder.mycompany.com:8080/NASApp/OCSPResponder/OCSPResponderServlet

What is the AIA of this iTTM? https://myhost.mycompany.com

Enter the password to use for the tokenkeystore? password

## OCSPResponder

What is the Base DN of the LDAP Server that stores your certificate revocation list?

What is the Bind DN of the LDAP server that stores your certificate revocation list?

What is the Bind password?password

On what host is your LDAP? myhost.mycompany.com

On what port is your LDAP? 387

## JMSProxy

What Port is your ittm listening on? 80

On what host is your iTTM iPlanet Web Server ? [ myhost.uk.sun.com ]

On what HTTP port is your iTTM iPlanet Webserver running ? [ 80 ]

The JMS queue name for messages received from system backend ? [ backend_to_itps ]

The JMS queue server host ? [ myqueue.uk.sun.com ] { myqueue.mycompany.com }

The JMS queue server port ? [ 7676 ]

# iTTM certificates Aliases

(1) Location of alias = "IRCA" certificate e.g. "CN=Identrus Root,OU=Identrus Root,O=Identrus,C=US"

(2) Location of alias = "L1CA" certificate e.g. "CN=L1 Bank CA,OU=L1 Bank,O=L1,C=GB"

(3) Request/response for alias= "L1EESC" certificate e.g. "CN=L1 Bank End Entity Signing Certificate,OU=L1 Bank,O=L1"

(4) Request/response for alias= "L1EESSL" certificate e.g. "CN=L1 Bank SSL CertificateCertificate,OU=L1 Bank,O=L1"

(5) Request/response for alias= "L1IPSC" certificate e.g. "CN=L1 Bank Inter-Participant Signing Certificate,OU=L1 Bank,O=L1"

# iTPS 2.0

[0] Install location : /opt/ittm

[1] The user that will run iTTM? tbase

[2] The group that this user belongs to? iplanet

[3] JMS queue name for messages to Biab Backend ? itps_to_backend

[4] Asynchronous acknowledgment SMTP host smtp.mycompany.com

[5] Default "From:" email address for acknowledgments admin@mycompany.com

# iTPS Component Certificate Aliases

Trusted Root Certificate (e.g. IRCA).

Level One Certificate Authority Certificate. (e.g. L1CA)

End Entity Signing Certificate ( e.g. ClientSC) The AIA field within this certificate is used to determine the destination for the payments message)

SSL Client Transaction Certificate ( e.g. ClientSSL)

SSL Server Certificate (This name is enforced by the Web Server Server-Cert)

# BFI

[0] Installation Location /opt/itps-bfi

[1] The user that will run BFI? tbase

[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-bfi-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA ]

[11] The database user is [ tbase ]

[12] The database password is [ tbase ]

[13] The database host is [ mydatabase.mycompany.com ]

[14] The database port is [ 1521 ]

[15] The database sid is [ orcl ]

# BIAB

[0] Installation Location /opt/itps-biab

[1] The user that will run BIAB? tbase
[2] The group that this user belongs to? iplanet

[3] The Web Server location is [ /opt/iws6 ]

[4] The Web Server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-biab-deploy ]

[7] The queue driver location is [ /opt/SUNWjmq/lib/jmq.jar ]

[8] The from itps queue name [ itps_to_backend ]

[9] The too itps queue name [ backend_to_itps ]

[10] The queue server host [ myqueue.mycompany.com ]

[11] The queue server port [ 7676 ]

[12] The database user is [ tbase ]

[13] The database password is [ tbase ]

[14] The database host is [ mydatabase.mycompany.com ]

[15] The database port is [ 1521 ]

[16] The database sid is [ orcl ]

# CPI

[0] Installation Location /opt/itps-cpi

[1] The user that will run CPI? tbase
[2] The group that this user belongs to? iplanet

# CPI Certificate Aliases

"IRCA" certificate e.g. "CN=Identrus Root,OU=Identrus Root,O=Identrus,C=US"

"L1CA" certificate e.g. "CN=L1 Bank CA,OU=L1 Bank,O=L1,C=GB"

"BuyerSC" certificate e.g. "CN=Buyer SC, OU=L1 Bank, O=L1"

"SellerSC" certificate e.g. "CN=Seller SC, OU=L1 Bank, O=L1"

# Tooledup

[0] Installation Location /opt/itps-tdup

[1] The user that will run TooledUp? tbase
[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-tdup-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA]

[11] The database user is [ tbase ]

[12] The database password is [ tbase ]

[13] The database host is [ mydatabase.mycompany.com ]

[14] The database port is [ 1521 ]

[15] The database sid is [ orcl ]

# Obligation Management

[0] Installation Location /opt/itps-om

[1] The user that will run om? tbase
[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-om-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA]

# Condition Management

[0] Installation Location /opt/itps-cond

[1] The user that will run Cond? tbase
[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-cond-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA ]

[11] The absolute path of the temporary directory for file downloads [/opt/temp]

Recommended Installation Template

# Introduction to Payment Initiation

This chapter provides an overview of iPlanet Trustbase Payment Services. It discusses a payment initiation model that is based upon the Identrus framework. It is a set of open specifications that allow the Banks and customer vendors to support implementation of an open network based Payment initiation solution. The chapter looks at some of the key features that go into making payments over an open network such as the Internet. It provides an overview of:

- Payment Initiation Products

- Payment Initiation Schemes

- Payment Initiation Processing Models

- Payment Initiation Reference Components of iPlanet Trustbase Payment Services

# Payment Products

Every Payment Scheme includes a number of payment products. Each product has a particular set of features that are made up of a sequence of messages sent between the Buyer, Seller, Seller's Financial Institution and Buyer's Financial Institution.

## Kinds of Payment products

iTPS supports the following Payment products, product codes are expressed in brackets:

- Payment Order (xPx)

- Certified Payment Obligation (xPC)

- Payment Obligation (xPO)

- Conditional Payment Order (CPx)

- Conditional Payment Obligation (CPO)

- Certified Conditional Payment Obligation (CPC)

You need to consult your Payment Scheme specification for more details about which kinds of Payment products are supported by iPlanet Trustbase Payment Services (iTPS). These products are initiated using the iTPS Tooledup Website and Managed using the iTPS Condition and Obligation Management Websites. We now define them in turn

### Payment Order (xPx)

A Payment order is a revocable, unconditional electronic instruction from the Buyer requesting the Buyer's Bank to execute a credit payment to the Seller on a specific date for a specified amount.

### Certified Payment Obligation (xPC)

Where an Assured Payment is used, the Buyer requests the Buyer's Bank to underwrite (or assure) the payment to the Seller.

### Payment Obligation (xPO)

The commitment from a Buyer to pay a Seller a specified amount on a specified date. There is no obligation on the Buyers Financial Institution to pay if there are insufficient funds available on the due date. The instruction is only revocable bilaterally, i.e. with the assent of the current Holder of the obligation. This product is only supported in the SFI Model, although it will be possible to build it into a procurement application using the CPI library.

### Conditional Payment Order (CPx)

The Conditional Payment Order has the same core characteristics as the Payment Order product with the additional requirement that payment will not be released until evidence that all conditions attached to the payment have been met or waived. This product is also unilaterally revocable by the Buyer.

### Conditional Payment Obligation (CPO)

The Conditional Payment Obligation has the same core characteristics as the payment Obligation product, with the additional requirement that payment will not be released until evidence that all conditions attached to the payment have been met or waived. As with the Payment Obligation, the Buyers Financial institution is not obliged to make the payment if, for instance, there are insufficient funds available in the Buyers account, and the product is bilaterally revocable.

### Certified Conditional Payment Obligation (CPC)

This product has the same core characteristics as the Payment Obligation product, with the additional requirement that payment will not be released until evidence that all conditions attached to the payment have been met or waived. Since the Payment is certified the BFI is obliged to make the payment since the Buyer requests the Buyer's Bank to underwrite (or assure) the payment to the Seller.

# Payment Schemes

With the use of a payment scheme, a payment is secured by digitally signing payment instructions, providing authentication, message integrity, non-repudiation and confidentiality. The payment is efficient because parties have pre-established instructions with their banks for payment authorisation, routing and settlement that enables the Buyer to initiate a payment on-line, simultaneously with the purchase transaction, instead of through a separate, off-line step. Additional efficiencies are created through standardised payment processing procedures at the banks. In the case where the Seller requires assurance of payment, the Buyer can electronically request its bank, when initiating payment, to assume the responsibility to pay the Seller. This model does not create a new interbank payment system. It is a new channel or front end to initiate payments on existing, back office payment system.

In the early stages iPlanet Trustbase Payment Services will be supporting one kind of scheme:

## Eleanor

You need to consult your Eleanor Documentation as to what payment products will be supported by this scheme.

# Payment Processing Models

Depending on the particular e-commerce application different Payment Initiation models may apply. iPlanet Trustbase Payment Services supports the following Payment Initiation models.

## Buyer to Buyer's Financial Institution

This is where the Buyer initiates a payment directly via the buyers bank. This is also referred to, within The Eleanor Payment Initiation Scheme as the Buyer's Financial Institution Model (BFIM)

## Identrus Four Corner Model

The Identrus Four Corner model is utilised to provide enhanced payment initiation services to buyers and sellers. Two trading parties with no previous trading relationship can complete an online purchase or trade and simultaneously arrange for a secure, efficient and, optionally, bank certified payment because there exists the Identrus trust model, which contains pre-established banking relationships between businesses and their respective banks. This is also referred to, within The Eleanor Payment Initiation Scheme as the Sellers Financial Institution Model (SFIM)

The "Four Corner" model, as depicted below, forms the basis of the Identrus PKI network.

**Figure  1-1**    Identrus Four-Corner Model
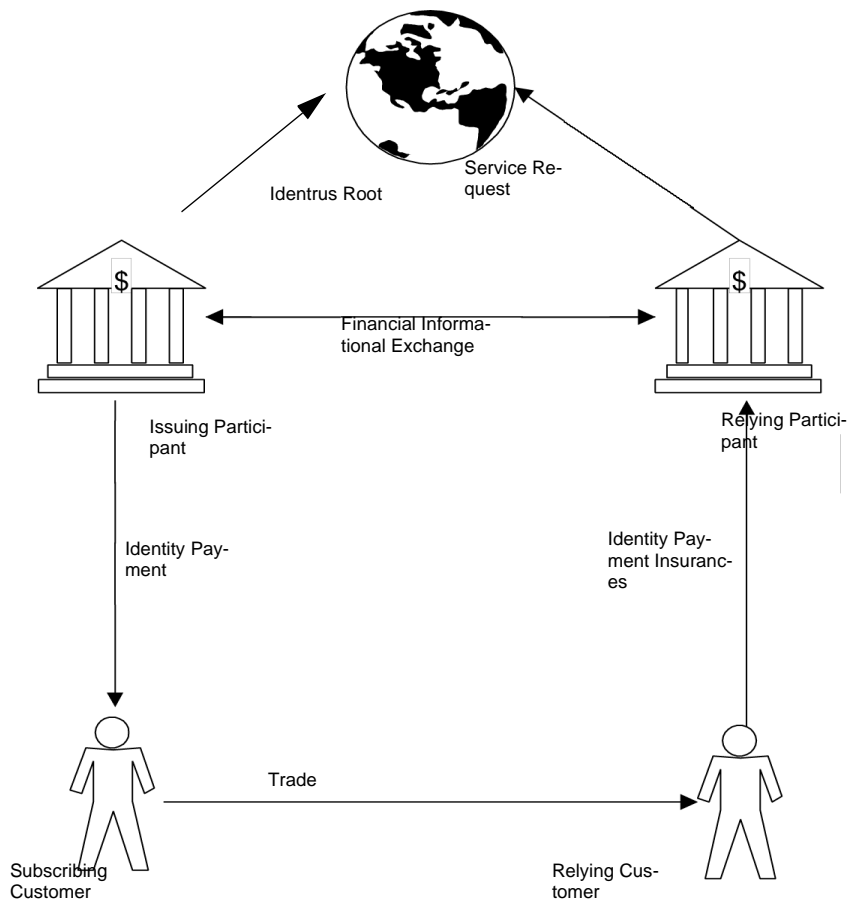
# Four Corner Payment Processing

Both the Buyer's Bank and the Seller's Bank needs to be Identrus scheme members. Both the Buyer and the Seller also need to be Identrus enabled by their banks. Within the Eleanor Scheme this is referred to as SFIM

**Figure 1-2**     Four Corner Payment Model (SFIM)
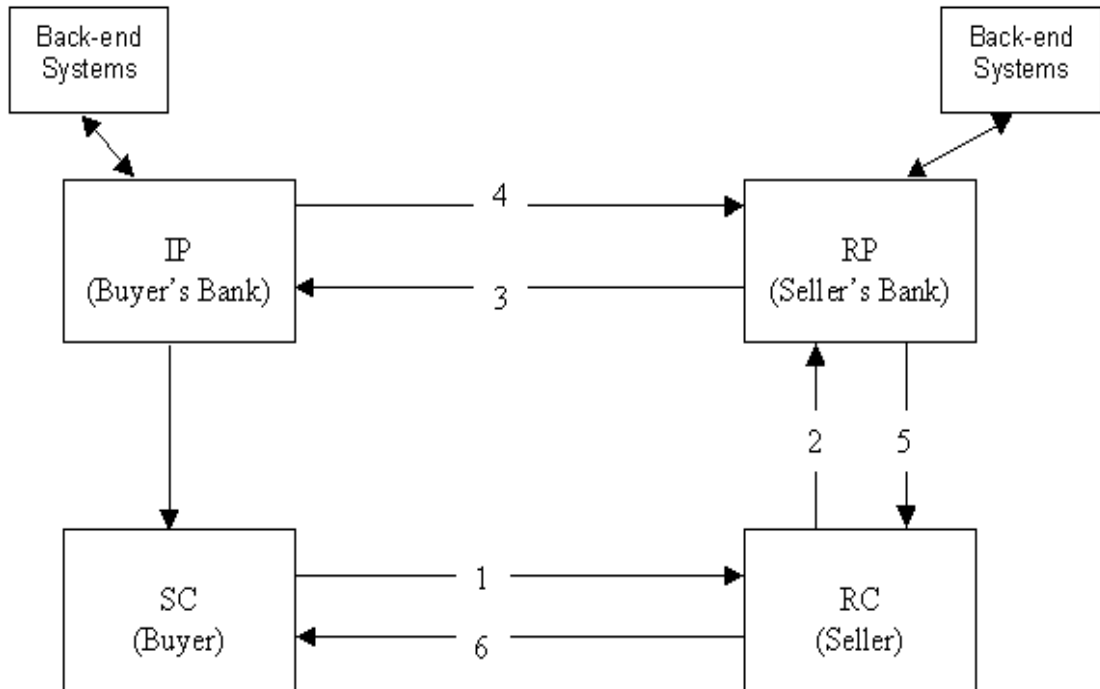


The message flow is as follows:

1. Buyer sends signed payment information to Seller

   a. The Buyer contacts the seller, and places an order.

   b. The Seller provides some payment information for the Buyer to sign with its certificate, which has been supplied by its Identrus bank (Buyer's Bank)

   c. Buyer signs payment information and sends to the Seller.

2. Seller sends message to Seller's Bank

   a. Seller verifies buyer signature.

   b. Seller creates the product (i.e. Payment Order) selected by the communication between itself and the buyer.

   c. Seller signs the Payment Order message with its certificate, supplied by its Identrus bank.

   d. Sends the message to its bank.

3. Seller's Bank sends message to the Buyer's Bank

   a. Seller's Bank verifies certificate and signature of seller's message.

   b. Seller's Bank informs its legacy systems of the received message.

   c. Seller's Bank finds the location of Buyer's Bank from the Buyer's certificate.

   d. Sends message to the Buyer's Bank.

4. Buyer's Bank sends message to the Seller's Bank

   a. Buyer's Bank verifies the Seller's Bank signature and certificate.

   b. Buyer's Bank verifies the Buyer's signature and certificate and also its authority.

   c. Buyer's Bank informs its legacy systems of the received message.

   d. Sends the appropriate response back to the Seller's Bank

5. Seller's Bank sends response to the Seller

   a. Seller's Bank verifies the Buyer's Bank signature and certificate

   b. Seller's Bank informs its legacy systems of the received response.

   c. Re-signs response

   d. Sends response back to the Seller.

6. Seller informs Buyer of result.

   a. Seller verifies the signature and certificate of its bank

   b. Sends the results of the response message back to the Buyer.

# Three Corner Payment Processing

The Three-Corner Model (3CM) is a special case of the SFIM where the Buyer and Seller accounts are held at the same bank. The Buyer's Bank needs to be an Identrus scheme member. Both the Buyer and the Seller needs to be Identrus enabled by their bank.

**Figure  1-3**     Three Corner Payment Overview
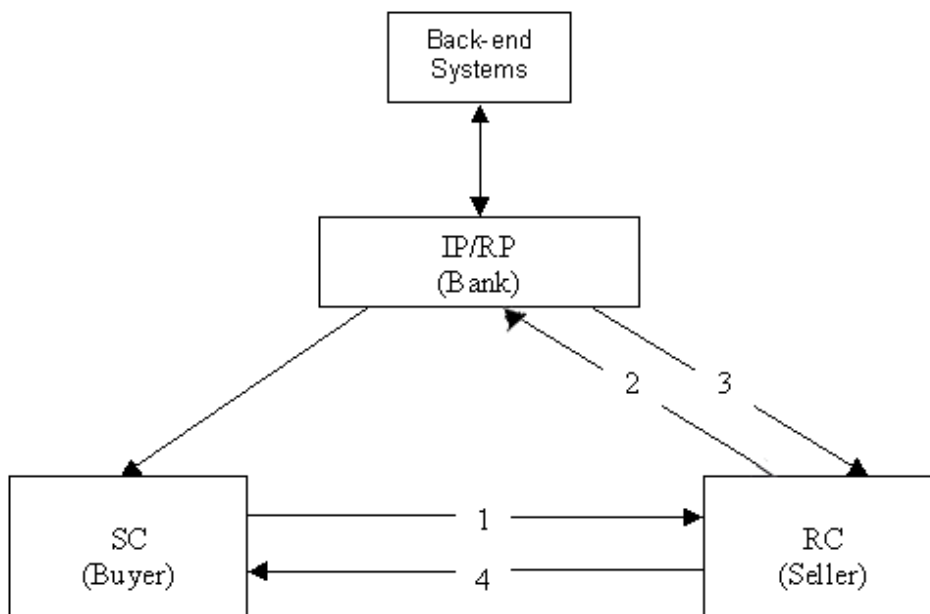


The message flow is as follows:

**1.**   Buyer sends signed payment information to Seller

    **a.**   The Buyer contacts the Seller, and places an order.

    **b.**   The Seller provides some payment information for the buyer to sign with his/her certificate, which has been supplied by its Identrus bank (Buyer's Bank)

    **c.**   Buyer signs payment information and sends to the Seller.

**2.**  Seller sends message to the Bank

    **a.**   Seller verifies buyer signature.

    **b.**   Seller creates the product (i.e. Payment Order) selected by the communication between itself and the buyer.

    **c.**   Seller signs the Payment Order message with its certificate, supplied by its Identrus bank.

    **d.**   Sends the message to its bank.

**3.**  Bank sends response to the Seller

    **a.**   Bank verifies certificate and signature of seller's message.

    **b.**   Bank verifies the Buyer's signature and certificate and also its authority.

    **c.**   Bank informs its legacy systems of the received message.

    **d.**   Sends response back to the Seller.

**4.**  Seller informs Buyer of result.

    **a.**   Seller verifies the signature and certificate of its bank

    **b.**   Sends the results of the response message back to the Buyer.

---

**NOTE**    More Information about how each payment scheme defines its Models and Payment products can be found at http://www.identrus.com

            Examples of supported Schemes include:

            Eleanor Payment Reference Specification

---

# Payment Reference Components

In order to initiate a payment around a banking system a number of components are required. The iPlanet Trustbase Payment Services are made up of the following components:

## iPlanet Trustbase Payment Services

This comprises of a set of services that are configured within iPlanet Trustbase Transaction Manager and acts as the main banking server to route Payment Messages.

## Bank in a Box Back End

Bank in a Box package allows you to test interfacing with legacy systems.

## Bank in a Box Admin Tool

In addition to the Back End there is an Admin tool that provides a web interface to the Bank in a Box Back End.

## The Seller's Website: Tooled Up (SFIM)

This is an example application, in conjunction with the supplied Corporate Payment Initiation Library (CPI) API, that demonstrates how a customer can purchase goods and services through a vendor website that initiates a payment instruction, coupled with the ability to view and cancel a history of payment instructions

## Buyers Website (BFIM)

This example, in conjunction with the supplied Corporate Payment Initiation Library (CPI) API, enables a buyer to initiate and cancel payment instructions directly with its bank. This is used when the buyer runs procurement systems or the seller is not a member of the Payment scheme.

# Corporate Payment Initiation Library (CPI) API

The Corporate Payment Initiator (CPI) Library API is a Java library providing Eleanor messaging and associated services.

# Condition Management

This appears as a separate website and is used to hold Payments in a Registry until all conditions have been met.

# Obligation Management

This occurs when Payments are transferred from one institution to another. Under such circumstances a website is needed to manage payment transfers within a Registry until they are complete.

# Architectural Overview

The product comprises of a number of distinct components. Each of these components has a distinct set of interfaces that may be categorised as public or private. Every bank implements both the Buyer's Bank and Seller's Bank roles. There is no concept of a separate deliverable for Buyer's Bank and Seller's Bank. The following table identifies the classification of each of the product components. This is necessary as some of the delivered components are not intended for use in an operational environment These components are however required for the Eleanor Reference Application (ERA) contract signed with Identrus, and will be delivered to provide customers with a 'working' payments initiation solution for internal and interoperability testing.

| Component | Category | Installation Directory |
|---|---|---|
| iWS 6.0 SP2 and iAS 6.5 | Standard product | /opt/iws6 and /opt/ias6 |
| ITTM 3.0.1 | Standard product | /opt/ittm |
| ITPS 2.0 Core services | Private | /opt/ittm |
| IMQ for Java 2.0 | Standard product | /opt/SUNWjmq |
| JMS Proxy | Private | /opt/ittm |
| Bank in a Box Back End | Public | /opt/itps-biab |
| Bank in a Box Admin Tool | Public | /opt/itps-biab |
| Condition Management Web site | Public | /opt/itps-cond |
| BFI web site | Public | /opt/itps-bfi |
| Obligation Management web site | Public | /opt/itps-om |
| CPI | Private | /opt/itps-cpi |

The categories are:

- Standard product – Provided as another product
- Private – Supplied with no ability to directly extend

- Public – Supplied as either source code or the ability to extend programmatically

Only private components are licensed for use in production environments. The diagram below illustrates how the components fit together for both the buyer and buyers bank (blocks on the left) and the seller and the sellers bank (blocks on the right).

**Figure 1-4** Architectural Overview
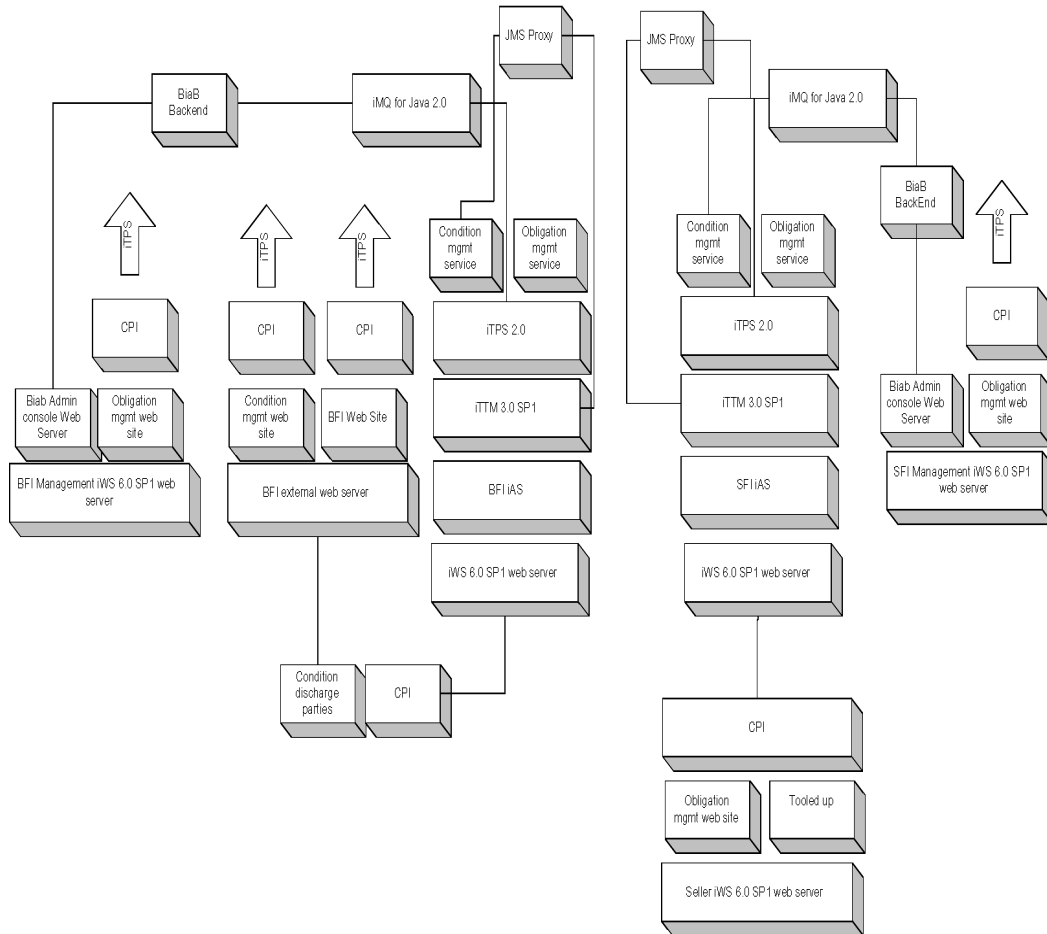
# Installation

The following chapter outlines the installation procedures for the various components.

# Installation Overview

The diagram below illustrates how the various components are related to each other, and the message paths between each component. In order to have a fully functional system all of these components require installation and configuration.

**Figure 2-1**     Installation Overview
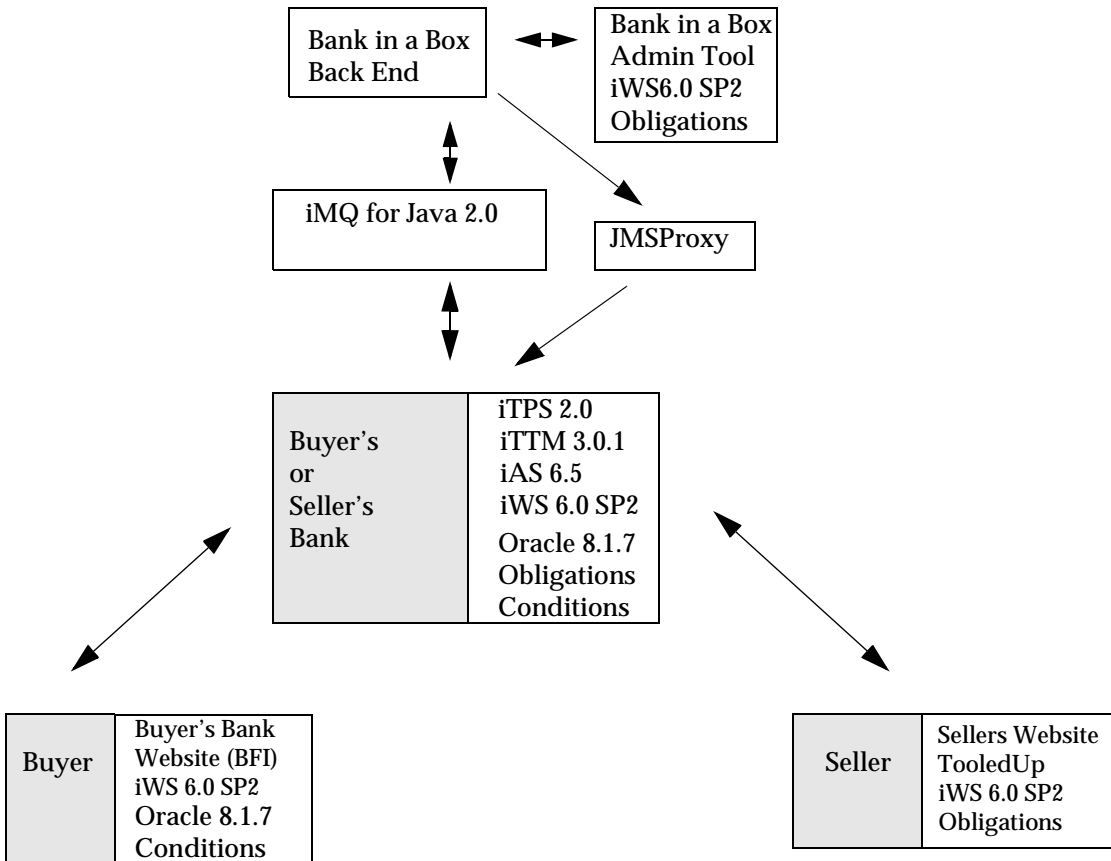
# Installation Script

.The following table summarises the kind of installations that are possible.

| Product Components | ? | Considerations |
|---|---|---|
| iTTM separated from iAS | Not Possible | If iAS and iWS are installed on separate machines make sure iTTM is installed with iAS |
| iWS separated from iAS | Yes | See Section on Configurator Plug-in `http://docs.iplanet.com/docs/manuals/ias.html` and also the section on webless installs<br><br>http://docs.sun.com/source/816-5788-10/app1.htm#13421<br><br>The webserver's documents directory must be made accessible by the iTTM installer. This accessibility only needs to be present when the installer is functioning ( ie it will need to be re-instated during upgrade or silent installs ). |
| Oracle separated from iTTM | Yes | See iTTM Installation manual<br><br>http://docs.sun.com/source/816-6283-10/index.html |
| HSM separate from iTTM | No | We do not support HSM's with iTPS components on separate machines |
| SSL Proxy separated from iTTM | Yes | See iTTM Installation manual<br><br>http://docs.sun.com/source/816-6283-10/index.html |
| SMTP Proxy separated from iTTM | Yes | See iTTM Installation manual<br><br>http://docs.sun.com/source/816-6283-10/index.html |
| iAS with other Web Servers | No | Not supported |
| iTPS components separate from iTTM | Yes | |
| iTTM separate from iTPS | No | Not possible |
| iTPS components using different Oracle Users | Yes | Different Usernames are allowed for each component. However, you may need to copy all SQL scripts to the local machine and install to each new username. |
| iTPS components using the same iWS Web Server Instance | No | New Web Server instances must be created for each iTPS component that is installed on the same machine. |

For instance, although it is not necessary to install the components on individual machines the "Installation Overview," on page 42 however can be used for testing purposes. Other configurations may be possible

For instance, each machine acting as both a buyer and sellers bank. There are a number of main steps that need to be applied appropriately to the four machines labeled Machine A - Machine D in the figure "Installation Overview," on page 42. It is recommended that the page is copied or detached to assist you install and cross-reference the install sections.

1. Install Sun Software

    a. The Solaris 8 Operating System that should have already been supplied to you by separate CDROM

    b. The JDK 1.3.1 java programming language should be downloaded from http://www.javasoft.com

    c. The iPlanet Certificate Management System or any other third party PKI identrus compliant software. For instance,

       http://www.iplanet.com/products/iplanet_certificate/home_certificate.html

    d. The iPlanet Messaging Server or any other Corporate Mail Server. For instance,

       http://www.iplanet.com/products/iplanet_messaging/home_iplanet_messaging.html

2. Install the pre-requisite third party software

    a. An Oracle 8.1.7 database must be installed and available for use by all of the machines running in the iTPS installation. An Oracle database may be installed on each node in the system, a single node in the system, or an independent node that is accessed by each of the machines.

    b. Install an Identrus compliant PKI. This must include an appropriate Validation Authority component and be capable of supporting the Identrus Certificate Status Check protocol.

    c. Install an nCipher HSM on each machine in order to perform cryptographic operations

3. Install the base components for the Buyer and Seller's banks

   a. Install the iTTM 3.0.1 on all Machines.

   b. Install, if you have not already installed with iTTM, the iMQ for Java 2.0 and its patch on all Machines.

   c. Install the iWS 6.0 SP2 for the Bank in a Box administration tools on all machines.

   d. Mail Server availability

4. Install the components that make up the Payments Services product

   a. Install the iTPS 2.0

   b. Configure JMSProxy that was installed with iTTM

   c. Install the Bank in a Box (BiaB) back office simulator

   d. Install the Bank in a Box (BiaB) administrator tool

   e. Condition Management Website

   f. Obligation Management Website

5. Install the Buyer and seller web site components

   a. Install the iWS 6.0 SP2 on both machines

   b. Install the Buyers Bank Website (BFI)

   c. Install the Sellers Bank Website (Tooledup demonstrator)

6. Optionally install the CPI library for use in developing applications (See the iPlanet Trustbase Payment Services Developer Guide for details on how to install this).

# Assumptions

1. The '\' is used to indicate a line continuation

2. The following default installation locations will be used

   a. iws6: /opt/iws6

   b. ias6: /opt/ias6

3. Before using the install scripts, ensure your terminal type is set to vt100 or vt220. For example:

   ```
   TERM=vt100;export TERM
   ```

4. The documentation assumes four machines for the install. You may however use less. Typically sellers and buyers banks appear on the same machine. In the examples illustrated in the next sections it is assumed that all sellers, buyers, sellers bank and buyers bank operate from one machine and the oracle host is on another as indicated below:

   a. Oracle host name mydatabase.mycompany.com

   b. iTPS machine name myhost.mycompany.com

5. You should be logged in as root to perform these installs

6. GemSAFE IS 1.1 for Identrus System 16000 Smartcards are configured on Buyer PC for use with Tooledup Seller Website.

7. When installing the iWS 6.0 SP2 make sure that you select the option that specifies an external JDK 1.3.1 that needs to either be downloaded from http://www.javasoft.com to /usr/java1.3

# Third Party Pre-requisites

## Availability

The CD supplied with the product contains all of the required components to install the system EXCEPT:

1. Oracle 8.1.7

2. An appropriate Certificate Authority

3. An appropriate OCSP responder

4. nCipher software

These will need to be acquired from the appropriate vendor, installed and configured, prior to installing any of the iPlanet Payments Services components.

## Oracle 8.17 requirements (step 1a)

Your Oracle 8.17 installation must be configured with a user capable of:

1. Creating tables

2. Updating tables

3. Dropping tables

4. Running SQL scripts to populate the database

When installing Oracle you will need to allocate sufficient space to the user. We would recommend the following:

- For every 1000 expected messages you will need a minimum of 20Mb of table space.

- The default block size should set to a minimum of 8k

You will be required to provide the details of the Oracle installation at various points during the installation. The information required will be:

1. Hostname - As appropriate

2. Port number - Default 1521

3. SID - Default ORCL

The Oracle instance must be available during the installation of the product as most components require the capability to log into the database using SqlPlus and populating tables from information supplied in SQL scripts.

The User should also be familiar with the chapter on Configuration Recovery in the iTTM Installation and Configuration manual

```
http://docs.sun.com/source/816-6283-10/index.html
```

or in

```
/cdrom/cdrom0
```

and also the datamodel described in the Systems Administration Guide

# PKI Requirements (step 1b)

Your software must be configured as PKI compliant with Identrus (See Identrus Document IT-PKI http://www.identrus.com ) including all Transaction Coordinator profiles.

It is expected that the RA, CA, and VA components are available during the installation as certain components require certificates to be issued.

You must have Identrus Compliant Certificates with the appropriate email extensions for email acknowledgements to work.

# nCipher requirements (step 1c)

The nCipher components are generally stand alone and little information is required about the nCipher components. It is however useful to know the port that the nCipher Hardserver is running on (Default is 9000) as this is required at some points during installation.

If using a native provider you do not need an Operator card, if however you are using a PKCS11 provider you do. It also requires the admin card to be present for the first Crypto operation and can then be removed. A three corner test would provide this first Crypto operation.

You should consult the iTTM Installation and Configuration Guide for details on this

# Smart Cards and Browsers (step 1d)

- A SmartCard, such as a credit card, which will be issued to you by a thirty party vendor. An Identrus compatible SmartCard is a mandatory requirement. iPlanet Trustbase Payment Services is currently compatible with the GemPlus SmartCards GemSAFE IS 16000. See
  `http://www.gemplus.com/app/banking/gemsafe_is_mkt.htm`

- A SmartCard Reader with browser plug-in, which will be issued to you by a third party vendor. An Identrus compatible SmartCard Reader is a mandatory requirement. iPlanet Trustbase Payment Services is currently compatible with the GemPlus Card Readers GemPC430 and GemPC410 see
  `http://www.gemplus.com/products/hardware/index.htm`

- GEMSafe Enterprise Workstation 1.0 software is compatible with iPlanet Trustbase Payment Services see
  `http://www.gemplus.com/products/software/gemsafe/index.html`

- The Netscape Navigator v4.75 and Internet Explorer 5.0. These should be configured automatically with the software that comes with your SmartCard and SmartCard Reader.

- The supported email client for asynchronous support for SMIME acknowledgements is Netscape Messenger 4.7 for Solaris.

- The Client browser is compatible with GemPlus SmartCard and iPlanet Trustbase Payment Services as such the following operating systems are supported: Windows NT 4.0 Service Pack 5 see
  `http://www.microsoft.com/ntserver/nts/downloads/recommended/sp5/allsp5.asp` or alternatively Windows 98 see
  `http://www.microsoft.com/Windows98/`

  `or Solaris 8`

# Buyer and Seller Bank base components

## iTTM 3.0.1 (step 2a)

Each Bank machine will need to have an iTTM installed and configured.

In order to install these components you will need to follow the instructions in the iTTM 3.0 SP1 installation guide found in

`/cdrom/cdrom0`

or

`http://docs.sun.com/source/816-6283-10/index.html`

The instructions in chapter 1 Pages 13-62 provide information on how to install the following:

1.  iWS 6.0 SP2

2.  iAS 6.5

3.  iTTM 3.0.1

Chapter 4 provides information on how to configure and check that the components are operational.

We assume that this is installed on

`/opt/ittm`

NOTE: All of the software for the above installation is included on the iTPS CD.

# iPlanet Message Queue for Java 2.0 (step 2b)

If you did not already do so when you installed iTTM, you will need to install iMQ for Java 2.0.

The iPlanet message Queue (iMQ) component provides a means for the iTPS and the Bank in a Box components to communicate with each other. This means that an iMQ installation must be performed on both the Buyers and Sellers bank machines.

iPlanet Message Queue for Java is shipped with iTPS and may be found in the iMQ2.0 sub directory on the CD.

```
/cdrom/cdrom0/imq2.0
```

## Installation

The iMQ installation uses the Solaris package mechanisms to install the software on the machine. Assuming that the supplied CD has been mounted on /cdrom then the following commands will install the software:

```
pkgadd -d /cdrom/cdrom0/imq2.0/imq2_0-pkgs
```

This will automatically install to

/opt/SUNWjmq

You will be asked a question during the installation. Unless you have specific installation requirements then by using the defaults provided you will install all of the iMQ packages.

These settings will fulfill all the iTPS iMQ requirements.

If you require further information then details of how to install iMQ 2.0 can be found in point 7 within the following document that requires vi or a text document to read:

```
http://docs.sun.com/db/prod/s1.ipmsgquj
```

```
http://docs.iplanet.com/docs/manuals/javamq/20/install.pdf
```

### Example installation and Configuration

```
bash-2.03# pkgadd -d /cdrom/cdrom0/imq2.0/imq2_0-pkgs

Select package(s) you wish to process (or 'all' to process all
packages). (default: all) [?,??,q]:

do you wish to run the jmqbroker so that jmqbroker will start
automatically at boot time? ? [y,n] y
```

## Installing iMQ for Java SP1 Patch

Once the iMQ is installed, install the SP1 patch. This process is documented in the file using a text editor, e.g:

```
vi /cdrom/cdrom0/imq2.0/SP1/111858-01/install.pdf
```

NOTE: The file has a .pdf extension but is a text file and may be read using the vi editor. Once the software has been installed on either the buyer or seller machine, perform the second installation before progressing to patch the iAS installation.

The command to install the patch is:

```
cd /cdrom/cdrom0/imq2.0/SP1/111858-01

./installpatch .
```

## Running iMQ for Java

After install, make sure jmq is run for the first time. Subsequent reboots will start the application automatically

```
/etc/init.d/jmq start
```

or if already running, it will tell you:

```
Starting /opt/SUNWjmq/bin/jmqbroker -bgnd -silent ... jmqbroker
is already running.
```

and to stop:

```
/etc/init.d/jmq stop
```

If it becomes necessary to clear out the contents of the queue then start the broker in the following way

```
/etc/init.d/jmq stop

/opt/SUNWjmq/bin/jmqbroker -reset store
```

## Configuring with iAS

The next step is to configure the iTTM/iAS instance to use the appropriate iMQ installation. This operation will need to be performed on both of the Buyer and Seller machines. Before performing this operation it is important to ensure that the iAS has been shut down., but slapd should still be running.

If the iTTM had been installed in '/opt/ittm' the commands would be:

```
/opt/ittm/Scripts/stoptbase

/opt/ittm/Scripts/stopias

/opt/ias6/slapd-myhost/stop-slapd

/opt/ias6/slapd-myhost/start-slapd
```

To configure iAS for use with iMQ, execute jmssetup. This must be performed as the root user. You will be asked several questions, now illustrated below:

```
bash-2.03# cd /opt/ias6/ias/jms/bin

bash-2.03# ./jmssetup

iAS install directory is /opt/ias6/ias

Are you using IBM MQ v5.1 as message provider [Y] :n

Enter the dynamic library run path (LD_LIBRARY_PATH) for your JMS
message provider. When finished, hit return only) :

Will append to LD_LIBRARY_PATH? Is this correct? [Y] :

Enter the elements (absolute path) for the JMS provider CLASSPATH

When finished, hit return only. :/opt/SUNWjmq/lib/jmq.jar

Enter the elmements (absolute path) for the JMS provider
CLASSPATH

When finished, hit return only. :/opt/SUNWjmq/lib/jmqadmin.jar

Enter the elmements (absolute path) for the JMS provider
CLASSPATH

When finished, hit return only. :

Will append
:/opt/SUNWjmq/lib/jmq.jar:/opt/SUNWjmq/lib/jmqadmin.jar to
CLASSPATH?

Is this correct? [Y] :y

Connected to LDAP server on myhost.mycompany.com port 388
```

Once configured on one machine, configure the second machine before progressing to installing the iTPS components.

At this point there is no need to start the iMQ services. Instructions for starting the iMQ service are shown in Chapter 4.

# Installing iWS 6.0 for iTPS components(step 2c)

In order to be able to install the Bank in a Box administrator component, a web Server needs to be available. The iTPS CD contains a iWS 6.0 package that is shipped for this use. Run the iWS6.0 setup tool located in

```
/cdrom/cdrom0/iws6
```

Selecting the default values for the installation may cause the iWS 6.0 installation to clash with the iWS 6.0 SP2 installed for the iTTM 3.0.1. In order to avoid this, ensure that the Administration server port and the Web server port are set to values other than **8888** and **80** respectively. We recommend using **8890** and **90** respectively. If in doubt about which ports the webserver for iTTM was using, restart the webserver and the admin server:

```
./opt/iws6/https-myhost.mycompany.com/stop

./opt/iws6/https-admserv/stop

./opt/iws6/https-myhost.mycompany.com/start

./opt/iws6/https-admserv/start
```

When installing the iWS 6.0 make sure that you select the option that specifies an external JDK 1.3.1downloaded from http://www.javasoft.com into /usr/java1.3

Ensure that a web server is installed on both the Buyer and Seller bank machines prior to moving on to the installation of the iTPS components.

If you make a mistake while installing your webserver, remove the web server either in its entirety as illustrated below

```
cd /opt/iws6

./uninstall

rm -rf /opt/iws6
```

or removing an individual instance from the console using the < remove server> option. You should also stop the webserver first.

If you are installing an iTPS component on the same machine you will need to create a new web server instance for each component.

1. Go to the Web Server Admin:

2. For instance, http://myhost.mycompany.com:8888

3. Select <Add Server>

4. The following naming convention should be used for each Web Server Instance:

- Web server host https-myhost.mycompany.com

- iTPS instance https-itps.mycompany.com

- BFI instance https-itps-bfi.mycompany.com

- Biab instance https-itps-biab.mycompany.com

- TooledUp instance https-itps-tdup.mycompany.com

- Conditional Management instance https-itps-cond.mycompany.com

- Obligation Management instance https-itps-om.mycompany.com

However for the purpose of this document we are assuming that the webserver instance is always set to https-myhost.mycompany.com

## Mail Server (step 2d)

The mail server is used for asynchronous payment messages and can be provided by your corporate mail server or an installation of a new mail server such as iPlanet Messaging Server installed on an available machine. To check you have a mail Server type

```
telnet mymailhost 25
```

A mail user will be required by the iTPS install script in step 3a. You should make a note of this. For example if the mail server is on the same machine as the iTPS installation then this would be

```
myhost.mycompany.com:25
```

# Installing iTPS Components

The iTPS components reside on both the Buyer and Seller bank machines. The following sections describe the installation of these components.

## Payments Services installation (step 3a)

Make sure you have installed and configured iPlanet Trustbase Transaction Manager 3.0.1 and iPlanet Message Queue for Java 2.0

1. Make a security back up of your Trustbase directory structure:

   ```
   cp -r /opt/ittm /opt/trustbase.bak
   ```

This is required because the iTPS install cannot be un-installed, and installing the iTPS more than once on a iTTM installation will not work. If an installation of the iTPS fails for any reason you are advised to restore the backup and start again.

2. Make sure your slapd is running. From the root account, run the UNIX install script and answer the questions. Select the appropriate menu option for itps from

   ```
   ./cdrom/cdrom0/itps/setup -g
   ```

the following options are available for Silent Install:

   a. -g Performs a complete graphic install

   b. -s Operates on Command line answers silently

   c. -c Performs complete command line install interactively

   d. -k Asks for command line answers

   e. -m Gathers settings from installed packages

   f. -p Reinstalls, adds or patches a package

   g. -u Uninstalls an installed package

You should consult the iTTM Installation and Configuration Guide for more information on this

**Figure 2-2** iPlanet Trustbase Payment Services Installation Welcome Screen
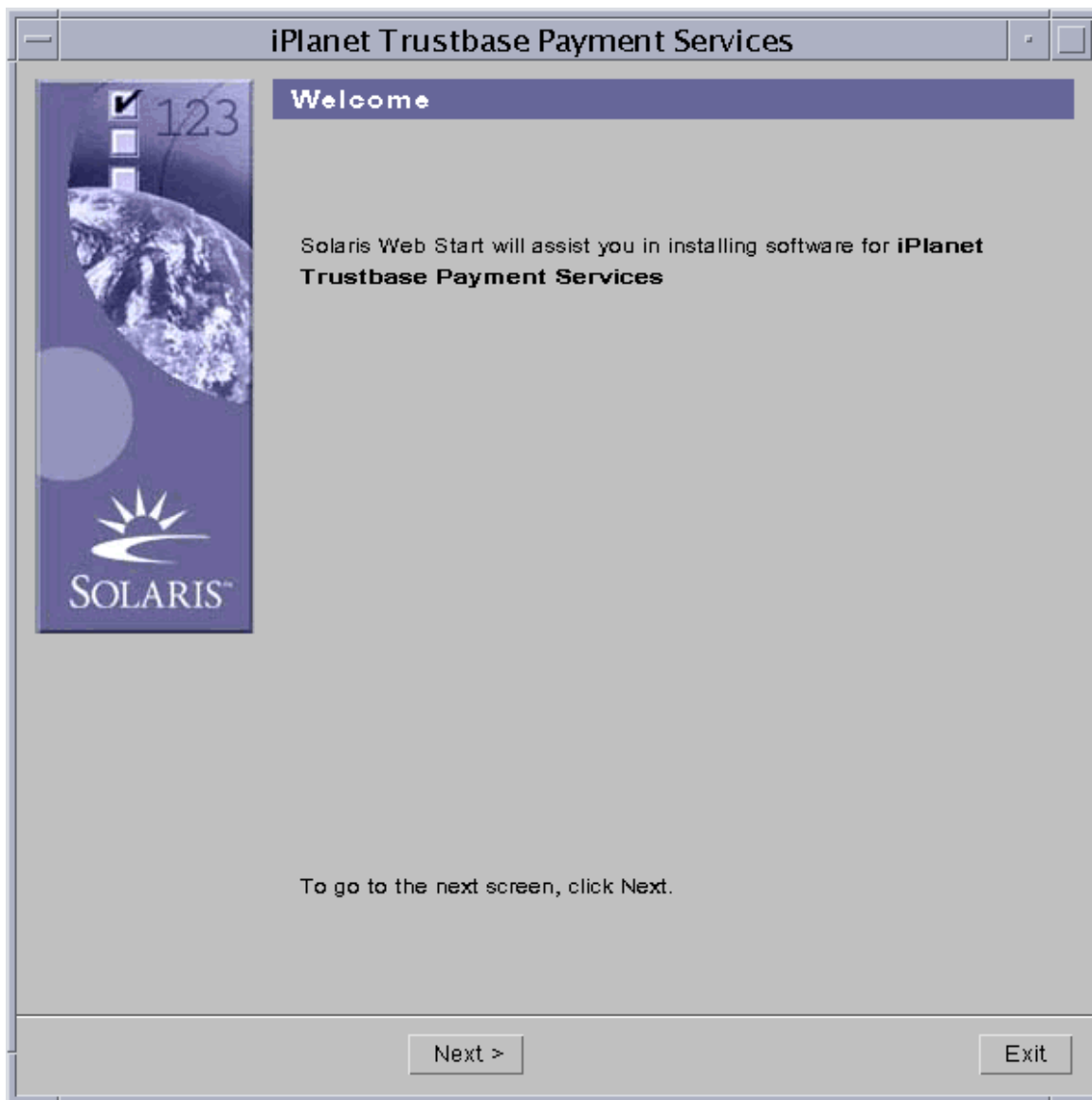
**Figure 2-3** Locale SelectionDatabase Settings
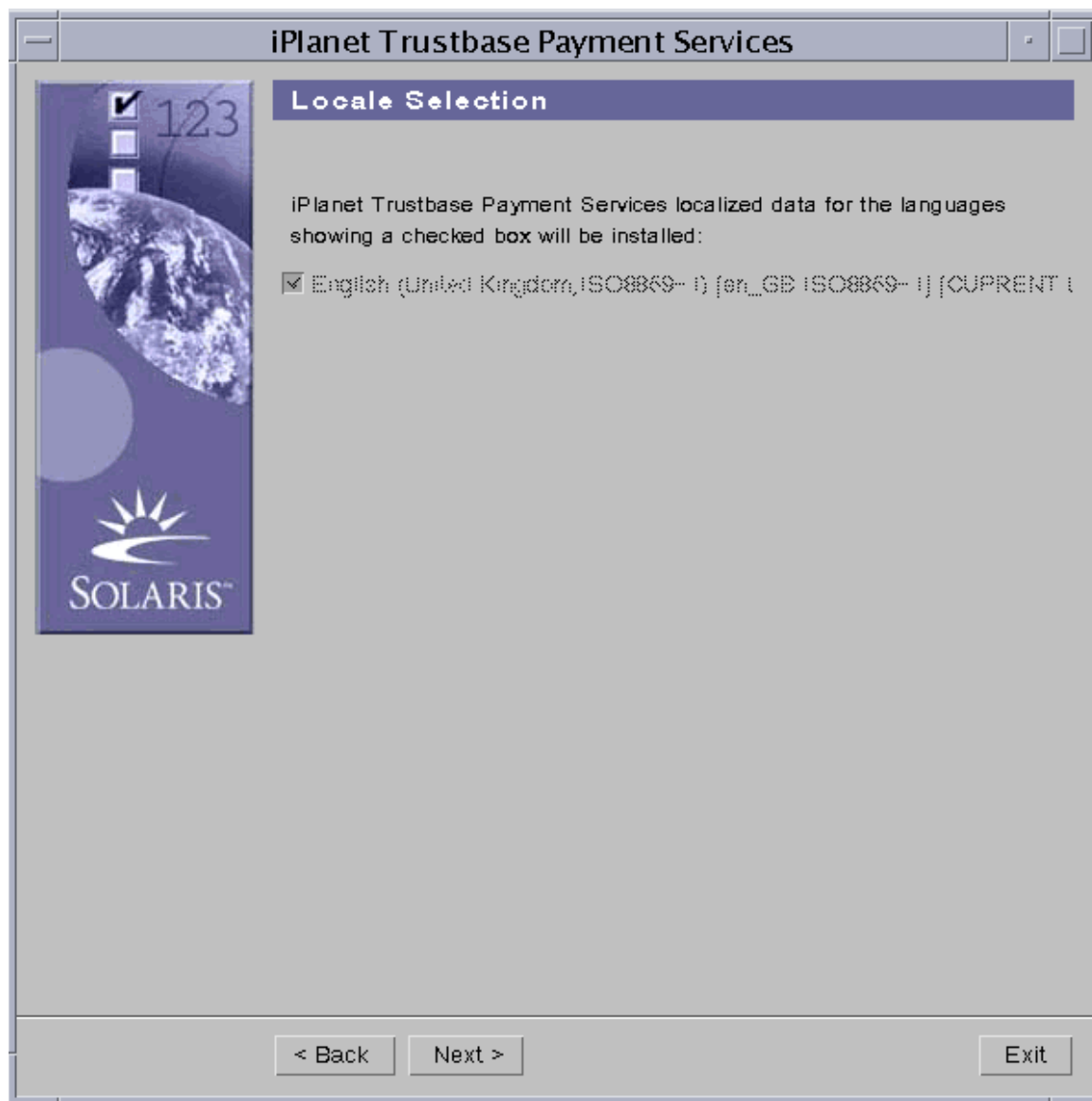
**Figure 2-4** iPlanet Message Queue For Java Settings
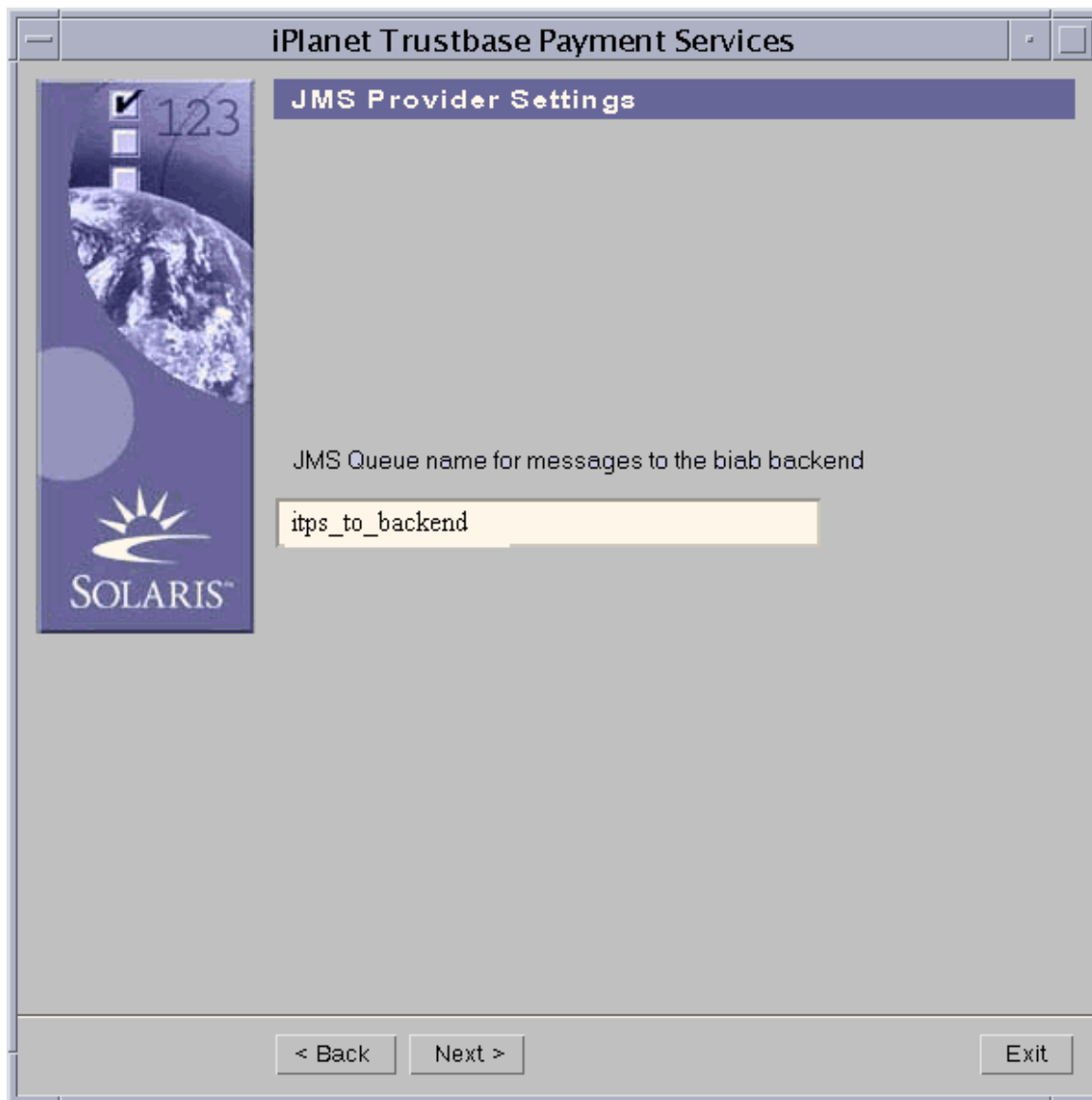


Notes: This Outbound Queue name is the queue going from the iTPS to BiaB and will need to be recorded for later use. itps_to_backend is a suitable name for this.

**3.** Please reference your company mail server

**Figure 2-5** Payments Mail Settings



Next enter the following as illustrated above.

- SMTP host. This is the host where customer email acknowledgements are sent.

- From field. This is the From field of the customer acknowledgement email

**Figure  2-6**      iPlanet Trustbase Payment Server Verification Panel



The screen displays the user's choices in order to aid the correct installation. You will need to make a note of the information in this screen as the information is required to install other components later in the process.

**Figure 2-7** Component Selection
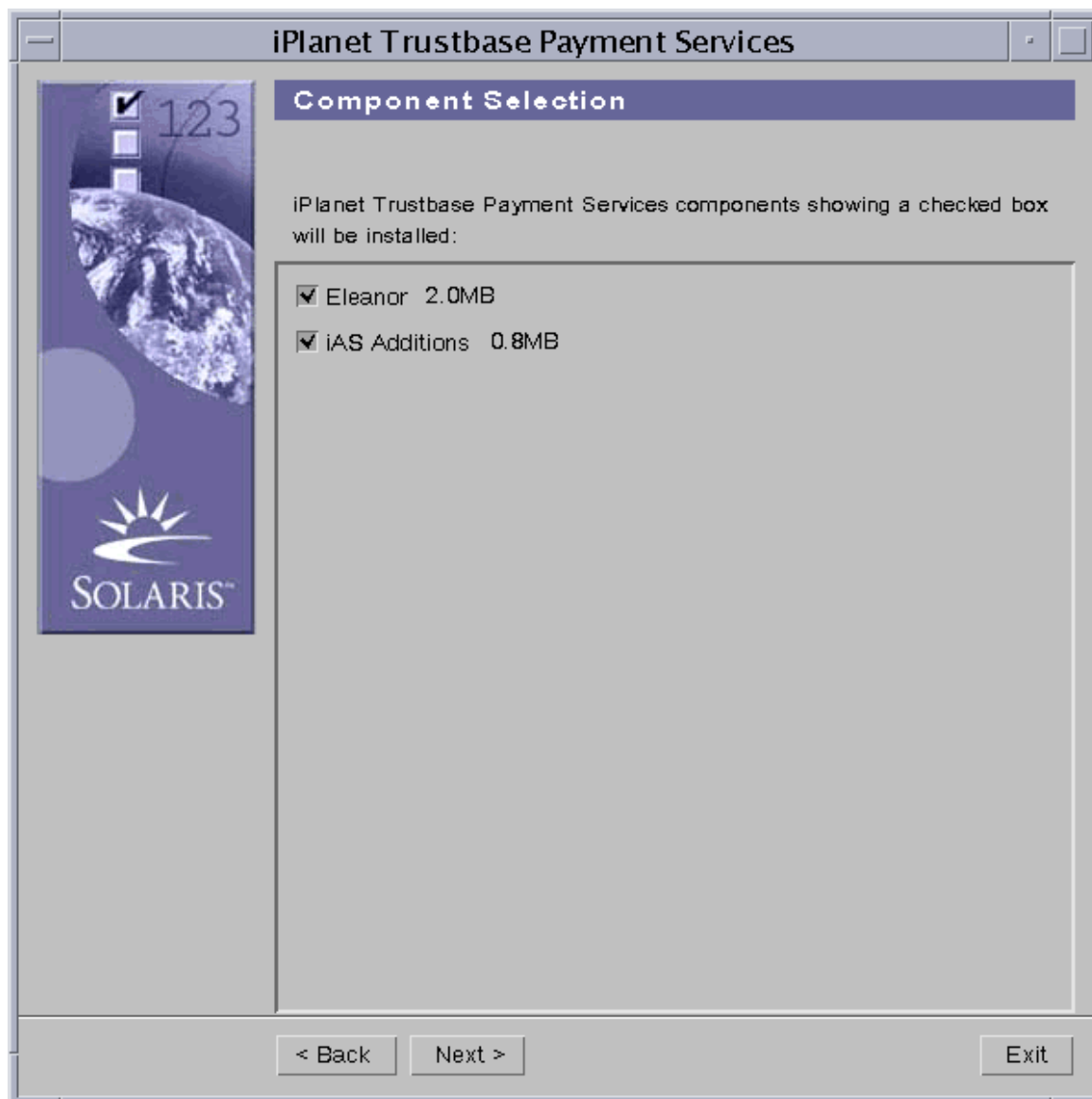


On entering the screen the size of iPlanet Trustbase Payment Services software application is displayed. In order to install this software the user needs to select the checkbox.

**Figure 2-8**     Ready to Install
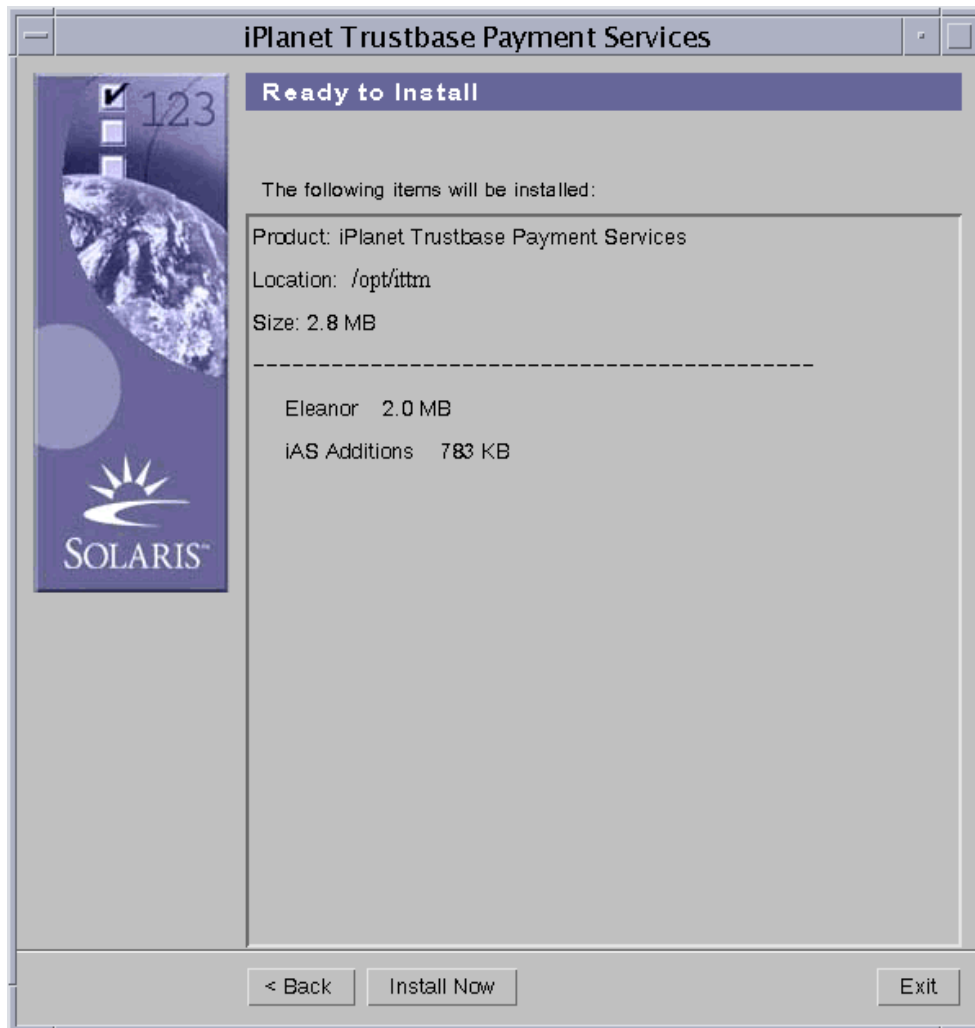


This screen indicates the amount of space that is required to install iPlanet Trustbase Payment Services software. It also indicates the location of the iPlanet Trustbase Transaction Manager system that the iPlanet Trustbase Payment Services plug-in will be installed into.

You should make a note of these locations as they will be required later in the installation process. There are then two screens that update settings within iTTM and iAS.

**Figure 2-9** Updating iPlanet Trustbase Transaction Manager
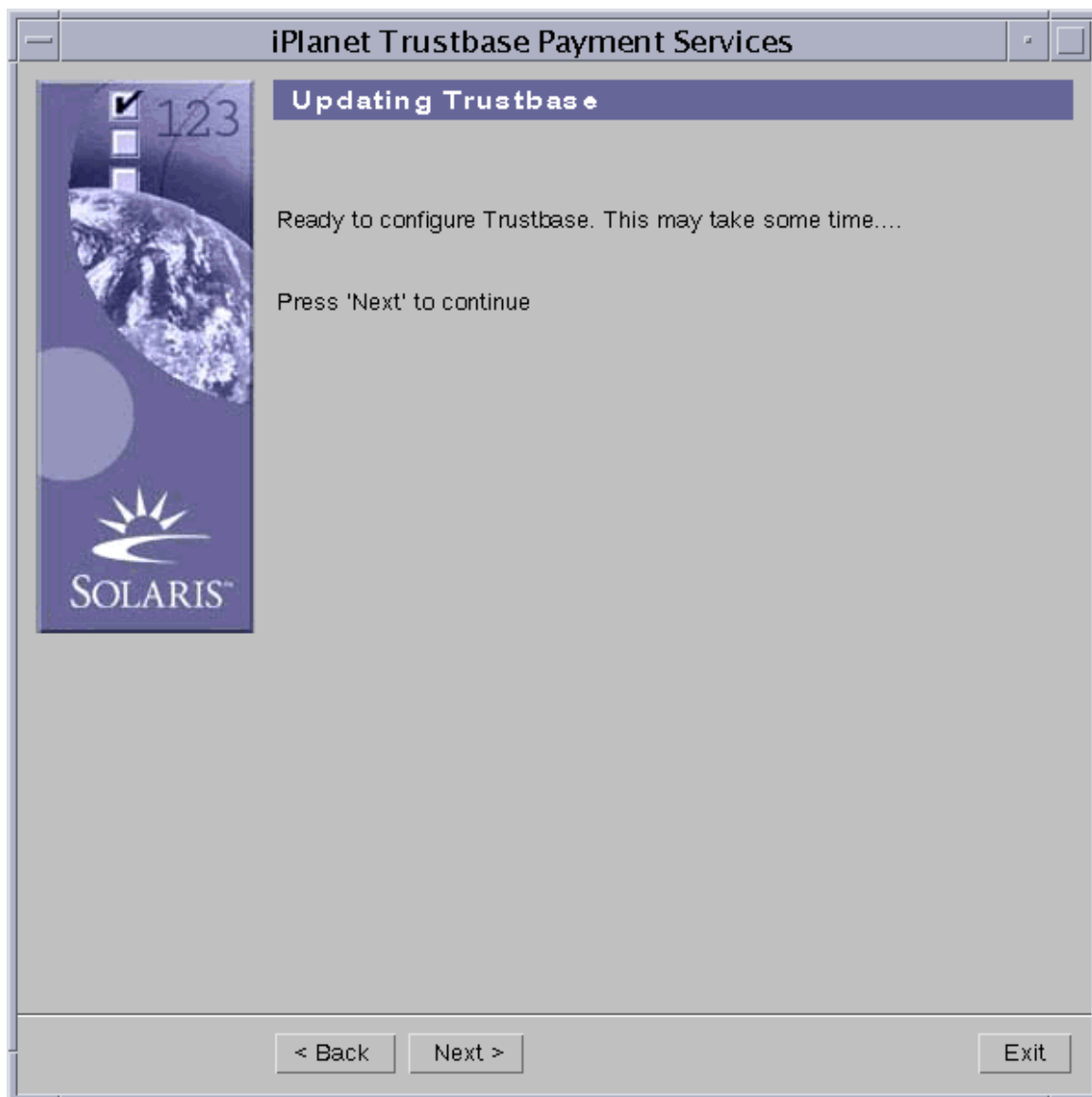
**Figure 2-10** Installation Summary
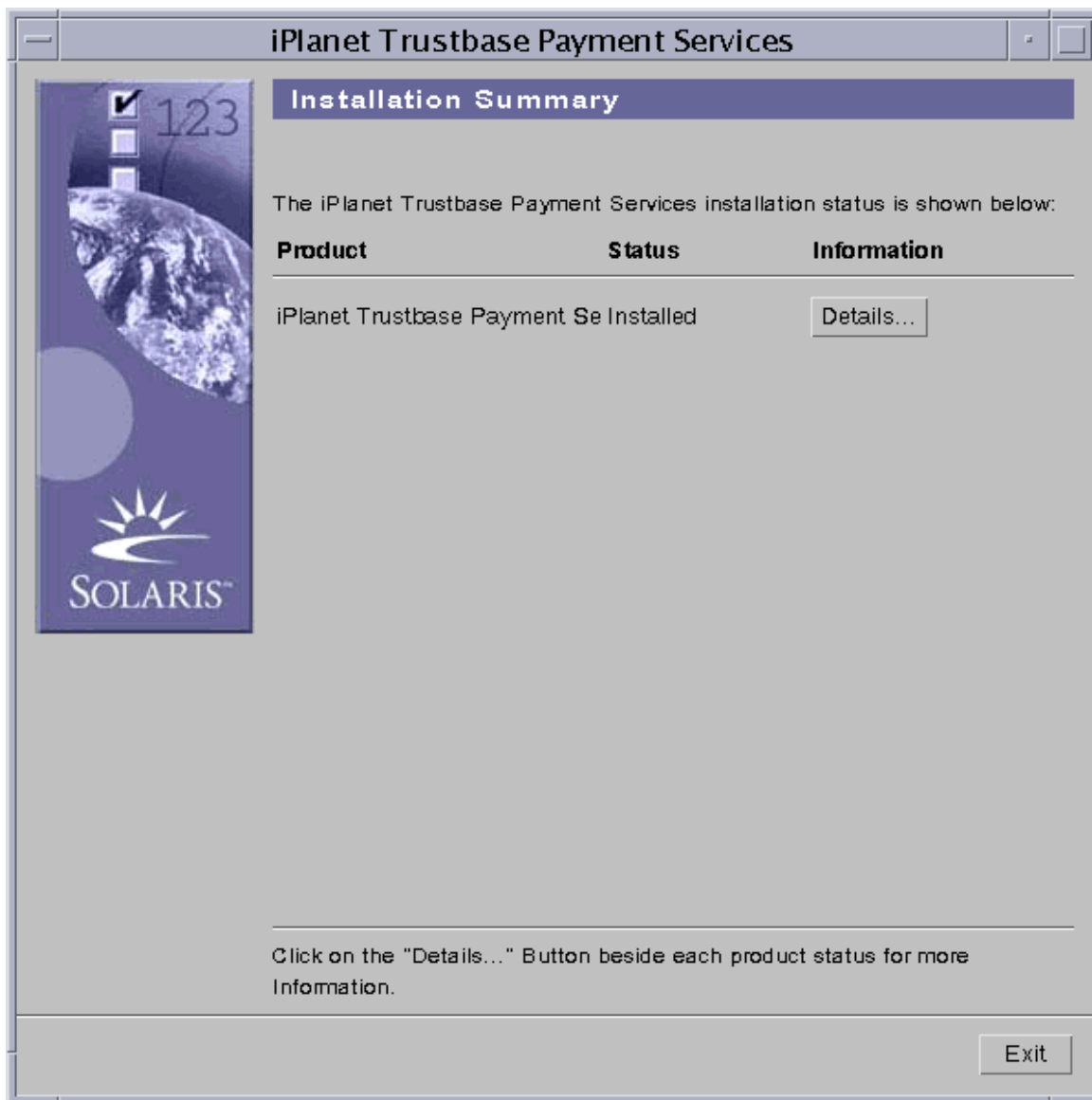


Pressing the details button will display the software installed on the system and alterations to the existing configurations of iPlanet Trustbase Transaction Manager.

## Set up iTPS database tables

You will now need to run oracle scripts. If Oracle is not installed on the same machine as the iTPS installation then you either have to copy the /opt/ittm/current/Config/sql directory to the database server or install the Oracle client on the machine. There are two alternative situations here.

1.  Oracle on same machine as iTPS. Alternatively this can be an Oracle client.

```
mydatabase% su - oracle
mydatabase% cd /opt/ittm/current/Config/sql
mydatabase% sqlplus tbase/tbase
SQL*Plus: Release 8.1.7.0.0 - Production on Fri Feb 15 12:07:11 2002
(c) Copyright 1999 Oracle Corporation. All rights reserved.
Enter user-name: tbase
Enter password:
Connected to:
Oracle 8i Enterprise Edition Release 8.1.7.0.0 - Production
PL/SQL Release 8.1.7.0.0 - Production
SQL>spool myoutput.txt
SQL>set echo on
SQL>@PaymentsNew.sql
```

You should check the output file to ensure that all SQL tables were created successfully.

/opt/ittm/current/Config/sql/myoutput.txt

2.  Oracle on different machine as iTPS. For example:

    a.  cd /opt/ittm/current/Config/sql

    b.  ftp myhost.mycompany.com <username><password>

    ftp> hash

    ftp> prompt

    ftp> mput *

    ftp> quit

    c.  telnet myhost.mycompany.com <username><password>

    d.  Follow the instructions in step 1

This will need to be executed on the database(s) used by both the Buyer and Seller banks iTPS installations.

# JMS Proxy Configuration (step 3b)

The JMS Proxy provides a mechanism for the iTTM to receive inbound messages from an iMQ queue. Messages are taken from the queue and forwarded to iTTM over HTTP. You will need to configure a JMS Proxy on both the Buyer and Seller bank machines.

**Figure 2-11**    Configuring JMS Proxy
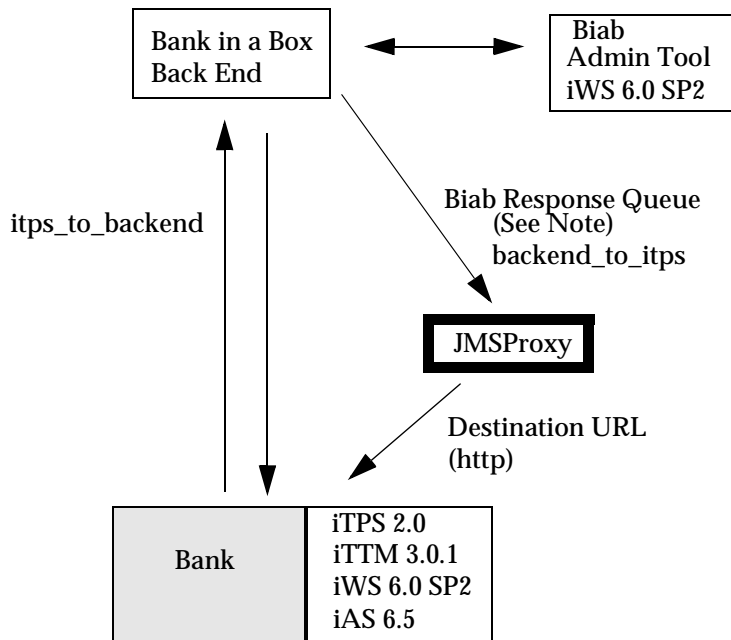
Normally this section is already done for you. However in some situations you may wish to change some settings.

1. Check the following lines in the jmsproxy /opt/ittm/myhost/jmsproxy.properties:

- Destination is the URL to which message content will be forwarded (See figure Figure 2-11)

   ```
   destination=http://myhost.mycompany.com/NASApp/NASAdapter/Tbase
   NASAdapter?Forwarded-by:JMSProxy
   ```

   You will need to change just the hostname component to an appropriate value e.g.

   ```
   http://myhost.mycompany.com/NASApp/NASAdapter/TbaseNASAdapter?Fo
   rwarded-by:JMSProxy
   ```

- queue.host is the hostname of the machine where the JMS broker is listening. Since this is part of iTTM this should not normally change.

   ```
   queue.host=queue_hostname
   ```

   e.g. queue.host=myhost.mycompany.com

- queue.port The port on which the JMS broker is running by default this will be 7676 unless it was changed during the iMQ installation.

   ```
   queue.port=queue_port
   ```

   ```
   e.g. queue.port=7676
   ```

- queue.name The name of the queue on which to receive messages. This is the asynchronous send queue as specified in the Bank in a Box configuration

   ```
   queue.name=backend_to_itps
   ```

Note: Make sure the destination URL is the server host name of the appropriate Buyer or Seller bank iTTM installation. Make a note of this URL as you will need this again when configuring the Bank in a Box components. If you make any changes you should also stop and start iTTM in order for these changes to take effect:

   ```
   /opt/ittm/Scripts/stoptbase
   ```

   ```
   /opt/ittm/Scripts/starttbase
   ```

# BiaB Back End office simulator (step 3c)

The Bank in a Box (BiaB) back office simulator is designed to create responses to messages received by the iTPS from the buyer and seller web sites. The BiaB must be installed on both the Buyer and Seller Banks servers.

It is not imperative that the iTTM and iTPS are running during installation, however they should be running before starting BiaB.

In order to install the BiaB on each machine follow the instructions below:

**1.** If you are installing an iTPS component on the same machine make sure you install it to a unique Web Server instance.

**Figure  2-12**    Adding a New iWS Web Server instance



**a.** Go to the Web Server Admin:

**b.** http://myhost.mycompany.com:8888
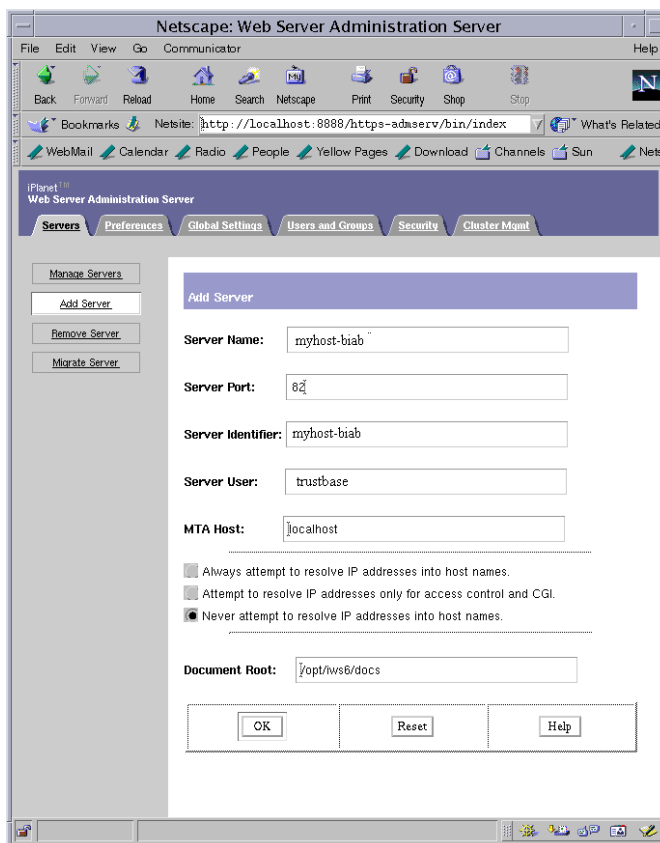
**c.** Select <Add Server>

      **d.**   Select for instance a unique port iD of 82

      **e.**   Use the same user, e.g. tbase, as you entered when you installed iWS

      **f.**   Define a unique Server id

      **g.**   Select <Add>

**2.**   From the root account, run the UNIX install script and answer the questions. Select the appropriate menu option for itps-biab from

```
./cdrom/cdrom0/itps-biab/setup -c
```

Not a graphic version is not available is not available for itps components and as such you must select the command line interactive setup option. This will automatically install to

```
/opt/itps-biab
```

**3.**   The following defaults are recommended:

[1] The user that will run BIAB? tbase
[2] The group that this user belongs to? iplanet
[3] The Web Server location is [ /opt/iws6 ]

[4] The Web Server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-biab-deploy ]

[7] The queue driver location is [ /opt/SUNWjmq/lib/jmq.jar ]

[8] The from itps queue name [ itps_to_backend ]

[9] The to itps queue name [ backend_to_itps ]

[10] The queue server host [ myqueue.mycompany.com ]

[11] The queue server port [ 7676 ]

[12] The database user is [ tbase ]

[13] The database password is [ tbase ]

[14] The database host is [ mydatabase.mycompany.com ]

[15] The database port is [ 1521 ]

[16] The database sid is [ orcl ]

**4.** Run the biabNew.sql SQL script on the payments database server. This can be found in:

```
/opt/itps-biab/config/sql/biabNew.sql
```

This may involve copying the SQL script to the appropriate machine if Oracle is remotely located. Also logging onto Oracle. As in the example mentioned in the previous section headed "Set up iTPS database tables," on page 67:

```
mydatabase% su - oracle
mydatabase% cd /opt/itps-biab/config/sql/
mydatabase% sqlplus tbase/tbase
SQL*Plus: Release 8.1.7.0.0 - Production on Fri Feb 15 12:07:11 2002
(c) Copyright 1999 Oracle Corporation. All rights reserved.
Enter user-name: tbase
Enter password:
Connected to:
Oracle 8i Enterprise Edition Release 8.1.7.0.0 - Production
PL/SQL Release 8.1.7.0.0 - Production
SQL>spool myoutput.txt
SQL>set echo on
SQL>@biabNew.sql
```

You should check the output file to ensure that all SQL tables were created successfully.

```
/opt/itps-biab/config/sql/myoutput.txt
```

**5.** Having installed the BiaB on either the Buyer or Seller Bank machines, install the BiaB on the other machine before moving on to the BiaB administration tool.

# BiaB Admin Tool (step 3d)

Biab Admin tool is automatically installed with the biab backend (step3c). The BiaB administration tool is a Web application designed to run on the iWS 6.0 Web server set up earlier. A BiaB administrator tool should be installed on both the Buyer and Seller Bank machines that host the iTPS and BiaB components. The BiaB Admin tool web application is located on the BiaB directory.

In order to start the Web application you must perform the following:

1.  From the root account

2.  You now need to remember the correct Web Server Instance that you created in "Installing iWS 6.0 for iTPS components(step 2c)," on page 54 for both itps and biab

3.  Once installed, restart the Web server and Admin Server instance. For instance:

    ```
    ./opt/iws6/https-admserv/start
    ```

    ```
    ./opt/iws6/https-myhost.mycompany.com/start
    ```

4.  From the tbase account, Start the bank in a box back end in a separate window:

    ```
    ./opt/itps-biab/scripts/biab
    ```

5.  Once deployed successfully, the Web Site can be accessed from the browser with the following url.

    ```
    http://<hostname>:<port>/<uri_path>/biab.
    ```

    The BiaB admin tool deployed using the deploy directory would be accessed using:

    ```
    http://myhost.mycompany.com:82/itps-biab/logon.html
    ```

If the server is running and the Web application has deployed successfully the following page will be displayed:

**Figure 2-13** Bank in a Box Admin Tool Welcome Screen
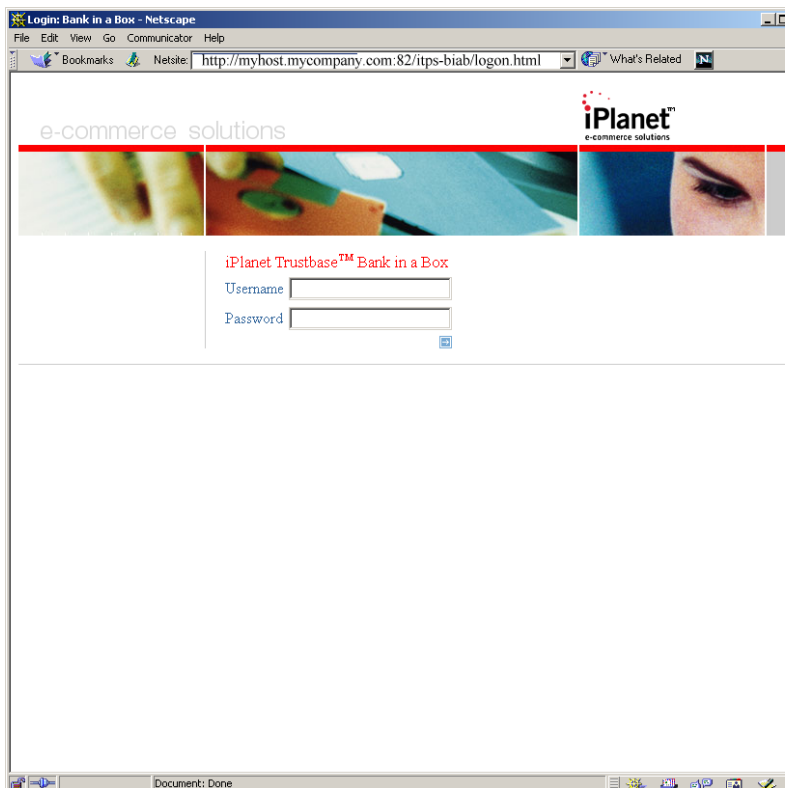


Before logging in you need to add a username and password, in order to do this you should consult chapter 3 "Running the System" in the iTPS Systems Administration Guide.

# Condition Management Website (step 3e)

Before you can begin to install the Condition Management Website, you will need to create a local Certificate Database inside the Webserver for it to use. This certificate database will contain from 3-5 certificates depending on how many roles you assign the certificates to perform, the roles are as follows.

    **a.** Root Certificate or Trust Anchor Certificate (e.g. IRCA).

    **b.** Level One Certificate Authority Certificate. (e.g. L1CA)

    **c.** End Entity Signing Certificate ( e.g. ClientSC) The AIA field within this certificate is used to determine the destination for the payments message)

    **d.** SSL Client Transaction Certificate ( e.g. ClientSSL)

    **e.** SSL Server Certificate (This name is forced upon you by the Web Server Server-Cert)

If installing itps components on the same machine, the same certificates may be used, depending on your security requirement.

To create the certificate databases and import the certificate complete the following steps:

**1.** You now need to remember the correct Web Server Instance that you created in "Installing iWS 6.0 for iTPS components(step 2c)," on page 54

**2.** If you are installing an iTPS component on the same machine make sure you install it to a unique Web Server instance.

    **a.** Go to the Web Server Admin:

    **b.** http://myhost.mycompany.com:8888

    **c.** Select <Add Server>

    **d.** Select for instance a unique port iD of 83

    **e.** Use the same user, e.g. tbase, as you entered when you installed iWS

    **f.** Define a unique Server id

    **g.** Select <Add>

**3.** Create The Webserver Database

    ❍ Access the iWS6 admin server e.g.:

```
./opt/iws6/startconsole
```

    This will start a browser and allow you to log into the admin server.

- Choose the server to manage and click manage.

- Click on the security tab (it defaults to 'Initialise Trust Database' screen)

- Type in a new password for database and click <ok>. This will create a new database that can only be accessed using the password you have just given so ensure that you do not forget the password!

4. Install The Root Certificate (e.g. IRCA).

- Click the <Install Certificate> Tab.

- Select <Trusted Certificate Authority>, select <message text> and paste in the Base 64 cert from your Identrus Root CA

- Click <ok>

- Click <Add Server Certificate>

5. Install The CA Certificate (e.g. L1CA)– Use the same process as Import The Root Certificate (above)

6. Create and import an End Entity Signing Certificate (e.g. ClientSC)

- Click the <request certificate> tab.

- Select <CA URL>

- In the <CA URL> field enter "None"

- Enter "password"

- Fill in the address details part of the form and press <ok>.

- Copy and paste the BASE 64 Request into your Seller Banks CA certificate request form.

- Retrieve reply from CA and copy the Base 64 cert into the webserver form.

- Click <Install Certificate.>

- Select <This Server>, input a name for the cert (e.g. ClientSC), make a note of the name as you will need it later, Select Message Text and paste in the base 64 cert from the CA.

- Click <ok>

- Click <Add Cert>

7. Request, Generate and Import SSL Client Transaction Certificate – Same as for End Entity Signing Cert, but make sure that the name for the certificate is different (e.g. ClientSSL), and keep a note of the name as you will need it later.

8.  Request, Generate and Import SSL Server Certificate – Same as for End Entity Signing Cert except – do not give this certificate a certificate name as the webserver will assign it 'Server-Cert'; use an appropriate type "SSL Server certificate" profile at the CA.

9.  You are now ready to install the Condition management Component. From the root, run the UNIX install script and answer the questions. Select the appropriate menu option for itps-cond from

    ```
    ./cdrom/cdrom0/itps-cond/setup -c
    ```

    Not a graphic version is not available is not available for itps components and as such you must select the command line interactive setup option. This will automatically install to

    ```
    /opt/itps-cond
    ```

10. The following default settings should be used:

[1] The user that will run Condition Website? tbase
[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-cond-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA ]

[11] The absolute path of the temporary directory for file downloads [/temp]

11. Restart the Webserver

/opt/iws6/https-myhost.mycompany.com/stop

/opt/iws6/https-myhost.mycompany.com/start

12. Go to the Condition Management website

http://myhost.mycompany.com:83/itps-cond/logon.html

Before accessing the website or sending Conditional Payment requests, the Condition Registry needs to be configured to accept the Buyer of the payment The seller of the payment and the Conditional Discharge Party. You should consult your System's Administration Guide for details on how to configure the Condition Registry.

# Obligation Management Website (step 3f)

Before you can begin to install BFI you will need to create a local Certificate Database inside the Webserver for it to use. This certificate database will contain from 3-5 certificates depending on how many roles you assign the certificates to perform, the roles are as follows.

    **a.**  Root Certificate or Trust Anchor Certificate (e.g. IRCA).

    **b.**  Level One Certificate Authority Certificate. (e.g. L1CA)

    **c.**  End Entity Signing Certificate ( e.g. ClientSC) The AIA field within this certificate is used to determine the destination for the payments message)

    **d.**  SSL Client Transaction Certificate ( e.g. ClientSSL)

    **e.**  SSL Server Certificate (This name is forced upon you by the Web Server Server-Cert)

If installing itps components on the same machine, the same certificates may be used, depending on your security requirement.

To create the certificate databases and import the certificate complete the following steps:

**1.** You now need to remember the correct Web Server Instance that you created in "Installing iWS 6.0 for iTPS components(step 2c)," on page 54

**2.** If you are installing an iTPS component on the same machine make sure you install it to a unique Web Server instance.

    **a.**  Go to the Web Server Admin:

    **b.**  http://myhost.mycompany.com:8888

    **c.**  Select <Add Server>

    **d.**  Select for instance a unique port iD of 84

    **e.**  Use the same user, e.g. tbase, as you entered when you installed iWS

    **f.**  Define a unique Server id

    **g.**  Select <Add>

**3.** Create The Webserver Database

    ❍  Access the iWS6 admin server e.g.:

```
./opt/iws6/startconsole
```

    This will start a browser and allow you to log into the admin server.

- ❍ Choose the server to manage and click manage.
- ❍ Click on the security tab (it defaults to 'Initialise Trust Database' screen)
- ❍ Type in a new password for database and click <ok>. This will create a new database that can only be accessed using the password you have just given so ensure that you do not forget the password!

4. Install The Root Certificate (e.g. IRCA).

- ❍ Click the <Install Certificate> Tab.
- ❍ Select <Trusted Certificate Authority>, select <message text> and paste in the Base 64 cert from your Identrus Root CA
- ❍ Click <ok>
- ❍ Click <Add Certificate>

5. Install The CA Certificate (e.g. L1CA)– Use the same process as install The Root Certificate (above)

6. Create and import an End Entity Signing Certificate (e.g. ClientSC)

- ❍ Click the <request certificate> tab.
- ❍ Select <CA URL>
- ❍ In the <CA URL> field enter "None"
- ❍ Enter "password"
- ❍ Fill in the address details part of the form and press <ok>.
- ❍ Copy and paste the BASE 64 Request into your Seller Banks CA certificate request form.
- ❍ Retrieve reply from CA and copy the Base 64 cert into the webserver form.
- ❍ Click <Install Certificate.>
- ❍ Select <This Server>, input a name for the cert (e.g. ClientSC), make a note of the name as you will need it later, Select Message Text and paste in the base 64 cert from the CA.
- ❍ Click <ok>
- ❍ Click <Add Cert>

7. Request, Generate and Import SSL Client Transaction Certificate – Same as for End Entity Signing Cert, but make sure that the name for the certificate is different (e.g. ClientSSL), and keep a note of the name as you will need it later.

8.  Request, Generate and Import SSL Server Certificate – Same as for End Entity Signing Cert except – do not give this certificate a <certificate name> as the webserver will assign it 'Server-Cert'.

9.  From the root, run the UNIX install script and answer the questions. Select the appropriate menu option for itps-om from

    ```
    ./cdrom/cdrom0/itps-om/setup -c
    ```

    Not a graphic version is not available is not available for itps components and as such you must select the command line interactive setup option. This will automatically install to

    ```
    /opt/itps-om
    ```

10. The following default settings should be used

[1] The user that will run Obligation Website? tbase
[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-om-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA ]

11. Restart the Webserver

/opt/iws6/https-myhost.mycompany.com/stop

/opt/iws6/https-myhost.mycompany.com/start

12. Go to the Obligation Management website

http://myhost.mycompany.com:84/itps-om/logon.html

Before accessing the website or sending Obligation Payment requests, the relevant users needs to be configured to accept, for example to allow The seller of the payment to transfer an obligation. You should consult your System's Administration Guide for details on how to add a users using userdbtool.

# Installing the Buyer and Seller websites

The following sections describe how to install the components required to run the Buyer and Seller web sites. These web sites will be used to interact with the Buyer and Seller iTPS components installed previously.

## Installing the iWS 6.0 (step 4a)

In order to run the web applications that make up the buyer and sellers web sites, a web Server needs to be available on each machine. The iTPS CD contains an iWS 6.0 package that is shipped for this use.

Run the iWS6.0 setup tool located in

```
/cdrom/cdrom0/iws6
```

Selecting the default values for the installation of the iWS 6.0 should be sufficient for most installations. The only non-standard option you will need to specify is the option that specifies an external JDK 1.3.1 either downloaded from http://www.javasoft.com to /usr/java1.3

This is because the JDK included does not support the buyer and seller web site functionality tools.

Ensure that a web server is installed on both the Buyer and Seller machines prior to moving on to the installation of the Buyer and Seller web applications.

# Installing Buyers Bank Website (step 4b)

It does not matter whether iTTM and iTPS are running during installation. However they, and all their associated components such as iAS and iWS, should be running if you need to run this component

Before you can begin to install the Buyers Bank Website (BFI) you will need to create a local Certificate Database inside the Webserver for it to use. This certificate database will contain from 3-5 certificates depending on how many roles you assign the certificates to perform, the roles are as follows.

    **a.** Root Certificate or Trust Anchor Certificate (e.g. IRCA).

    **b.** Level One Certificate Authority Certificate. (e.g. L1CA)

    **c.** End Entity Signing Certificate ( e.g. ClientSC) The AIA field within this certificate is used to determine the destination for the payments message)

    **d.** SSL Client Transaction Certificate ( e.g. ClientSSL)

    **e.** SSL Server Certificate (This name is forced upon you by the Web Server Server-Cert)

If installing itps components on the same machine, the same certificates may be used, depending on your security requirement.

To create the certificate databases and import the certificate complete the following steps:

**1.** If you are installing an iTPS component on the same machine make sure you install it to a unique Web Server instance.

    **a.** Go to the Web Server Admin:

    **b.** http://myhost.mycompany.com:**8888**

    **c.** Select <Add Server>

    **d.** Select for instance a unique port iD of 85

    **e.** Use the same user, e.g. tbase, as you entered when you installed iWS

    **f.** Define a unique Server id

**2.** Create The Webserver Database

    o Access the iWS6 admin server e.g.:

```
./opt/iws6/startconsole
```

    This will start a browser and allow you to log into the admin server.

- ❍ Choose the server to manage and click manage.

- ❍ Click on the security tab (it defaults to 'Initialise Trust Database' screen)

- ❍ Type in a new password for database and click <ok>. This will create a new database that can only be accessed using the password you have just given so ensure that you do not forget the password!

3. Install The Root Certificate (e.g. IRCA).

- ❍ Click the <Install Certificate> Tab.

- ❍ Select <Trusted Certificate Authority>, select <message text> and paste in the Base 64 cert from your Identrus Root CA

- ❍ Click <ok>

- ❍ Click <Add Certificate>

4. Install The CA Certificate (e.g. L1CA)– Use the same process as Import The Root Certificate (above)

5. Create and import an End Entity Signing Certificate (e.g. ClientSC)

- ❍ Click the <request certificate> tab.

- ❍ Select <CA URL>

- ❍ In the <CA URL> field enter "None"

- ❍ Enter "password"

- ❍ Fill in the address details part of the form and press <ok>.

- ❍ Copy and paste the BASE 64 Request into your Seller Banks CA certificate request form.

- ❍ Retrieve reply from CA and copy the Base 64 cert into the webserver form.

- ❍ Click <Install Certificate.>

- ❍ Select <This Server>, input a name for the cert (e.g. ClientSC), make a note of the name as you will need it later, Select Message Text and paste in the base 64 cert from the CA.

- ❍ Click <ok>

- ❍ Click <Add Cert>

6. Request, Generate and Import SSL Client Transaction Certificate – Same as for End Entity Signing Cert, but make sure that the name for the certificate is different (e.g. ClientSSL), and keep a note of the name as you will need it later.

7. Request, Generate and Import SSL Server Certificate – Same as for End Entity Signing Cert except – do not give this certificate a certificate name as the webserver will assign it 'Server-Cert'.

8. You are now ready to install BFI Website From the root, run the UNIX install script and answer the questions. Select the appropriate menu option for itps-bfi from

   ```
   ./cdrom/cdrom0/itps-bfi/setup -c
   ```

   Not a graphic version is not available is not available for itps components and as such you must select the command line interactive setup option. This will automatically install to

   ```
   /opt/itps-bfi
   ```

9. The following default settings are recommended:

[1] The user that will run BFI? tbase
[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-bfi-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA ]

[11] The database user is [ tbase ]

[12] The database password is [ tbase ]

[13] The database host is [ mydatabase.mycompany.com ]

[14] The database port is [ 1521 ]

[15] The database sid is [ orcl ]

**10.** After you have finished your changes, you will need to re-start the web server for those changes to take effect. To verify the installation:

   **a.** Remove all existing Web Server processes using

   ps -ef | grep iws

   kill -9 <process_number>

   **b.** Alternatively use the script supplied with iWS to do this for you:

   ./opt/iws6/https-myhost.mycompany.com/stop

   **c.** ./opt/iws6/https-admserv/start

   ./opt/iws6/https-myhost.mycompany.com/start

   **d.** If you are using a netscape browser you'll need to apply for a certificate from your L1CA. Finally, you'll need to enable your browser as follows: Select <netscape Security><certificate signers> locate the level 1 CA certificate and make sure the following settings are made as illustrated in the diagram below:

**Figure 2-14**   Netscape browser certificate settings
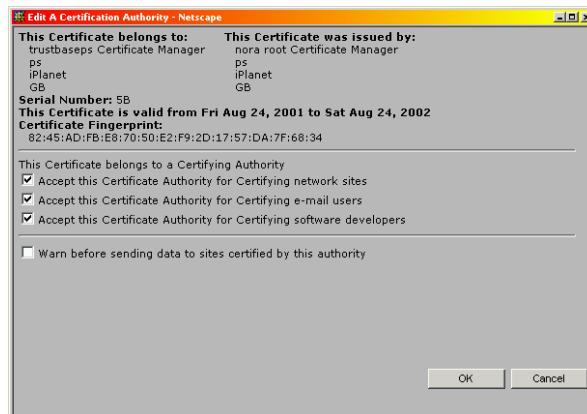


   **e.** From your browser

   http://<hostname>:<webserver Port ID>/itps-bfi/logon.html

   For instance

http://myhost.mycompany.com:85/itps-bfi/logon.html

The BFI login screen should now appear

# Seller's Website TooledUp (step 4c)

The Sellers Website (Tooledup demonstration) is delivered in the form of a tar file called merchant.tar.

Before you can begin to install the Sellers Website (Tooled Up) you will need to create a local Certificate Database inside the Webserver for it to use. This certificate database will contain from 3-5 certificates depending on how many roles you assign the certificates to perform, the roles are as follows.

    **a.** Root Certificate or Trust Anchor Certificate (e.g. IRCA).

    **b.** Level One Certificate Authority Certificate. (e.g. L1CA)

    **c.** End Entity Signing Certificate ( e.g. ClientSC) The AIA field within this certificate is used to determine the destination for the payments message)

    **d.** SSL Client Transaction Certificate ( e.g. ClientSSL)

    **e.** SSL Server Certificate (This name is forced upon you by the Web Server Server-Cert)

If installing itps components on the same machine, the same certificates may be used, depending on your security requirement.

To create the certificate databases and import the certificate complete the following steps:

**1.** If you are installing an iTPS component on the same machine make sure you install it to a unique Web Server instance.

    **a.** Go to the Web Server Admin:

    **b.** http://myhost.mycompany.com:8888

    **c.** Select <Add Server>

    **d.** Select for instance a unique port iD of 86

    **e.** Use the same user, e.g. tbase, as you entered when you installed iWS

    **f.** Define a unique Server id

**2.** Create the Webserver Database

    ❍ Access the iWS6 admin server e.g.:

```
./opt/iws6/startconsole
```

      This will start a browser and allow you to log into the admin server.

    ❍ Choose the server to manage and click manage.

&#9702;    Click on the security tab (it defaults to 'Initialise Trust Database' screen)

&#9702;    Type in a new password for database and click <ok>. This will create a new database that can only be accessed using the password you have just given so ensure that you do not forget the password!

3.    Install The Root Certificate (e.g. IRCA).

&#9702;    Click the <Install Certificate> Tab.

&#9702;    Select <Trusted Certificate Authority>, select <message text> and paste in the Base 64 cert from your Identrus Root CA

&#9702;    Click <ok>

&#9702;    Click <Add Certificate>

4.    Install The CA Certificate (e.g. L1CA)– Use the same process as Import The Root Certificate (above)

5.    Create and import an End Entity Signing Certificate (e.g. ClientSC)

&#9702;    Click the <request certificate> tab.

&#9702;    Select <CA URL>

&#9702;    In the <CA URL> field enter "None"

&#9702;    Enter "password"

&#9702;    Fill in the address details part of the form and press <ok>.

&#9702;    Copy and paste the BASE 64 Request into your Seller Banks CA certificate request form.

&#9702;    Retrieve reply from CA and copy the Base 64 cert into the webserver form.

&#9702;    Click <Install Certificate.>

&#9702;    Select <This Server>, input a name for the cert (e.g. ClientSC), make a note of the name as you will need it later, Select Message Text and paste in the base 64 cert from the CA.

&#9702;    Click <ok>

&#9702;    Click <Add Cert>

6.    Request, Generate and Import SSL Client Transaction Certificate – Same as for End Entity Signing Cert, but make sure that the name for the certificate is different (e.g. ClientSSL), and keep a note of the name as you will need it later.

7.  Request, Generate and Import SSL Server Certificate – Same as for End Entity Signing Cert except – do not give this certificate a certificate name as the webserver will assign it 'Server-Cert'.

8.  You are now ready to install the Tooled Up Website. From the root, run the UNIX install script and answer the questions. Select the appropriate menu option for itps-tdup from

    ```
    ./cdrom/cdrom0/itps-tdup/setup -c
    ```

    Not a graphic version is not available is not available for itps components and as such you must select the command line interactive setup option. This will automatically install to

    ```
    /opt/itps-tdup
    ```

9.  If the webserver is not running you will get an error saying "Reconfigure Failed" this can be ignored at this stage.The following defaults are recommended:

[0] Installation Location /opt/itps-tdup

[1] The user that will run TooledUp? tbase
[2] The group that this user belongs to? iplanet

[3] The Web server location is [ /opt/iws6 ]

[4] The Web server instance is [ myhost.mycompany.com ]

[5] The virtual server id is [ https-myhost.mycompany.com ]

[6] The deployment location [ /opt/iws6/itps-tdup-deploy ]

[7] The keystore password is [ password ]

[8] The signing certificate alias [ ClientSC ]

[9] The SSL client certificate alias [ ClientSSL ]

[10] The trusted verification certificate alias [ IRCA ]

[11] The database user is [ tbase ]

[12] The database password is [ tbase ]

[13] The database host is [ mydatabase.mycompany.com ]

[14] The database port is [ 1521 ]

[15] The database sid is [ orcl ]

**10.** Log onto your oracle account and run the script
/opt/itps-tdup/SQLscripts/install_merchant_oraUpgradeNew.sql

**11.** Oracle on same machine as iTPS. Alternatively this can be an Oracle client.

   **a.** Assuming the sql directory has been copied to the DB server, log on to the database server, su - oracle

   **b.** Change to directory e.g.

   cd /opt/itps-tdup/SQLscripts

   **c.** Run SQLPlus and enter the username and password

   **d.** Execute the script e.g. sqlplus>@install_merchant_oraUpgradeNew.sql;

   **e.** Exit SQLPlus & the Oracle user.

**12.** Oracle on different machine as iTPS. For example:

   **a.** cd /opt/itps-tdup/SQLscripts

   **b.** ftp mydatabase.mycompany.com <username><password>

```
ftp> hash
ftp> prompt
ftp> mput *
ftp> quit
```

   **c.** telnet mydatabase.mycompany.com <username><password>

   **d.** sqlplus tbase/tbase

   **e.** @install_merchant_oraUpgradeNew.sql;

This installation area now contains several directories and files that are detailed below:

   ○ /opt/itps-tdup/scripts : This directory contains the install scripts and any data they need.

   ○ /opt/itps-tdup/SQLscripts : This directory contains the SQL database creation scripts that will create the tables that tooledup needs to run.

   ○ /opt/itps-tdup/bin : This directory contains the binaries ( shared-objects ) that tooledup needs to run.

In order to use the Tooled up sellers application you will need a SmartCard that will be issued to you by a third party vendor that contains an end entity signing certificate that has been issued by the Sellers Bank CA.

**13.** Restart the iws6 to be able to access the newly installed web application.You are now ready to run tooledup, access the url tooledup url e.g. http://myhost.mycompany.com:86/itps-tdup/logon.html

The following screen appears:

**Figure  2-15**     Sellers Website Tooled Up Welcome Screen
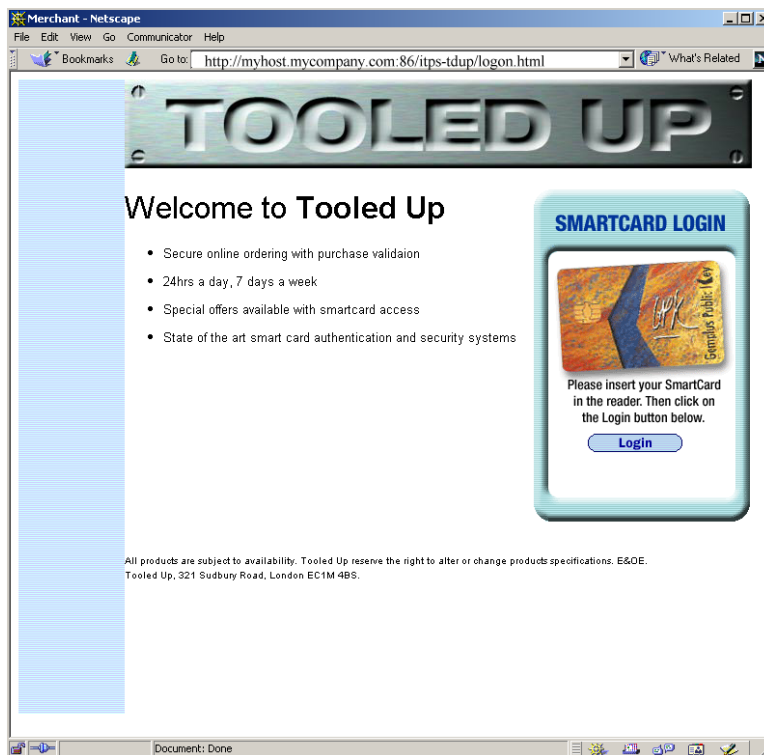


Make sure the server publishes the pages in the same language as the browser. For example

```
cp /opt/itps-tdup/jsp/en /opt/itps-tdup/<locale>
```

where <locale> is the language you are using.

# Error checking

If there was a problem you should check the following error logs

```
/opt/ittm/Scripts/*.log
```

```
/opt/iws6/https-myhost/logs/errors
```

```
/opt/ias6/ias/logs
```

```
/var/sadm/install/logs
```

```
/opt/ittm/Scripts/regservlet.output
```

In order to test that a complete iTPS, and all its associated components, are installed and configured successfully you should attempt to make a payment through tooledup. Consult the Administrators guide for more details on this.

# Backup, Uninstall, Reinstall and Restore

This chapter discusses how you can reinstall your system.

# Overview

We now discuss a procedure for backing up key configuration data and installation settings prior to uninstalling, reinstalling and restoring saved parameters. This procedure can be applied for as many or as few packages or components as you wish.

1. Uninstall iTPS

1. iTTM Uninstall

   Consult the iTTM manual

2. Save your itps component settings. The following options illustrate how to save the settings you used for itps-biab. For example,

   ```
   /cdrom/cdrom0/itps-biab/setup -m /outputdir/itps-biab
   ```

3. Remove iTPS components. For instance,

   ```
   /cdrom/cdrom0/itps-biab/setup -u
   ```

4. iWS 6.0 SP2Uninstall

   For those versions of software placed on an iWS 6.0 it may be possible to reinstall iTPS without having to reinstall the entire Web Server and all its instances. See

   http://docs.iplanet.com/docs/manuals/enterprise/50/ig/unix.htm

5. iTPS 2.0 Reinstall. Repeat the instructions in this manual. Note, however, In this case it is possible to reinstall the components using previous settings

   ```
   cd /opt
   ```

   ```
   /cdrom/cdrom0/itps-biab/setup -s /outputdir/itps-biab
   ```

6. You may need to remove your iTPS Oracle database. In some cases scripts are provided for you.

# Example walkthrough

Reinstallation splits into four main steps

1.  Backup

2.  Uninstall

3.  Reinstall

4.  Restore

Stop the jmqbroker using <CTRL-C> . This will have a knock on effect of correctly stopping the biab and jmsproxy processes. Stop ias using the script /opt/ittm/Scripts/stopias. It is assumed that a directory called /temp exists for storing config info required during the re-install:

## Backup

Backup should be done from the user account. For instance user: tbase group: iplanet.

| Step | Description of backup steps |
|------|------------------------------|
| 1 | Backup TokenKeystore cert databases (Only need *.db and identrus.domain but copy the whole hostname directory for simplicity): |
|   | cp /opt/ittm/store /temp |
|   | cp /opt/ittm/myhost/* /temp |
|   | From the configuration screen select <config><export> |
| 2 | Backup the component website configurations to allow a quick and accurate re-install e.g.: |
|   | ./cdrom/cdrom0/itps-biab/setup -m /outputdir/itps-biab |
| 3 | Backup TooledUp table cdpcert and CDP_issuer_DN, email, and CDP_DN entries: |
|   | cd /temp |
|   | Logon to database as TooledUp user and: |
|   | spool cdpcerts.txt |
|   | select * from cdpcert; |
| 4 | Backup userdb users to a text file: |
|   | ./runuserdbtool |
|   | lookupusers |
|   |   |
|   | In another window, vi /temp/userdbusers.txt |
|   | Paste in all user info from other window and save file. |
| 5 | Backup Membership details: |
|   | Access each membership entry and copy each required line to a text file (e.g. /temp/config.txt) to aid with adding them back accurately. |
| 6 | Backup Authorisation cert details to /temp/config.txt |
|   | To aid adding it back accurately. |

# Uninstall

Uninstall should be done from the root account.

| Step | Description of uninstall steps |
|------|-------------------------------|
| 1 | Run uninstall script for iTTM:<br><br>./cdrom/cdrom0/ittm/setup -u<br><br>./cdrom/cdrom0/itps/setup -u |
| 2 | Remove the install directory:<br><br>rm –r /opt/ittm |
| 3 | Make sure that all the /opt/{package} directories are gone and that the deploy directories from the webserver root are also gone. If not, then remove manually. for instance,<br><br>./cdrom/cdrom0/itps-biab/setup -u<br><br>Also delete all jsps from each webserver instance e.g.<br><br>cd /{server_root}/{instance}/ClassCache/https-{instance}<br><br>rm –r * |
| 4 | Log on to database as user for iTTM and run Drop scripts:<br><br>@Drop_PaymentsAll<br><br>@Drop_tbaseAll<br><br>@Drop_biab<br><br>commit;<br><br>Now manually drop views and functions that were not dropped by the script (if any):<br><br>drop view errorview<br><br>drop view raw_data_payments_view<br><br>drop function biab_req_insert<br><br>commit;<br><br>Log on as tdup user :<br><br>@Drop_merchantAll |

# Reinstall

Reinstall should be done from the root account

| Step | Description of Re-installation steps |
|------|--------------------------------------|
| 1 | Tidy up SLAPD processes. Kill any running and then<br><br>cd /ias_root/start-myhost<br><br>./start-slapd |
| 2 | Reinstall ittm using the settings you saved<br><br>/cdrom/cdrom0/ittm/setup -s /outputdir/ittm<br><br>or using a graphical or command line install, for instance:<br><br>cp /cdrom/cdrom0/ittm/* .<br><br>./setup -g<br><br>The settings you used previously can be found in /temp/myhost/*.properties |
| 3 | Select all three components<br><br>iTTM<br><br>OCSPResponder<br><br>JMSProxy |
| 5 | Now install itps:<br><br>.<br><br>./cdrom/cdrom0/itps/setup -s /outputdir/itps |
| 6 | Re-install the component websites. For instance,<br><br>./cdrom/cdrom0/itps-biab/setup -s /outputdir/itps-biab |

# Restore

Restore should be done from the user account. For instance user: tbase group: iplanet.

| Step | Description of restore steps |
|------|------------------------------|
| 1 | Copy your tokenkeystore cert database back into ittm: <br><br> cp /temp/*.properties /opt/ittm/host <br><br> cp -r /temp/store/* /opt/ittm/store <br><br> cp -r /temp/xmlconfig /opt/ittm/myhost <br><br> From the iTTM configuration screen select <config><import> |
| 2 | Now re-instate database tables for ittm, itps, biab and tdup: <br><br> ftp ALL the sql files from the installation to your database host machine. <br><br> Required Files are in: <br><br> /opt/ittm/current/Config/sql <br><br> /opt/itps-biab/config/sql <br><br> /opt/itps-tdup/SQLscripts <br><br><br> Logging on to database host as applicable users for each component if they are different: <br><br> Logon as ittm user: <br><br> @tbaseNew <br><br> @PaymentsNew <br><br> @biabNew <br><br> commit; <br><br> Logon as TooledUp database user (if different): <br><br> @install_merchant_oraUpgradeNew <br><br> Use DBVisualiser OR Logon as TooledUp database user: <br><br> Re-instate CDPCERT entry (saved to a text file /temp/cdpcert.txt for use by TooledUp, e.g. <br><br> Update table CDPCERT set CDP_ISSUER_DN='CN=??????', CDP_DN='CN=?????', email='CDPUser@cdphost.com' |

| 3 | Now add admin user to BiaB: |
|---|---|
| | cd /opt/itps-biab/scripts |
| | ./biab –admin |
| | adduser admin admin |
| | exit |
| 4 | Re-instate userdb users: |
| | cd /opt/ittm |
| | ./runuserdbtool |
| | |
| | Add roles for SELLER, BUYER, BANK and organisation of "SPD:seller.name" |
| | Then adduser, for each saved set of user info from the uninstall process. . |
| 5 | Restart all your webserver instances |
| | If they fail then you might need to manually kill them first. If they still fail then you may need to check the contents of /{server_root}/{instance}/config/web-apps.xml |
| | and magnus.conf, and the back-up copies in the webservers. |
| 6 | Now restart your F.I. using different open windows: |
| | cd /opt/itps-biab/scripts |
| | /biab –debug |
| | cd /opt/ittm/Scripts (assuming you are using the provided SSL Proxy) |
| | ./starttbase |
| | cd /opt/ittm/Scripts |
| | ./startias |

| 7 | Log in to tbase and Re-instate all Configuration info from text file /temp/config.txt |
| | Add Authorisation Cert |
| | Add Membership details |
| | Add Settlement Chain |
| | Add Condition Registry URL |
| | |
| | And recheck any settings that are not required to be default. |
| | |
| | Restart ias because Authorisation setting is NOT dynamic. |
| 8 | Use TooledUp to do a quick integrity check. Send a Conditional Payment Request and check that no emails were sent. Then go to BiaB to do a PayInst Ack and check that the correct emails have been sent. |
| | Then go to CR website at BFI and Discharge the condition, check again for email acknowledgements. |

# Patches (for future use)

To Add/Patch a package (For future use only). This will patch all packages it finds in the distribution directory. From user: root

```
./cdrom/cdrom0/<itps_component_install_directory>/setup -p
```

Where <itps_componet_install_directory> is the location of the installed software that needs patching. For example:

```
/cdrom/cdrom0/itps-biab/setup -p
```

# Chapter 4

# Migration

This chapter discusses how you can migrate your system from

iTTM 2.2.1 and iTPS 1.0

to

iTTM 3.0.1 and iTPS 2.0

# Upgrade Procedure

To upgrade from an existing iTPS 1.0/iTTM 2.2.1 installation, the following procedure should be followed:

1. Follow the instructions in the iTTM 2.2.1 Installation and Configuration Guide on how to stop iTTM

2. Installation of iWS6.0 SP2. iWS must be upgraded to iWS6.0 SP2

   a. This requires a removal of your existing iWS and iAS. Before doing so it is advisable to stop the web servers from running.

   See http://docs.iplanet.com/docs/manuals/fasttrak/41/ig/unix.htm

   Or http://docs.iplanet.com/docs/manuals/enterprise/50/ig/unix.htm

   Go to the iWS install directory (typically /opt/netscape/server4 for iWS4.1 and /opt/iws6 for iWS6.0) and type

   ```
   cd /opt/iws6

   ./uninstall

   rm -rf /opt/iws6
   ```

   b. Now consult the iTTM 3.0.1 Installation and Configuration Guide for details on how to install iWS 6.0 SP2:

   ```
   http://docs.sun.com/source/816-6283-10/index.html
   ```

3. Installation of iAS 6.5

   a. Remove iAS6.0. Before doing so it is advisable to stop the application server from running. See

   http://docs.iplanet.com/docs/manuals/ias.html#sp3

   Go to the <ias_install_directory> (typically /opt/ias6) and type

   ```
   cd /opt/ias6

   ./uninstall

   rm -rf /opt/ias6
   ```

   b. Now consult the iTTM 3.0.1 Installation and Configuration Guide for details on how to install iAS 6.5:

   ```
   http://docs.sun.com/source/816-6283-10/index.html
   ```

**4.** iMQ for Java. You will need to reinstall and reconfigure iMQ for java with iAS. You should uninstall imq for java 2.0 using the instructions in the IMQ for java guide found in

```
http://docs.sun.com/db/prod/s1.ipmsgquj
```

```
http://docs.iplanet.com/docs/manuals/javamq/20/install.pdf
```

and reinstall and reconfigure using the section in this manual "iPlanet Message Queue for Java 2.0 (step 2b)," on page 51

**5.** Application of the upgrade script itself

```
cd /cdrom/cdrom0/upgrade
```

```
./upgrade
```

This asks the following questions

[0] Install location [/opt/ittm]: /opt/ittm

[1] The root location of iPlanet Application Server ? /opt/ias6

[2] The root location of iPlanet Web Server documents directory? /opt/iws6/docs

[3] Enter the password to use for the tokenkeystore? password

[4] The user that will start iTTM ? tbase

[5] The group that this user belongs to ? iplanet

[6] On what host is your iTTM iPlanet Web Server ? [ myhost.uk.sun.com ]

[7] On what HTTP port is your iTTM iPlanet Webserver running ? [ 80 ]

the script will also ask for confirmation before converting the certificate store to the new token key store format. Type <y> and <return> to generate the token key store. Pressing <return> to accept the default <n> will require that you run the following script later:

```
/opt/ittm/Scripts/ncipherupgrade
```

Note also that the conversion of the certificate store will fail if the ncipher box is not available

6. SQL Scripts to update your database can be found in

   ```
   /opt/ittm/current/Config/sql/tbaseUpgrade3_0.sql
   ```

   ```
   /opt/ittm/current/Config/sql/PaymentsUpgrade2_0.sql
   ```

   There is no upgrade path for Biab and Tooledup as such these databases will have to be reconfigured from scratch. Remove the existing iTPS component database as follows:

   ```
   @Drop_biab
   ```

   ```
   commit;
   ```

   ```
   Now manually drop views and functions that were not dropped by
   the script (if any):
   ```

   ```
   drop view errorview
   ```

   ```
   drop view raw_data_payments_view
   ```

   ```
   drop function biab_req_insert
   ```

   ```
   commit;
   ```

   ```
   Log on as tdup user :
   ```

   ```
   @Drop_merchantAll
   ```

7. You should uninstall all existing iTPS 1.0 components and reinstall iTPS 2.0 components from the cdrom by following the instructions in this guide:

   a. Before you install any component you will also first need to reinstall a Web Server instance for that component: See"Installing the iWS 6.0 (step 4a)," on page 83

   b. "BiaB Back End office simulator (step 3c)," on page 70

   c. "BiaB Admin Tool (step 3d)," on page 74

   d. "Installing Buyers Bank Website (step 4b)," on page 84

   e. "Seller's Website TooledUp (step 4c)," on page 89

8. You should install all new iTPS 2.0 components from the cdrom by following the instructions in this guide:

   a. "Condition Management Website (step 3e)," on page 76

   b. "Obligation Management Website (step 3f)," on page 80

9. Follow the iTTM 3.0.1 Installation and Configuration guide on how to Install

• OCSP Responder

• JMSProxy.

10. If jmsproxy.properties was in existence previously, this will have been preserved. If not, defaults will have been installed and this may need configuring

11. You should consult the Installation chapter of the iTTM 3.0.1 Installation and Configuration Guide. The following needs to be configured:

   a. The section on secure properties.

   b. Configure the iWS for URL rewriting and SSL Decryption

12. The configuration settings that you had with iTTM 2.2.1 are set automatically. For new configuration, consult the iTTM 3.0.1 Installation and Configuration Guide.

# Reverting

If an error occurs during the script the original installation can be recovered using the revert script. This will return the iTTM installation to its state before the first time the upgrade script was run.

```
cd /cdrom/cdrom0/upgrade

./revert
```

Numbered backups are made with each running of the upgrade script. However, revert will always restore from the last backup. Thus, to restore from an earlier backup, remove the first numbered backup after this version. Backups are named

```
<old ittm directory>.old.<version>
```

You can also revert your database using the following sql scripts

```
/opt/ittm/current/Config/sql/Drop_Payments2_0

/opt/ittm/current/Config/sql/Drop_tbase3_0
```

There is no revert procedure for Biab and TooledUp. Once you get the system to an old state it is then possible to run the upgrade script again.

# Advanced Silent Install options

iTPS Silent install has been designed so that the following kinds of installations are possible:

- Reinstallation

- Installing a similar installation on other machines is facilitated by editing a file that contains a list of settings.

- Seamless upgrades and patches for future distributions are now also possible.

The procedure for performing these kinds of installations can be found below:

1. Gather appropriate information in order to assist a silent iTTM 3.0.1 install

    a. To ask for command line answers and place the answers to questions in the directory /outputdir that can then be edited and used to do installs on other machines.

    `./cdrom/cdrom0/itps/setup -k /outputdir`

    b. To gather settings from existing packages and place the answers to questions in the directory /outputdir that can then be edited and used to do installs on other machines.

    `./cdrom/cdrom0/itps/setup -m /outputdir`

**2.** Perform the actual iTPS Installation using one of the following procedures

    **a.** To perform a complete graphic install on the entire product (itps only and not itps components)

```
./cdrom/cdrom0/itps/setup -g
```

    **b.** To perform a complete command line install on the entire product entering answers to questions at the terminal

```
./cdrom/cdrom0/itps/setup -c
```

    **c.** To perform a complete command line install from a file created in /outputdir and read from /inputdir. The output will also be sent to a log file

```
./cdrom/cdrom0/itps/setup -k /outputdir
```

```
./cdrom/cdrom0/itps/setup -s /inputdir logfilename
```

    **d.** To perform a complete command line install from existing package settings in order to perform a new install on a different machine created in /outputdir and read from /inputdir. The output will be sent to a log file.

```
./cdrom/cdrom0/itps/setup -m /outputdir
```

```
./cdrom/cdrom0/itps/setup -s /inputdir logfilename
```

# Glossary

| | |
|---|---|
| **Asynchronous Message** | (See also Eleanor Technical Specification and also Synchronous message) means that messages can be sent over a delayed time frame. Following a request, a response can be sent at any time. Whereas with a Synchronous message following a request the system waits until it gets a response. |
| **Bank Name** | The name of the Scheme Member to whom this entry relates. |
| **BIC-11** | is an 11 digit Bank Identifier Code. The Bank Identifier Code is a unique address which, in telecommunication messages, identifies precisely the financial institutions involved in financial transactions. The BIC Directory Site can be found at http://www.bicdirectory.swift.com/. |
| **BFI** | (See also Eleanor Technical Specification) The Buyers Bank or in Identrus terminology the IP. |
| **BFIM** | (See also Eleanor Technical Specification) This is the model used for making a payment. The instruction is submitted by the submitting Corporate through the Buyer Financial Institution. |
| **Biab** | Bank in a Box |
| **Buyer** | The Buyer wants to purchase goods or services from the Seller. The Buyer is in possession of an Identrus smartcard. The Buyer is granted access to the payment facility by his bank. This is also abbreviated as BU in the Eleanor Scheme and as the SC in the Identrus four corner model |
| **Buyers Bank** | The Buyer's Bank manages the Buyer's account from which payment is to be made. The Buyer's Bank issues the Buyer with his Identrus smartcard. The Buyer's Bank is a member of the Identrus schemes. |
| **Cache** | A cache is a 'local' store used to hold recently accessed information, so that if further access is required a local copy may be used rather than a 'remote' copy. In most schemes this specifically refers to a local store containing copies of responses from the Identrus Root to certificate status checks. |
| **Cancellation** | A cancellation is the revocation of a Payment Request. It may only be applied to a Payment Request, not the payment. Therefore payments that have been paid cannot be cancelled by this method. |
| **Certified Payment Obligation (xPC)** | Where an Assured Payment is used, the Buyer requests the Buyer's Bank to underwrite (or assure) the payment to the Seller. |
| **Certified Conditional Payment Obligation (CPC)** | This product has the same core characteristics as the Payment Obligation product, with the additional requirement that payment will not be released until evidence that all conditions attached to the payment have been met or |

waived. Since its certified the BFI is obliged to make the payment since the Buyer requests the Buyer's Bank to underwrite (or assure) the payment to the Seller.

**Conditional Payment Order (CPx)**    The Conditional Payment Order has the same core characteristics as the Payment Order product with the additional requirement that payment will not be released until evidence that all conditions attached to the payment have been met or waived. This product is also unilaterally revocable by the Buyer.

**Conditional Payment Obligation (CPO)**    The Conditional Payment Obligation has the same core characteristics as the payment Obligation product, with the additional requirement that payment will not be released until evidence that all conditions attached to the payment have been met or waived. As with the Payment Obligation, the Buyers Financial institution is not obliged to make the payment if, for instance, there are insufficient funds available in the Buyers account, and the product is bilaterally revocable.

**CMS**    iPlanet Certificate Management System

**CPI**    Corporate Payment Initiation API Library

**Customer**    For the purposes of this document this term describes a customer of a Member. of the Identrus Scheme.

**FI Code**    A BIC-11 code owned by the Scheme Member to whom this entry relates.

**Identrus four-corner Model**    This describes the four parties involved in an Identrus enabled transaction, namely two banks and their respective customers. Where two customers have the same bank, only three parties are involved, and this is known as a 'three party' model.

**Identrus Root**    The Identrus Root manages membership of the Identrus scheme. The Buyer's Bank and Seller's Bank verify each other's identity via the Identrus Root.

**Issuing Participant (IP)**    In the Identrus four-corner model this refers to the level 1 Identrus participant that issued the certificate to the Subscribing customer. This equates to "Buyer's Bank" in other payment transaction

**iWS**    iPlanet Web Server

**iAS**    iPlanet Application Server

**iTTM**    iPlanet Trustbase Transaction Manager

**iMQ**    iPlanet Message Queue

**iMS**    iPlanet Messaging System

| | |
|---|---|
| **iTPS** | iPlanet Trustbase Payment Services |
| **JMS** | is an API. Many implementations of JMS are available from different providers (like IBM MQ and iMQ) and any of them can be used with iTPS |
| **Membership** | The current status of the institution concerned. This can take the values Pending, Active, Suspended, Terminated. |
| **Payment Order (xPx)** | A Payment order is a revocable, unconditional electronic instruction from the Buyer requesting the Buyer's Bank to execute a credit payment to the Seller on a specific date for a specified amount. |
| **Payment Obligation (xPO)** | The commitment from a Buyer to pay a Seller a specified amount on a specified date. There is no obligation on the Buyers Financial Institution to pay if there are insufficient funds available on the due date. The instruction is only revocable bilaterally, i.e. with the assent of the current Holder of the obligation. This product is only supported in the SFI Model, although it will be possible to build it into a procurement application using the CPI library. |
| **Relying Customer (RC)** | In the Identrus four-corner model this is the organisation that relies on the identity of the Subscribing customer in order to conduct trade. This equates to 'Seller' in a payment transaction. |
| **Relying Participant (RP)** | This refers to the Relying Customer's bank. This equates to "Seller's Bank" in a payment transaction. |
| **Service** | The current status of a service. This is used to mark temporary service interruptions. The allowed values are Available and Unavailable. |
| **Seller** | The Seller wants to supply goods or services to the Buyer. The Seller is in possession of an Identrus private key. The Seller is granted access to the payment facility by his bank. This is also abbreviated as SE in the Eleanor Scheme and as the RC in the Identrus four corner model. |
| **Sellers Bank** | The Seller's Bank manages the Seller's account into which payment is to be made. The Seller's Bank is a member of the Identrus schemes. |
| **SFI** | (See also Eleanor Technical Specification) The Sellers Bank or in Identrus terminology the RP |
| **SFIM** | (See also Eleanor Technical Specification) This is the model used for initiating a payment.The instruction is submitted by the submitting Corporate through the Seller Financial Institution. This is essentially the same as the Identrus four corner model. |

| | |
|---|---|
| **Scheme Register** | (See also Eleanor Technical Specification) The Eleanor Scheme has membership criteria. Each participating Financial Institution ensures that corresponding institutions are members of the scheme. It does so via an XML message that is referred to as a scheme register. |
| **Subscribing Customer (SC)** | In the Identrus four-corner model this is the end customer of the Identrus enabled service. This equates to the 'Buyer' in a payment transaction. |
| **Synchronous Message** | (See also Eleanor Technical Specification) See Asynchronous Message.(See also Eleanor Technical Specification and also Synchronous message) means that messages cannot be sent over a delayed time frame. Following a request, a response is sent immediately before the system can proceed. Whereas with an asynchronous message, following a request, a response can be sent at anytime. |
| **Timeout** | is the amount of time (in seconds) for which a client will wait for a server to respond before dropping the connection and returning with a timeout error. In the context of these screens, it is the amount of time the Seller's Bank will wait for the Buyer's Bank to respond. |
| **Transaction** | This refers to a complete end to end transaction, potentially involving multiple request-response pairs. Where a single message in such a transaction is referred to the term 'message' is used. |
| **Transaction Reference** | (See also Eleanor Technical Specification) The provision and handling of transaction references is key to allowing the Eleanor Payment products to be used effectively from third party systems and to assist in reconciliation of data |

# Index

## A

Asynchronous Message  116, 119

## B

Backend Bank in the Box Welcome Screen  75
Bank in a box  10, 37
Bank Name  116
BFI  116
BFIM  37, 116
BIC-11  116, 117
Buyer  28, 29, 30, 31, 33, 34, 35, 36, 37, 116, 117, 118, 119
Buyers Bank  10, 31, 84, 116
Buyers Website (BFIM)  37

## C

cache  116
Cancellation  116
Certified Payment Obligation  28, 116
Component Selection  63
Corporate Payment Initiation Library API  38
Customer  27, 37, 117, 118, 119

# D

Database Settings  59

# E

Eleanor  11, 30, 31, 33, 116, 118, 119

# F

FI Code  117
Four Corner Payment Model (SFIM)  33
Four Corner Payment Processing  33

# G

Glossary  115

# H

HTTP  98

# I

Identrus Four-Corner Model  32, 117, 118, 119
Identrus four-corner Model  32, 117, 118, 119
Identrus Root  116, 117
Installation  41, 58, 62, 66
Installation Summary  66
Installing Bank in the Box  74
Installing Buyers Bank  84
Installing iPlanet Trustbase Payment Services  10, 57
Introduction  9, 10, 27
iPlanet Message Queue for Java 1.0  51

# J

# L

# M

# O

# P

# R

# S

# T

# U