OWNER:	ISSUE DATE:	VERSION:
DG TAXUD	15/07/2011	1.04

TAXATION AND CUSTOMS UNION DG

EMCS COMPUTERISATION PROJECT PHASE 3

PROJECT SPECIFICATIONS, DEVELOPMENT, MAINTENANCE AND SUPPORT OF EUROPEAN IT SERVICES IN THE AREA OF TAXATION AND EXCISE

Subject:

TA Installation Procedure Manual

(ECP3-FITSDEV2-TA-IPM)

Framework Contract TAXUD/[Removed]

Specific Contract No. [Removed]

Document History

Edi.	Rev.	Date	Description	Action (*)	Sections
0.01	01	18/10/2010	First draft. Submitted for internal Technical and Quality review.	I	All
0	01	18/10/2010	Upon internal review submitted to DG TAXUD for review.	U	As required
1	00	29/10/2010	Incorporated review comments. Submitted to DG TAXUD for acceptance.	I	All
1	01	26/01/2011	Upon internal review submitted to DG TAXUD for review.	I	All
1	02	24/05/2011	Added Section 15 – 'QUICK-UPLOAD Through The Web Interface'. Upon internal review submitted to DG TAXUD for review.	I	As required
1	03	02/06/2011	Incorporated review comments. Submitted to DG TAXUD for acceptance.	U	All
1	04	15/07/2011	Updated the database parameter "Open Cursors". Submitted to DG TAXUD for Information.	U	As required

(*) I = Insert, R = Replace, U = Update.

Table of Contents

List of Tables

List of Figures

1   INTRODUCTION

1.1   PURPOSE OF THE DOCUMENT

The aim of this document is to describe the Testing Application (TA) installation procedure.

1.2   SCOPE OF THE DOCUMENT

The scope of the present document is the installation of the TA software upon its required infrastructure (see section 3 Infrastructure Requirements). The installation and configuration of all other hardware or software products and tools required by TA is outside the scope of this document.

1.3   INTENDED READERSHIP

This document is for Common Domain users responsible for the installation and configuration of the TA into the Common Domain.

1.4   STRUCTURE OF THE DOCUMENT

This document is structured as follows:

- Chapter 1 'Introduction' summarizes the purpose and the scope of this document, lists the referenced or applicable documents and defines abbreviations, acronyms and definitions that are used in the document;
- Chapter 2 'Installation Procedure Overview' provides an overview of the installation process;
- Chapter 3 'Infrastructure Requirements' describes the environment needed in order to install TA;
- Chapter 4 'Create CCN/CSI Resources' describes the procedure to be followed to create CCN/CSI resources required by TA;
- Chapter 5 'Create the TA Database' describes the steps required to create the database and database objects used by TA;
- Chapter 6 'Configure WebLogic Server Instance' describes the procedure to be followed to create the BEA WebLogic resources required by TA;
- Chapter 7 'Configure TA Application' describes the steps to be followed in order to configure the application for build;
- Chapter 8 'Build the TA application' describes the steps required to build the TA;
- Chapter 9 'Deploy the TA Application' describes the procedure used for deploying the TA on WebLogic server;
- Chapter 10 'Install the CSI portdaemon' describes the procedure for installing the CSI port daemon;
- Chapter 11 'One-click upload' describes the upload of CTP entities into TA;
- Chapter 12 'Ctp Documents Update' describes the upload of CTP Documents into TA database and update of the CTP version;
- Chapter 13 'DDNEA Main Document Update' describes the way this document is uploaded into TA database and update of the DDNEA version;
- Chapter 14 'TA Version Update' describes the way the TA Version can be updated;

- Chapter 15 'QUICK-UPLOAD Through the Web Interface' describes the process of Uploading CTP Entities, CTP, DDNEA and TA Documents into TA database through the web interface;
- 'Annexes' provides complementary information on TA.

1.5 REFERENCE AND APPLICABLE DOCUMENTS

1.5.1 REFERENCE DOCUMENTS

Ref.	Reference	Title	Version
R01	ECP1-ESS-GLT	EMCS COMPUTERISATION PROJECT Glossary of Terms (GLT)	2.04
R02	ECP1-ESS-FESS	Functional Excise System Specifications (FESS)	3.41
R05	ECP3-FITSDEV2-TA-TST	Test Plan for TA	1.08
R06	ECP3-FITSDEV2-TA-OPM	TA Operation Manual	1.01
R07	ECP3-FITSDEV2-TA-UMN	TA User Manual	1.01
R08	ECP3-FITSDEV2-DDNEA	DDNEA for EMCS Phase 3	1.51
R09	ECP2-FITSDEV2-DDNEA	DDNEA for EMCS Phase 2	3.02
R10	ECP2-EMCSDEV-CTP	Conformance Test Protocol	2.08
R11	ECP3-EMCSDEV-CTP	Conformance Test Protocol	1.42

Table 1-1: Reference Documents

1.5.2 APPLICABLE DOCUMENTS

Ref.	Reference	Title	Version
A01	FITSDEV2-SC01-FQP	Framework Quality Plan	1.01
A02	FITSDEV2-SC03-CQP	Contract Quality Plan	1.00

Table 1-2: Applicable Documents

1.6 ABBREVIATIONS AND ACRONYMS

Abbreviation	Meaning
AAD	Administrative Accompanying Document
e-AD	Electronic Administrative Accompanying Document
ARC	AAD Reference Code
BPEE	Business Process Execution Engine
CCN	Common Communication Network
CCN/CSI	Common Communication Network/Common System Interface
CCN-TC	Common Communication Network - Technical Centre

Abbreviation	Meaning
CSI	Common System Interface
DBMS	Database Management System
DDL	Data Description Language
DDNEA	Design Document for National Excise Applications
DG TAXUD	Taxation and Customs Union DG
DML	Data Manipulation Language
ECP	EMCS Computerisation Project
EMCS	Excise Movement Control System
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GB	Gigabyte
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDL	Interface Definition Language
IP	Internet Protocol
IPM	Installation Procedure Manual
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
JNDI	Java Naming and Directory Interface
LCT	Local Conformance Testing
LST	Local Site Testing
MHz	Megahertz
MSA	Member State Administration
ND	National Domain
NDEA	Nationally Developed Excise Applications
PC	Personal Computer
RAM	Random Access Memory
SMF	Service Management Facility
SQL	Structured Query Language
SQP	Specific Quality Plan
T3	A proprietary protocol developed by BEA Systems
TA	Testing Applications
TCP/IP	Transmission Control Protocol/ Internet Protocol
UI	User Interface
WAR	Web Application Archive
WLS	WebLogic Server

Table 1-3: Abbreviations and Acronyms

2   INSTALATION PROCEDURE OVERVIEW

2.1 SYSTEM OVERVIEW

2.1.1 LOGICAL VIEW

TA consists of two modules:

- Testing Application Core Module

- Testing Application Web Module

The TA Core Module is based on service components that describe services having related functionalities
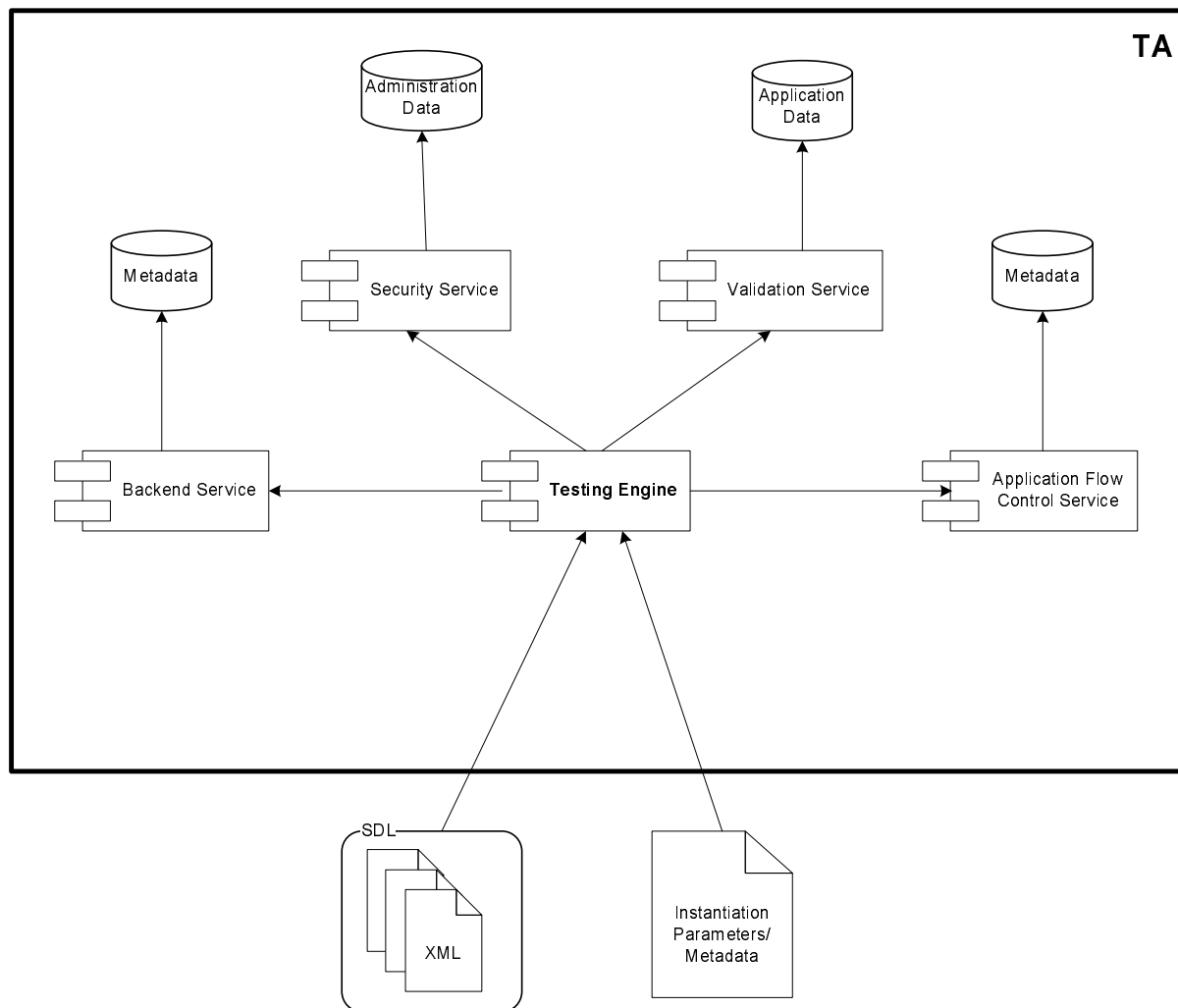
Figure 2-1: TA Core Module Component Architecture View

TA Core module defines the following components, as shown in the above figure:

Component	Purpose
Testing Engine	Is able to read scenarios exported from CTP as well as identify and execute

Component	Purpose
	actions described in the Scenario Definition Language.
Validation Service	Is responsible for four validation types, as follows: syntax, semantic, field-by-field and sequence.
Backend Service	Manages access to data resources and performs message instantiation and archiving operations.
Application Flow Control Service	Provides the communication means between TA deployed in the Common Domain and NEA under test deployed in the National Domain.
Security Service	Provides authentication security services to the internal users (system administrator) and authorisation security services to the external users (MSA operators).

Table 2-1: System Overview - Service Components

The TA Web Module is based on three-tier software architecture. The following diagram presents its architecture:
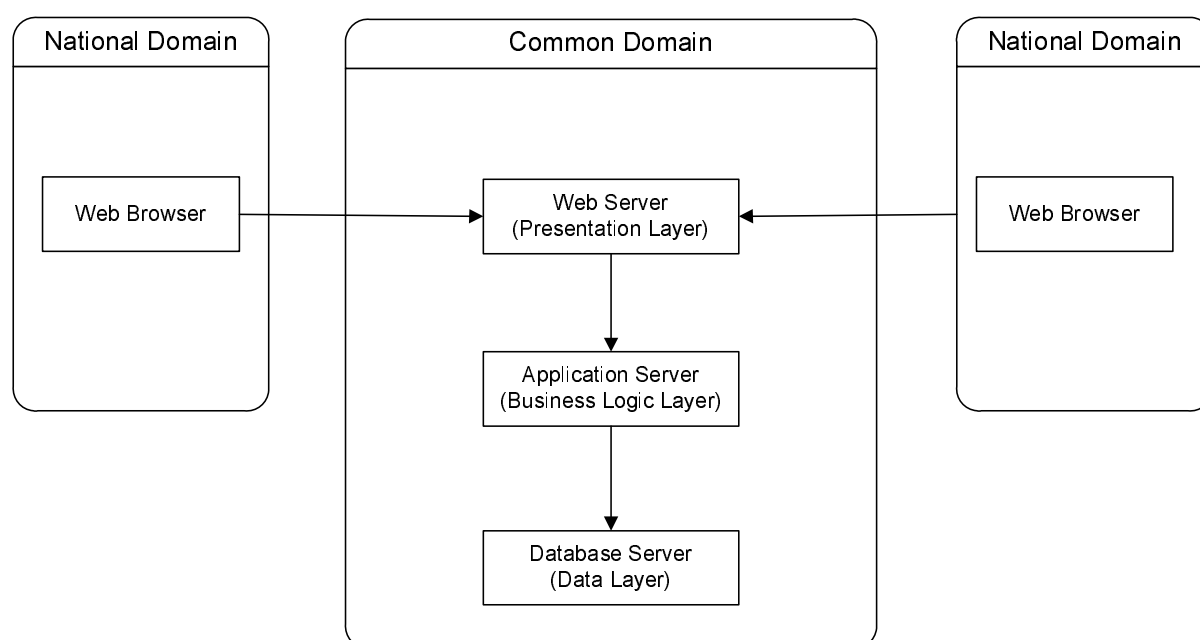
Figure 2-2: TA Web Module Architecture View

- o *The Presentation Layer* is the top-most level of the application and represents the GUI (Graphical User Interface). The main function of the user interface is to translate information from *The Business Logic Layer* to something the user can understand (i.e. a HTML page).

- o *The Business Logic Layer* is the layer that coordinates the application, processes commands, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers: *The Presentation Layer* and *The Data Layer*.

- o *The Data Layer* is where the information is stored and retrieved from a database system. The information is then passed back to *The Business Logic Layer* for processing, and then eventually back to *The Presentation Layer*.

2.1.2 DEPLOYMENT VIEW

The TA deployment topology is shown below:
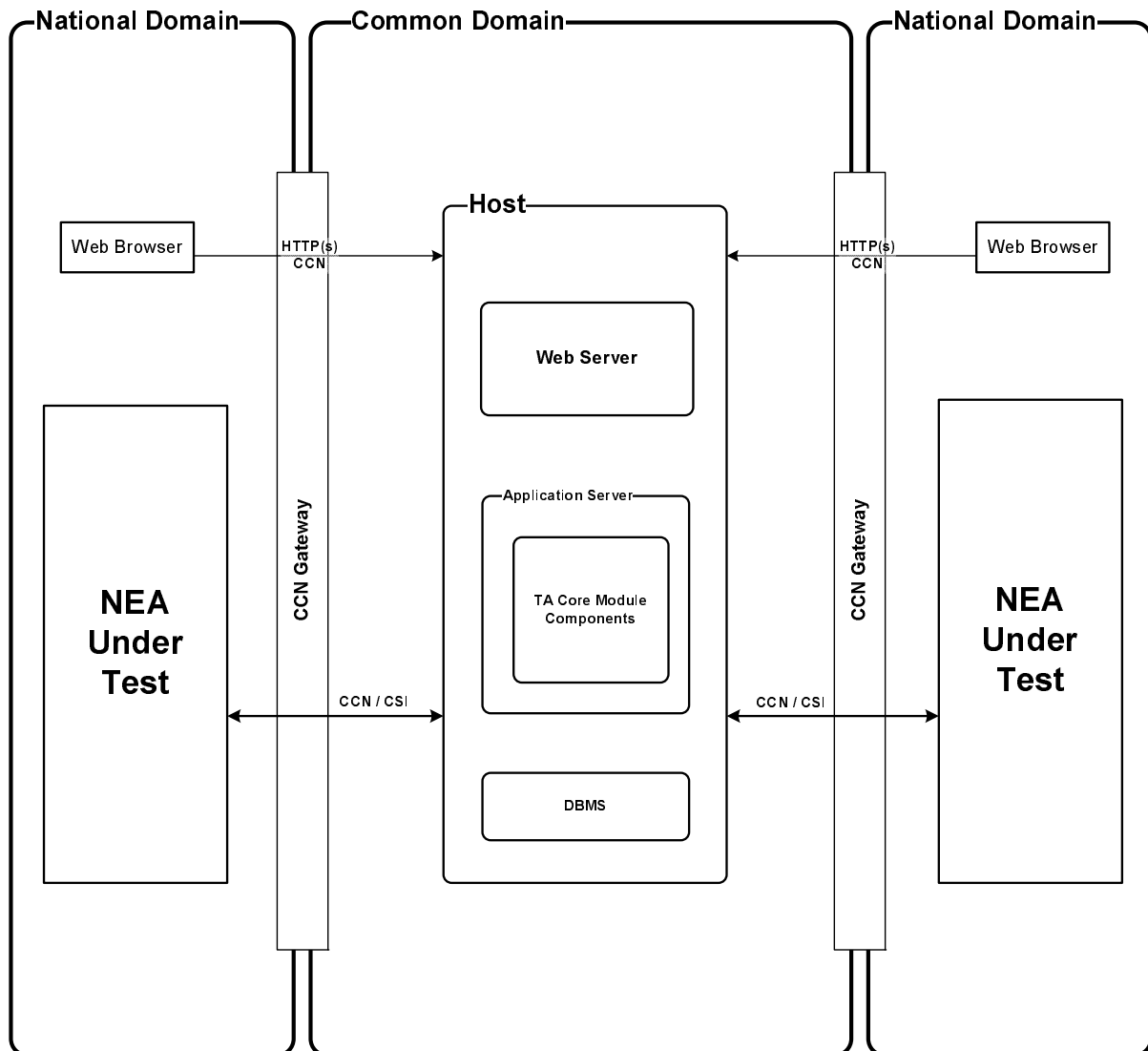
Figure 2-3: TA Deployment View

As presented in the figure above, the elements that compose TA are:

- Web Server;
- Application Server;
- DBMS.

The application will be accessed from the National Domain and is represented by the web browsers and the communication will be HTTP(s) / CCN.

The web server forwards the requests to the application servers that start the testing processes. The application will communicate with the NEA under test with CCN/CSI messages through a CCN Gateway.

In order to reduce the TA maintenance effort, there will be one single deployment of the Testing Application which will be accessible by all the Member States.

2.2 PROCEDURE OVERVIEW

The following table presents the steps involved in the installation of the TA, together with an indication of the privileges and skills that the individual (or organisation) performing the step must have.

Step	Purpose	Roles/Privileges	Skills
1	Create CCN/CSI Resources	CCN-TC Local CCN/CSI Administrator	CCN Gateway configuration and Administration
2	Create the TA Database	Database Administrator	Create the Database instance, Database User and Schema
3	Configure WebLogic Server Instance	WebLogic Administrator	Create the Domain, Server and Connection Pool
4	Configure TA Application	UNIX User	Basic UNIX user
5	Build the TA application	UNIX User	Basic UNIX user
6	Deploy the TA Application	WebLogic Administrator	Deploy J2EE applications

Table 2-2: Installation Procedure Overview

3 INFRASTRUCTURE REQUIREMENTS

3.1 NETWORK TOPOLOGY

The network topology required for building and deploying the TA is depicted in (Figure 3-1):

- One CCN/CSI Gateway providing connectivity to the Common Domain;
- One Server hosting the TA database;
- One Business Application Server hosting the TA application;
- One or more Workstations, each hosting client utilities (e.g. Web Browser, telnet client, FTP, Oracle-Client tools) to be used to connect to the various servers for their administration and configuration.
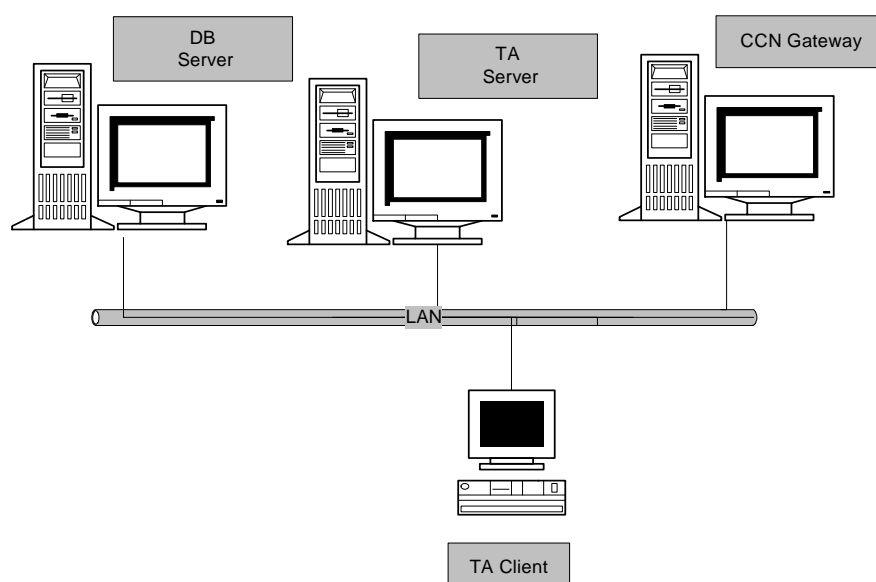
Figure 3-1: Network Topology

3.2 DATA COMMUNICATION REQUIREMENTS

In case a firewall is present between any of the aforementioned nodes, it should be configured to allow the data communications specified in the following table.

From Node	To Node	Protocol
TA Server	CCN Gateway	CSI
TA Client	TA Server	HTTPS/HTTP, telnet, FTP, SQL*NET
TA Server	DB Server	JDBC

Table 3-1: Data Communication Requirements

3.3 HARDWARE REQUIREMENTS

The minimum hardware requirements in order to perform the TA Installation:

Node	Hardware Configuration
TA Server	Sun Server 4 x UltraSPARC (750 MHz) 8 GB RAM 100 GB of available hard-disk space
DB Server	Sun Server 4 x UltraSPARC (750 MHz) 8 GB RAM 100 GB of available hard-disk space
TA Client	Standard PC Intel® Pentium® IV processor 1GB of RAM 10 GB of available hard-disk space
CCN Gateway	See the Common Communication Network - Technical Centre (CCN-TC)

Table 3-2: Hardware Configuration

3.4 SOFTWARE REQUIREMENTS

The following table specifies the necessary software configuration per node.

Node	Product	Version	Role
TA Server	Apache Ant	1.7.1	Build Tool
	Oracle BEA WebLogic Platform	10.3	J2EE Application Server
	CSI Stack for Solaris	5	Integration with CCN
	Sun Java Development Kit	1.6_05	Compilation of the Java source code
DB Server	Oracle Database 10g	10.2.0.4	Hosting of the TA data
TA Client	Web Browser, Telnet client, FTP Client, etc.	N/A	Connect to the Server nodes for administration and configuration purposes.
CCN Gateway	See CCN-TC	-	-

Table 3-3: Software Configuration

.

4 CREATE CCN/CSI RESOURCES

4.1 CONFIGURE THE CCN/CSI GATEWAY

The procedure for configuring the local CCN/CSI gateway for supporting TA consists of the following steps:

- CCN-TC is responsible for creating the local queues for the TA. Depending on the intended TA operation mode, these queues are:

Operation Mode	Queue Function	Queue Name
Development environment	Core flow	[Removed]
	Administration	[Removed]
	Reports	[Removed]
	External Domain	[Removed]
FAT environment	Core flow	[Removed]
	Administration	[Removed]
	Reports	[Removed]
	External Domain	[Removed]

Table 4-1: CCN/CSI Queue Names for TA

Notes:

- The queue names are provided as an example as this is subject to change depending on the deployment environment.
- In the table above [Removed] can take the value [Removed] to indicate 4 different queue sets for use by TA.
- The queue names are applicable for EMCS.
- CCN-TC is responsible for configuring the gateway so that it can accept connection requests from the TA Business Application Server. This includes specifying for each TA instance: the name of the proxy it will use in the gateway and the associated port number, the CSI application name and application key, the CSI user profiles to use, and the message types to use (in IDL format);

The CCN-TC has provided a set of forms in Microsoft Excel format for specifying all the information needed. A set of forms for configuring a gateway to support TA is provided as an appendix to this document. These forms must be sent to the CCN-TC after filling in the missing information and validating the information already included.

Upon receiving these forms, the CCN-TC connects to the gateway, uploads the necessary configuration information in the (CCN) X.500 directory, creates the queues, the user profiles, and the related information thus allowing TA to connect to this gateway. The CCN-TC furthermore provides to the requester the [Removed] file to be used on the Server.

5 CREATE THE TA DATABASE

5.1 CREATE THE DATABASE INSTANCE

Purpose:

- Create the Oracle database instance.

Prerequisites:

- The Oracle 10G is installed on the database server.
- The [Removed] tablespace was created with the properties described in the request form;
  If not already created, you can use the @createTablespace.sql script (available under [Removed]).

Procedure:

1. Using Oracle Database Configuration Assistant, create the database instance, taking into account the following:
   - EMCS application use UTF-8 character-set;
   - the tablespace used will be [Removed];
   - Oracle parameter *open_cursors* should be set to at least 800 – see Note in Section 8.3.

Outcome:

- The database instance has been created.

5.2 CREATE THE DATABASE USER

Purpose:

- Create the Oracle database user that is needed by the TA application.

Prerequisites:

- The database instance has been created.
- Verify that sqlplus is accessible for the user that will be used for executing the scripts.
- If the TA user is already created on this database instance, make sure you drop it before proceeding.

Procedure:

1. Unzip the TA application archive (TABuild-2.0.zip, for example) to a desired folder. The location of the "parent" folder (TA) will be referred as TA_HOME for the rest of the document.
2. Change the current working directory to [TA_HOME]/deployment/oracle
3. Execute the following command :

```
ant unix.fix
```
4. Connect to the database instance as SYSDBA or SYSTEM.
5. Execute the createUser.sql script.
6. Exit sqlplus utility.

Outcome:

- The [Removed] user has been created. The default password can be changed from the creation script.

5.3 CREATE THE SCHEMA

Purpose:

- Create the database schema used by the TA application.

Prerequisites:

- The [Removed] user has been created.

Procedure:

1. Change the current working directory to *[TA_HOME]/deployment/oracle*
2. Connect to the database instance as TA database user created in previous step ('[Removed]).
3. Execute the *createSchema.sql* script.
4. Execute the *populateSchema.sql* script.
5. Exit sqlplus utility.

Note: Alternate procedure:

When not using production queues, but [Removed] queues, please follow this steps:

1. Change the current working directory to *[TA_HOME]/deployment/oracle*
2. Open *populateSchema.sql*, find [Removed].sql script line and change the line as follow : [Removed].sql (for using [Removed] queues) or [Removed].sql (for using [Removed] queues)
3. Save [Removed].*sql*,and run the following command :

```
ant unix.fix
```

4. Connect to the database instance as TA database user created in previous step ('[Removed]).
5. Execute the *createSchema.sql* script.
6. Execute the *populateSchema.sql* script.
7. Exit sqlplus utility.

Note:

In order to optimize the server's memory usage, the Oracle settings can be updated, for example, by using "*alter system set sga_target=900m*".

Outcome:

- The [Removed] schema has been created and it also was populated with data.

6 CONFIGURE WEBLOGIC SERVER INSTANCE

6.1 CONFIGURE THE WEBLOGIC DOMAIN

Purpose:

- Create the BEA WebLogic Domain onto which the TA application will be deployed.

Prerequisites:

- The BEA WebLogic Platform has been installed on the server.

Procedure:

1. Using the BEA WebLogic Configuration Wizard, create the WebLogic domain that will host the TA Application. When asked, enter the HTTP port value, which will be used throughout this document. SSL will be configured in 6.6.
2. Start the newly created domain.

Note:

The Configuration Wizard is started by the [BEA-HOME]/wlserver_10.3/common/bin/config.sh shell script.

Outcome:

- The domain and the admin server have been created.

6.2 CONFIGURE THE NODE MANAGER PROPERTIES

Purpose:

- Configure the node manager.

Prerequisites:

- The domain has been created.

Procedure:

1. Change directory to "BEA_HOME/ wlserver_10.3/common/nodemanager"
2. Start the node manager running the following script
   BEA_HOME/wlserver_10.3/server/bin/startNodeManager.sh
3. At this point, the node manager is running. If the listen port has to be changed, please follow the steps from 4 to 6.
4. Open the *nodemanager.properties* file using a text editor.
5. Edit the setting:
   ListenPort = {the listen port for the node manager}.
6. Restart the node manager.

Outcome:

- The node manager was started.

6.3 CREATE THE MACHINE

Purpose:

- Create a machine.

Prerequisites:

- The domain has been created.
- The node manager was started.

Procedure:

1. Connect to the WebLogic console.
2. Go to Environment->Machines page.
3. Click on "New" button to create a new machine.
4. In the form text boxes provide the machine name and the machine Os.
5. Click on "OK" button.
6. Click on "Activate Changes" *.
7. Click on the machine just created.
8. Click on the "Node Manager" link under the "Configuration" Tab.
9. Click on "Lock & Edit".
   Edit the settings:
   Type: {SSL}
   Listen Address: localhost
10. Listen Port: {the listen port for the node manager configured earlier}
11. Click on "Save".
12. Click on the "Monitoring" tab. If everything is ok, the status of the node manager must be "Reachable".

Outcome:

- The machine was created.

Note:

* Clicking on "Activate Changes", "Lock & Edit" and "Release Configuration" might not be necessary if the parameter "Automatically Acquire Lock and Activate Changes" is enabled from the Console "Preferences". This note applies throughout this document.

6.4 CREATE THE MANAGED SERVER

Purpose:

- Create a new managed server.

Prerequisites:

- The domain has been created.

Procedure:

1. Connect to the WebLogic console.
2. Go to Environment->Servers page.
3. Click on "*New*" button to create a new server.
4. Provide the server name.
5. Click on "*Finish*" button.
6. Click on "*Activate Changes*".

Outcome:

- The managed server was created.

6.5 GENERATE THE SECURITY CERTIFICATES

Purpose:

- Generate the security certificate and keystore for the WebLogic server instance.

Prerequisites:

- The domain has been created.

Procedure:

1. With a web browser open the 'CCN gateway' login page (i.e: [Removed]/), and store the SSL certificate of this file into a '[Removed]' file. Note, that in some cases more than one certificate may be received, depending on your environment setup. In this case, use the certificate that has as its originator the gateway you are trying to access.
2. Change directory to the [TA_HOME] folder.
3. Open the [Removed].*sh* file using a text editor.
4. Replace the "[Removed]" with the full file path of the saved file from Step 1.
5. Replace the "[Removed]" with the name of the host were the application is deployed.
6. Verify that the [Removed].*sh* has execute rights for the user. These rights can be given using the following command:

```
chmod +x [Removed].sh
```

7. Run the script.
8. Enter "yes" as answer for the questions raised by the script.

Outcome:

- The certificate has been imported into the truststore and the required files have been generated.

Note:

Alternate procedure:

When not using CCN gateway, but the application's "fake" login page instead *, please follow these steps:

1. Change directory to the [TA_HOME]/pdf folder.
2. Verify that the [Removed].*sh* has executed rights for the user. These rights can be given using the following command :

```
chmod +x [Removed].sh
```

3. Run the [Removed].*sh* script.
4. When prompted for the following values, please input:

Question	Description	Sample value
What is your first and last name?	Full machine name, including DNS suffix, on which the application is deployed	[Removed]
What is the name of your organizational unit?	This value is only used for certificate description.	FITSDEV2
What is the name of your organization?	This value is only used for certificate description.	FITSDEV2
What is the name of your City or Locality?	This value is only used for certificate description.	[Removed]
What is the name of your	This value is only used for certificate	[Removed]

Question	Description	Sample value
State or Province?	description.	
What is the two-letter country code for this unit?	This value is only used for certificate description.	[Removed]

Table 6-1: Security certificate properties

5. Enter "yes" as answer to the remaining questions.

The certificate files will be generated in the same folder as the script ([Removed].jks, [Removed].jks, [Removed].cer).

Note:

* From the security point of view, TA can be configured to have either "CCN real login" or "fake login" mode. When setup as "fake login" TA will not use the CCN services for authentication, but a properties-defined list of possible users, as described under <TA_HOME>/pdf/TA-Security/src/main/resources/config/security-test-users.properties.

From the queue point of view, TA can be configured to use either "real CCN queue access through CSI portdaemon" or "file-based queue folders".

6.6 CONFIGURE THE MANAGED SERVER

Purpose:

- Configure the settings for the managed server instance.

Prerequisites:

- The domain has been created.
- The managed server has been created.
- The certificate has been imported into the truststore.

Procedure:

1. Connect to the WebLogic console.
2. Go to Environment->Servers page.
3. Click on the name of the server created in (section 6.1). Click the "Lock & Edit" button. Go to the "General" tab.
4. In the "*Machine*" combo box, select the machine just created.
5. In the "*Listen Address:*" input, enter the qualified name of the machine hosting the WebLogic Server including the full DNS suffix. (e.g "[Removed]").
6. Check the "*SSL Listen Port Enabled*" box. Also, verify that the HTTP and SSL ports are the same as the ones from the WebLogic settings provided when creating the domain.
7. Save the settings. Go to "Keystores" tab. Click the "Lock & Edit" button.
8. From the "*Keystores*" combobox, select "*Custom identity And Custom Trust*".
9. In the "*Custom Identity Keystore*" input, insert the path to "[Removed].jks" file (section 6.5, step 4).
10. In the "*Custom Identity Keystore Type*" input, insert "[Removed]".

11. In the "*Custom Identity Keystore Passphrase*" input, insert the password referred in the [Removed].*sh* script – the keypass parameter.

12. In the "*Confirm Custom Identity Keystore Passphrase*" input, insert the password referred in the [Removed].*sh (or generate*[Removed].*sh)* script – the keypass parameter.

13. In the "*Custom Trust Keystore*" input, insert the path to "[Removed].jks" file.

14. In the "Custom Trust Keystore Type" input, insert "JKS".

15. In the "*Custom Trust Keystore Passphrase*" input, insert "[Removed]".

16. In the "*Confirm Custom Trust Keystore Passphrase*" input, insert "[Removed]".

17. Click "Save". Go to "SSL" tab. Click the "Lock & Edit" button.

18. Edit the following settings with the corresponding values:
    - Private Key Alias : {the private key alias – the same as the one used to generate the certificates}
    - Private Key Passphrase: the password referred in the [Removed].*sh* script – the keypass parameter.
    - Confirm Private Key Passphrase: retype the password

These values are the same with the ones contained in the [Removed].*sh* or [Removed].*sh* scripts (the one used depends on the environment).

19. Save the settings, activate the changes. When the process is complete, restart the managed server.

Note: The input text will be entered without the quotes.
If using alternate generation method, for steps 8 and 12, the files will be located in the [TA_HOME]/pdf folder.

Note: In order to avoid potential "OutOfMemory" issues we recommend setting up the managed server memory option (for example, in the domain's [Removed].*sh* file) to at least:
MEM_ARGS="-Xms512m –Xmx512m"
MEM_PERM_SIZE="-XX:PermSize=256m"
MEM_MAX_PERM_SIZE="-XX:MaxPermSize=256m".
Also, we recommend increasing the values of the following parameters via the Admin Console:
    - From Service – JTA – Configuration – JTA, set the "*Timeout Seconds*" (for example, to 420);
    - From Environment – Servers - <TA Managed Server> - Configuration – Tuning, set the "Stuck Thread Max Time" (for example, to 1800).

Outcome:
- The server is configured with the new security settings.

6.7 CREATE THE DATASOURCE

Purpose:
- Create the datasource that will be used by the TA to communicate with the Oracle server.

Prerequisites:
- The Oracle WebLogic Platform has been installed on the server.
- The procedure from section 5 was completed successfully.

Procedure:
1. Connect to the WebLogic console.

2. Go to *Services -> JDBC -> Datasources*. Click the "*Lock & Edit*" button, then click "*New*" button.
3. Enter the desired datasource name (preferably, "jdbc. [Removed]").
4. Enter the JNDI name (preferably, "[Removed]").
5. From the "*Database Type*" combo, select *Oracle.*
6. From the "*Database Driver*" combo, select the one starting with **Oracle's Driver (Thin XA).*
7. Click *Nex*t twice.
8. In the *Connection Properties* form, use the values that were throughout the paragraph 5.
9. Click *Next.* Select the managed server as Target. Then click *Test Configuration.* The output should be "Connection test succeeded".
10. Click *Finish*, and then *Activate Changes.*
11. Click again *Lock & Edit* and then click on the newly created datasource.
12. In the *Targets* tab, select the managed server just created and click *Save.*
13. Click *Activate Changes* and then restart the application server.

Outcome:

- The datasource has been created.

Note: The Datasource connectivity can be tested in the Admin Console from Monitoring – Testing. A successful setup is demonstrated by a "*Test of jdbc.* [Removed]*on server* [Removed] *was successful*" message. If the message is "*Warning! Connectivity to backend database not verified. This is either because the required connection pool attribute "TestConnectionsOnReserve" has not been enabled, or an invalid value has been specified for attribute "TestTableName". Please check the server log for more details*" the *TestConnectionsOnReserve* must be enabled from Configuration – Connection Pool – Advanced form.

7 CONFIGURE TA APPLICATION

7.1 CONFIGURE THE TOOLS USED TO BUILD THE TA APPLICATION

Purpose:

- Install and configure JDK.

Prerequisites:

1. The installation kit (JDK) is available on the Application Server.

Procedure:

1. Install the JDK using the default settings.
2. Add an environment variable named JAVA_HOME that points to the location of the Java installation.

Outcome:

- The build tools are installed and configured

7.2 CONFIGURE THE TA APPLICATION

Purpose:

- Configure the TA Applications

Procedure:

1. Change directory to the [*TA_HOME*]/*pdf/TA-Common/src/main/resources/config* folder.
2. Open the [Removed].*properties* using a text editor. Edit its contents, using the following table for guidance:

Property	Description	Sample value
[Removed].host	Application Server node that will host CSI Portdaemon	[Removed]
[Removed].port	TCP/IP Port number that will be assigned to the CSI Portdaemon.	[Removed]
[Removed].application.name	CSI Application Name. This is described in the application ACF form, field "ccnApplicationName"	[Removed]
[Removed].application.key	CSI Application Key	[Removed]
[Removed].application.address	IP address of the CCN Gateway. This is part of the RAP address below.	[Removed]
[Removed].address	CSI RAP Address and Port. This can be found in the .cfg file received from CCN-TC, under section "Proxy <application_RAP_name>", field "Address"	[Removed]
[Removed].name	CSI RAP Name. This can be found in the application ACF form, field "[Removed]".	[Removed]

Property	Description	Sample value
[Removed].username	CSI User Name. This user should have access rights on the CCN queues and usually associated with all the profiles described in the application ACF form, field "[Removed]" (CCN queues access profiles).	[Removed]
[Removed]	CSI Password	[Removed]
[Removed].application.activationmode	The application will use polling for retrieving messages (instead of triggering by CCN). This can be found in the .cfg file received from CCN-TC.	Initiator
[Removed].authorized	CCN allowed authorization mechanisms. This can be found in the .cfg file received from CCN-TC.	[Removed]
[Removed].default	The default authorization mechanism. This can be found in the .cfg file received from CCN-TC.	[Removed]
[Removed].timeout	The inactivity interval in seconds that the supporting native executable (port daemon) remains available before automatically terminating	300
[Removed].waitinterval	The interval in milliseconds the port daemon will wait for a message to become available (or the time HL_mq_get will block waiting for a message to arrive)	5000
[Removed].lifetime	The time in tenths of a second a message must stay in a queue before it expires (zero means for ever)	3600

Table 7-1: AFC Runtime Properties

3. Open the *hibernate-test.properties* file using a text editor. Edit only the properties presented in the following table:

Property	Description	Sample value
hibernate.connection.defaultCatalog	Input the name of the user created at step 5.2	[Removed]
hibernate.connection.username	Input the name of the user created at step 5.2	[Removed]
hibernate.connection.password	Input the password of the user created at step 5.2	[Removed]
hibernate.connection.url	Input the the URL of the database connection.	[Removed]

Table 7-2: Datasource Properties

4. Open the *jndi.properties* file using a text editor. Edit the following properties:

Property	Description	Sample value
java.naming.provider.url	The URL of the JNDI provider for the Managed Application server. Replace "[Removed]" with the name of the machine that hosts the WebLogic Server and the "[Removed]" port value with the HTTP port specified when the WebLogic domain was created	[Removed]

Property	Description	Sample value
java.naming.factory.initial	The name of the Factory class for the InitialContext. For WebLogic, this value is : weblogic.jndi.WLInitialContextFactory	weblogic.jndi.WLInitialContextFactory
jndi.datasource.name	The JNDI name of the datasource created on the Managed Application Server (The same as in 6.7 step 4)	jndi. [Removed]

Table 7-3: JNDI Properties

5. Change directory to *[TA_HOME]/pdf/TA-Security/src/main/resources/config* folder.
6. Open the *security-preferences.properties* file using a text editor. Edit **only** the values presented in the following table:

Property	Description	Sample value
[Removed].degradedMode	A boolean parameter that permits to configure TA in a 'testing' security mode. When using "fake login", this must be set to "true", when using "real CCN login", this must be set to "false".	false
[Removed].authentication.services.protocol Schema	CCN authentication security service protocol schema	https
[Removed].authentication.services.host	Full host name of CCN authentication security service. When using "fake login" mode, this must the full name of the server hosting the TA (and the same as the Weblogic server's listen address defined above), e.g., "[Removed]"	[Removed]
[Removed].authentication.services.port	CCN authentication security service port number. When using "fake login", this must be the Managed Server's SSL port.	[Removed]
[Removed].authentication.services.loginUri	CCN authentication security service login URI. When using "fake login", the value must be [Removed]".	[Removed]
[Removed].authentication.services.logoutUri	CCN authentication security service logout URI. When using "fake login", the value must be " /EMCS-TA-WEB/ccnCsiServices/ccnServerLogout".	[Removed]
[Removed].usermanagement.services.proto colSchema	CCN user management security service protocol	http

Property	Description	Sample value
	schema	
[Removed].usermanagement.services.host	Full host name of CCN user management security service. When using "fake login" mode, this must the full name of the server hosting the TA (and the same as the Weblogic server's listen address defined above), e.g., "[Removed]"	[Removed]
[Removed].usermanagement.services.port	CCN user management security service port number. When using "fake login", this must be the Managed Server's normal HTTP port.	[Removed]
[Removed].usermanagement.services.useridentUri	CCN user identities (user name, user description and site name) security service URI. When using "fake login", the value must be " [Removed]".	[Removed]
[Removed].usermanagement.services.aclientUri	CCN user profiles (ACL – Access Control List) security service URI. When using "fake login", the value must be [Removed]".	[Removed]
[Removed].security.forceHttps	This parameter is used to force the communication between TA user and TA server to HTTPS protocol (secure connection). If set to true, HTTP request will be redirect to HTTPS URL otherwise TA will follow the user request protocol.	false
[Removed].http.port	HTTP port (the same value as in 6.1)	[Removed]
[Removed].https.port	HTTPS port (the same value as in 6.6)	[Removed]
[Removed].services.userProfileGroupSuffix	User profile group suffix as defined in CCN/CSI network	. [Removed]
[Removed].client.domain	This is the domain as seen by the NEA client. If the client will connect to TA with an URL like this: [Removed]/, then the domain will be : '.[Removed]	. [Removed]
[Removed].server.domain	This is the domain as seen by the TA application server. If TA application server will authenticate to CCN/CSI security server using an URL like this: [Removed]then the	. [Removed]

Property	Description	Sample value
	domain will be '.[Removed].	
[Removed].server.ssl.keyStore	The location of the keystore, generated in 6.5. By default, it is generated in the [TA_HOME]/pdf folder	[TA_HOME]/pdf/ [Removed].jks
[Removed].keyStorePassword	The keystore password (unless the [Removed].*sh* script is modified, the password will be "[Removed]")	[Removed]
[Removed].ssl.trustStore	The location of the truststore, as specified in 6.5 step 4. By default, it is generated in the [TA_HOME]/pdf folder	[TA_HOME]/pdf/ [Removed].jks

Table 7-4: TA Security Properties

7. Change directory to *[TA_HOME]/pdf/TA-Security/src/main/resources/spring* folder.

8. Open the [Removed].*xml* file using a text editor. Edit **only** the values presented in the following table:

Property	Description	Sample value
<property name="[Removed]"> <value>[Removed]</value> </property>	Input the name of the file that will be used by the Security module as ticket cache store in the hosting server's temporary folders. For each TA instance, this file name must be unique.	[Removed]

Outcome:

• The TA application has been configured.

8 BUILD THE TA APPLICATION

8.1 BUILD THE TA APPLICATION

Purpose:

- Build the TA application WAR.

Please note that in case of an existing TA deployment we recommend the Clean-up procedure described in Annex C.

Procedure:

1. Change directory to *[TA_HOME]/pdf* folder.
2. Open a command prompt here.
3. Verify that the user has executed rights for the script *apache-maven-2.2.1/bin/mvn*. If not, grant them.
4. Delete the contents of *[TA_HOME]/pdf/repository/*[Removed]
5. Execute the following command :

```
ant unix.fix
```

6. Execute the following command :

```
apache-maven-2.2.1/bin/mvn -o clean install
```

Outcome:

- In the [TA_HOME]/pdf/TA-Web/target folder, the [Removed].war will be found.

8.2 BUILD THE CSI PORTDAEMON

Purpose:

- Build the CSI Portdaemon on its target host machine.

Prerequisites:

The following software is available on the CSI Portdaemon target host:

1. The CSI Portdaemon source code (available in the TA application source, under the '[Removed]' subdirectory).
2. The Sun C compiler, Java JDK, Apache Ant tool have been installed and configured and their respective executables (i.e. cc, java and ant) are referenced in the PATH environment variable of the user performing the build.
3. The CCN/CSI stack has been installed.

Procedure:

1. Login to the TA Server.
2. Change the current working directory to the directory where the portdaemon source is located (referred to as [PORTDAEMON-BASE] for the remaining of this document).

```
$ cd [PORTDAEMON-BASE]
```

3. Copy the "constant.h" C header file and the .cfg file provided by CCN-TC for the TA Server under the directory [PORTDAEMON-BASE]/data/csiconfig. Please cross-check the configuration properties from the .cfg file with [Removed].properties (see Table 7 1: AFC Runtime Properties).

4. Edit the file [PORTDAEMON-BASE]/ build.properties to reflect your environment

```
$ vi build.properties
```

- Set the full path to where the portdaemon will be installed as a service (*PORTDAEMON_HOME* property)
- Set the full path to where the portdaemon source is located (*PORTDAEMON_BASE* property as already defined in step 2 above)
- Set the full path to the Sun C compiler (*CC* property).
- Set the portdaemon host name (*HOSTNAME* property)
- If the default port range ([Removed]) is not appropriate for current environment, edit the *PORT_RANGE* property accordingly.
- Set the C CSI home (*CSI_HOME* property).

5. Invoke Apache Ant command with the 'clean dist' arguments:

```
$ ant clean dist
```

Outcome:

- The CSI Portdaemon scripts and binaries are available under the [PORTDAEMON-HOME] directory.

8.3 UPLOAD PRELOADED DATA

Purpose:

- Upload preloaded data required by the TA into the database.

Procedure:

1. Change directory to *[TA_HOME]/pdf* folder.
2. Verify that the user has execute rights on the [Removed].*sh script.* These rights can be given using the following command :

```
chmod +x [Removed].sh
```

3. Execute the [Removed].*sh* script.

Note:

It is possible for the script to fail with the "*ORA-01000: maximum open cursors exceeded*". In this case, first check the Oracle parameter **open_cursors** as an Oracle SYSTEM user by running "*sho parameters open_cursors*". To increase its value, run "*ALTER SYSTEM SET OPEN_CURSORS=800 SCOPE=BOTH SID='*';*". Note that the number may be set higher or lower than 800 depending on local needs; SCOPE can be MEMORY|SPFILE|BOTH and the SID, when specified as '*', means for all instances. Then recreate the schema by running the *dropSchema.sql*, *createSchema.sql*, *populateSchema.sql* and finally, re-run [Removed].*sh*.

Outcome:

- Preloaded data has been uploaded into the database.

9 DEPLOY THE TA APPLICATION

Purpose:

- Install the TA application on the Managed Application Server.

Prerequisites:

All previous steps were completed with success.

Procedure:

1. Connect to the WebLogic console.
2. Click *Lock & Edit.*
3. Go to *Deployments* screen and click *Install.*
4. Point to the location of the [Removed].war, select it, and then click *Next.*
5. Finish the installation using default settings. Activate the changes.
6. Start the EMCS-TA-Web application. (To start it, check the checkbox near the application, select "Start Servicing all Requests" form the table menu above and then click "Yes" when asked to confirm the start of the application.)

Outcome:

- The deployment of the application is complete.

The application can be accessed in one of the following ways:

- if a CCN authentication is used, the URL will be:

   [Removed], if accessing through HTTP or https[Removed], if accessing through HTTPS

- if the CCN gateway will not be used (testing mode), the URL will be:

[Removed]

where [Removed] is the one used in paragraph 6.6, step 4, <[Removed]> and <[Removed]>are the HTTP and HTTPS ports specified when the BEA WebLogic domain was created.

For the second login mode, select a user from the list, double-click on it, click *Login* button and then click on the link below the user selection form. The main page of the application will appear

10 INSTALL THE CSI PORTDAEMON

Purpose:

- Install the CSI Portdaemon on Server node.
- Add the CSI Portdaemon to the [Removed]-managed services.

Prerequisites:

1. A range[1] of TCP ports must be available for allocation to the CSI Portdaemon.

Procedure:

1. Login to the Server node as '[Removed]user. All other steps will be executed as '[Removed]user.
2. Create a directory where the Portdaemon will be installed, if not already created. We will refer to this directory as the [PORTDAEMON-HOME] directory.
3. Change into the [PORTDAEMON-HOME] directory.
4. Grant to the 'noaccess' group write access to the 'log' and 'tmp' subdirectories:

```
chmod g+w log tmp
chown :noaccess log tmp
```

5. Change into the 'bin' subdirectory.
6. If the default port range ([Removed]) is not appropriate for current environment, edit the 'portdaemon' script and set the PORT_RANGE variable accordingly.
7. Change the group of the 'portdaemon' script and the '[Removed]' executable to 'noaccess':

```
chown :noaccess portdaemon [Removed]
```

8. Edit the file */etc/services* and define the port where the [Removed] will listen for CSI Portdaemon client requests, by adding a line like the following:

```
TA_PORTDAEMON   [Removed]/tcp  #  TA CSI Portdaemon
```

9. Edit the file */etc/*[Removed] and add a line like the following to add the CSI Portdaemon service:

```
TA_PORTDAEMON    stream  tcp  nowait  noaccess  [PORTDAEMON-HOME]/bin/
portdaemon taportd [PORTDAEMON-HOME]
```

10. Create an SMF manifest for the new service by issuing the command:

```
$ [Removed]
```

11. Verify the new service is up and running by issuing the 'netstat' command below:

```
$ netstat -a | grep TA_PORTDAEMON
*.TA_PORTDAEMON     *.*       0      0 [Removed] 0 LISTEN
```

12. Verify the new service is actually reachable by running the command below as the Unix user who owns the <TA_HOME>:

    telnet <portdaemon_server> <portdaemon_service_port>

    If the connection is not successful, you may try uninstalling the portdaemon as described in the Uninstalling Portdaemon annex then re- installing the portdaemon as service for the <[Removed]>-owning user following the alternate procedure below (steps performed for building the Portdaemon described in section 8.2 are still available if executed as the <[Removed]> owning user).

Alternate procedure

1. Login to the Server node as the <[Removed]>-owning user, for example "[Removed]", as used in the next steps. All other steps will be executed as '[Removed]' user.

---

[1] Not all ports in the range need to be free for use by the CSI Portdaemon; if a port is already used, the CSI Portdaemon will try with the next one.

2. Create a directory where the Portdaemon will be installed, if not already created. We will refer to this directory as the [PORTDAEMON-HOME] directory.

3. Change into the [PORTDAEMON-HOME] directory.

4. Grant to the owning group write access to the 'log' and 'tmp' subdirectories:

```
chmod g+w log tmp
```

5. Ensure the access rights on the 'log' and 'tmp' subdirectories are correctly defined following the previous step (for example as "drwxrwxr-x", the owning user being '[Removed]) by running "ls -l"; if necessary change the access using the chmod command;

6. Change into the 'bin' subdirectory.

7. If the default port range ([Removed]) is not appropriate for current environment, edit the 'portdaemon' script and set the PORT_RANGE variable accordingly.

8. Ensure that the '[Removed]' user has full control (rwx) of the "portdaemon" and "[Removed]" files by running "ls -l"; if necessary change the access using the chmod command; for example, a correct result:

```
-rwxr-xr-x   1 [Removed]other         739 Aug 31 17:36 portdaemon
-rwxr-xr-x   1 [Removed]other      138564 Aug 31 17:36 [Removed]
```

9. Edit the file */etc/services* and define the port where the inetd will listen for CSI Portdaemon client requests, by adding a line like the following:

```
TA_PORTDAEMON  [Removed]/tcp  #  TA CSI Portdaemon
```

10. Edit the file */etc/inetd.conf* and add a line like the following to add the CSI Portdaemon service:

```
TA_PORTDAEMON     stream   tcp  nowait   [Removed]   [PORTDAEMON-HOME]/bin/
portdaemon taportd [PORTDAEMON-HOME]
```

11. Create an SMF manifest for the new service by issuing the command:

```
$ [Removed]
```

12. Verify the new service is up and running by issuing the 'netstat' command below:

```
$ netstat -a | grep TA_PORTDAEMON
*.TA_PORTDAEMON     *.*        0      0 [Removed] 0 LISTEN
```

13. Verify the new service is actually reachable by running the command below as the Unix user who owns the <[Removed]>:

telnet <portdaemon_server> <portdaemon_service_port>

Outcome:

- The CSI Portdaemon has been installed as a managed [Removed] service.

11 ONE-CLICK UPLOAD

Purpose:

- Upload XSDs, CTP entities (IE Templates, Datasets, Scenarios and Instantiation data) and CTP Main Document into TA database.

Procedure:

1. Replace the old XSD files from the directory *[TA_HOME]/pdf/TA-Common/src/main/resources/xsd* with the new ones received in the package.
2. Replace the old template files from the directory *[TA_HOME]/pdf/TA-DataService/src/main/resources/template* with the new ones received in the package.
3. Replace the old scenario files from the directory *[TA_HOME]/pdf/TA-DataService/src/main/resources/scenario* with the new ones received in the package.
4. Replace the old file '*CTPInstantiationData.xml*' from the directory *[TA_HOME]/pdf/TA-DataService/src/main/resources/instantiation_data* with the new one received in the package.
5. Replace the old *[TA_HOME]/pdf/TA-Web/src/main/webapp/docs* directory with the new one received in the package.
6. Login in the web logic console.
7. Stop servicing all requests for TA application.
8. Change directory to *[TA_HOME]/pdf* folder.
9. Verify that the user has execute rights on the [Removed].*sh script.* These rights can be given using the following command:

```
chmod +x [Removed].sh
```

10. Execute the [Removed].*sh* script.
11. Start servicing all requests for TA application.

Outcome:

- XSDs and CTP data has been uploaded into the database.

  After each operation there is a confirmation message, on each functional stage FS1 and FS2 that reports the number of success and failed items. If the number of failed imported items is more than 0 that means the whole operation failed and the transaction will be rolled back. About what needs to be done to upload files again, depends on the error(s) reported in the log files. As an example, you can find below the confirmation messages for each entity and functional stage:

  - `XSD import completed for FS1: success = 29 ; fail = 0`
  - `Datasets import completed for FS1 - A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,Q - 113 template(s) analyzed successfully, 0 template(s) failed`
  - `Template import completed for FS1: success = 113 ; fail = 0`
  - `Instantiation data import completed for FS1: success = 28 ; fail = 0`
  - `Scenario import completed for FS1 stage: success = 126 ; fail = 0`
  - `XSD import completed for FS2: success = 44 ; fail = 0`
  - `Datasets import completed for FS2 - A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q - 184 template(s) analyzed successfully, 0 template(s) failed`
  - `Template import completed for FS2: success = 184 ; fail = 0`
  - `Instantiation data import completed for FS2: success = 28 ; fail = 0`
  - `Scenario import completed for FS2 stage: success = 233 ; fail = 0`

12 CTP DOCUMENTS UPDATE

Purpose:

- Upload CTP Documents into TA database and update CTP version as displayed by TA without re-deployment.
- Possible CTP documents to be changed follow the same structure as it can be found published on CIRCA and are the following:

Document description	Containing folder
CTP Datasets	\TA-Web\src\main\webapp\docs\CTP\FSx\[Removed]
CTP Scenarios	\TA-Web\src\main\webapp\docs\CTP\FSx\[Removed]
IE713	\TA-Web\src\main\webapp\docs\CTP\FSx\[Removed]
IE734	\TA-Web\src\main\webapp\docs\CTP\FSx\[Removed]
IE931	\TA-Web\src\main\webapp\docs\CTP\FSx\[Removed]
Scenarios XSDs	\TA-Web\src\main\webapp\docs\CTP\FSx\[Removed]D
Scenarios to be re-executed	\TA-Web\src\main\webapp\docs\CTP\FSx\CTP[Removed]
CTP Main package	\TA-Web\src\main\webapp\docs\[Removed]

where FSx can be FS1 or FS2 depending on the source CTP.

Procedure:

- For each document to be updated, go to its Containing folder as described in the table above;
- Delete the folder named as the previous version of the document together with its content;
- Create a new folder named as the new version of the document;
- Copy the document itself in the folder created in the previous step (in the same format as the previous version of the document);
- If the Documents update is associated with an effective CTP data update, follow the One-click Upload procedure as described in section 11; if only a document update is necessary, follow the following steps instead:
  - Change directory to *[TA_HOME]/pdf* folder.
  - Verify that the user has execute rights on the [Removed].*sh* script. These rights can be given using the following command:

```
chmod +x [Removed].sh
```

  - Execute the [Removed].*sh* script.

Outcome:

- CTP Documents have been uploaded into the database and can be accessed from TA's Home Page and EMCS Documents Screen, where the CTP version displayed is also updated, after re-login.

13 DDNEA MAIN DOCUMENT UPDATE

Purpose:

- Upload DDNEA Main Document into TA database and update DDNEA version as displayed by TA without re-deployment.

Procedure:

1. Go to the \TA-Web\src\main\webapp\docs\[Removed] folder, where the FSx can be FS1 or FS2 depending on the source of the document;
2. Delete the folder named as the old version of the document;
3. Create a new folder named as the new version of the document;
4. Copy the DDNEA Main Document (in PDF format) itself in the folder created at step 3;
5. Change directory to *[TA_HOME]/pdf* folder;
6. Verify that the user has executed rights on the [Removed].*sh* script. These rights can be given using the following command:

```
chmod +x [Removed].sh
```

7. Execute the [Removed].*sh* script.

Outcome:

- DDNEA Main Document has been uploaded into the database and can be accessed from TA's Home Page and EMCS Documents Screen, where the DDNEA version displayed is also updated, after re-login.

14 TA VERSION UPDATE

Purpose:

- Update TA version as displayed by TA without re-deployment.

Procedure:

1. From sqlplus run the following SQL:
   UPDATE APPLICATION_SETTINGS SET APS_VALUE = 'x.xx' WHERE APS_KEY = 'TA_VERSION';
   commit;

   Please note that x.xx should be replaced with the TA's new version value.

Outcome:

- Access TA's EMCS Documents Screen, where the TA version displayed is updated after re-login.

15 QUICK-UPLOAD THROUGH THE WEB INTERFACE

Purpose:

- Upload XSDs, CTP entities (IE Templates, Datasets, Scenarios and Instantiation data), CTP, DDNEA and TA Documents into TA database through the web interface.

Prerequisites:

1. The Quick Upload Archive was received.

   The Quick Upload archive must have the following directory structure:

   - ctp
     - FSX
       - instantiation_data
       - scenario
       - template
       - xsd
   - docs
     - FSX
       - CTP_CORE
         - version
       - CTP_DATASETS
         - version
       - CTP_IE713
         - version
       - CTP_IE734
         - version
       - CTP_IE931
         - version
       - CTP_SCENARIOS
         - version
       - CTP_SCENARIOSTOBEREEXECUTED
         - version
       - CTP_SCENARIOXSD
         - version
       - DDNEA_MAINDOC
         - version

   where FSx can be FS1 and/or FS2;

   The entities will be uploaded ONLY if they are present and located in the correct directory structure.

Procedure:

1. Connect to TA as an Administrator;
2. From 'Administration' menu, go to 'Set Up Test Environment' and choose 'CTP Upload' Tab;
3. In the text field 'File', select the Quick Upload archive;
4. After pressing the button 'Upload', a small window '[Removed] CTP Upload - Processing' will appear while the entities are uploaded into the database;
5. In the end, a report is generated and can be downloaded by pressing the button 'Download Report'.

Outcome:

- XSDs, CTP entities and Documents has been uploaded into the database.
  The report generated has the following name '[Removed].pdf'

  The report will contain details about all the entities uploaded like the example below:

  Report: [Removed].pdf

  Performed by:

  [Removed].EC

  CTP Upload Execution Date/Time:

  2011-05-23_12_36

  23-May-2011 15:32:07 - XSD import completed for FS1: success = 29 ; fail = 0

  23-May-2011 15:32:07 - Datasets import completed for FS1 - A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,Q - 113 template(s) analyzed successfully, 0 template(s) failed

  23-May-2011 15:32:41 - Template import completed for FS1: success = 113 ; fail = 0

  23-May-2011 15:33:30 - Instantiation data import completed for FS1: success = 28 ; fail = 0

  23-May-2011 15:34:02 - Scenario import completed for FS1: success = 126 ; fail = 0

  23-May-2011 15:34:03 - Document 'ECP2-FITSDEV2-SC03-CTP-v2.08.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:03 - Document 'CTP for Phase 2 v2.08 Datasets.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:03 - Document 'IE713-for-CT_v1.04.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:03 - Document 'IE734-v0.9.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:03 - Document 'IE931-for-CT_v1.04.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:04 - Document 'Scenarios to be re_executed by testing team.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:04 - Document 'CTPv2.08 Scenarios.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:04 - Document 'scenarioXSD.zip' for FS1 was succesfully uploaded

  23-May-2011 15:34:05 - Document 'ECP2-FITSDEV2-DDNEA-v3.02-EN.pdf' for FS1 was succesfully uploaded

  23-May-2011 15:34:06 - XSD import completed for FS2: success = 44 ; fail = 0

  23-May-2011 15:34:06 - Datasets import completed for FS2 - A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S - 184 template(s) analyzed successfully, 0 template(s) failed

  23-May-2011 15:34:37 - Template import completed for FS2: success = 184 ; fail = 0

  23-May-2011 15:36:06 - Instantiation data import completed for FS2: success = 28 ; fail = 0

  23-May-2011 15:36:31 - Scenario import completed for FS2: success = 233 ; fail = 0

  23-May-2011 15:36:33 - Document 'ECP3-FITSDEV2-SC03-DLV-6.8-3.8.2.0-CTP-SfI-v1.42.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:33 - Document 'CTPv1.42 Datasets.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:33 - Document 'P3-IE713-for-CT-v1.04.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:33 - Document 'P3-IE734-EXTRACT-ALL-v1.02.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:33 - Document 'P3-IE931-for-CT-v1.06.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:34 - Document 'Scenarios to be re_executed by testing team.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:34 - Document 'CTPv1.42 Scenarios.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:34 - Document 'scenarioXSD.zip' for FS2 was succesfully uploaded

  23-May-2011 15:36:41 - Document 'ECP3-FITSDEV2-SC03-DDNEA_P3-v1.51-EN.pdf' for FS2 was succesfully uploaded

  23-May-2011 15:36:42 - Document 'ECP3-FITSDEV2-TA-UMN-v1.00-EN.pdf' for FS2 was succesfully uploaded

ANNEXES

A. DELIVERY ARCHIVE CONTENT

The following table provides an overview of the TA Delivery Archive content.

Directory	Content
deployment/oracle/	DDL and DML scripts used for creation and initial population of the TA database schema.
documentation/	Project relevant documentation, such as IPM, OPM, UMN, STC, TSS and TST.
pdf/	TA source codes, required libraries, build scripts, configuration files, etc. required for building TA from source code.

Table 0-1: TA Delivery Archive Content

B. CCN CONFIGURATION REQUEST FORMS

The ZIP archive ECP2-EMCSDEV-SC02-TA-IPM_APP_A_0.10-EN.zip (Appendix A of this document) contains sample CCN Configuration Request Forms (in MS Excel format) along with the IDL definitions of the messages pertinent to the TA application, as listed in Table 0-2.

File	Description
CD701A_MSG_EMCS.CCNIDL	CD701A-MSG.EMCS IDL Definition
CD702A_MSG_EMCS.CCNIDL	CD702A-MSG.EMCS IDL Definition
CD801A_MSG_EMCS.CCNIDL	CD801A-MSG.EMCS IDL Definition
CD802A_MSG_EMCS.CCNIDL	CD802A-MSG.EMCS IDL Definition
CD803A_MSG_EMCS.CCNIDL	CD803A-MSG.EMCS IDL Definition
CD810A_MSG_EMCS.CCNIDL	CD810A-MSG.EMCS IDL Definition
CD813A_MSG_EMCS.CCNIDL	CD813A-MSG.EMCS IDL Definition

File	Description
CD815A_MSG_EMCS.CCNIDL	CD815A-MSG.EMCS IDL Definition
CD818A_MSG_EMCS.CCNIDL	CD818A-MSG.EMCS IDL Definition
CD821A_MSG_EMCS.CCNIDL	CD821A-MSG.EMCS IDL Definition
CD837A_MSG_EMCS.CCNIDL	CD837A-MSG.EMCS IDL Definition
CD904A_MSG_EMCS.CCNIDL	CD904A-MSG.EMCS IDL Definition
CD905A_MSG_EMCS.CCNIDL	CD905A-MSG.EMCS IDL Definition
CD906A_MSG_EMCS.CCNIDL	CD906A-MSG.EMCS IDL Definition
CD917A_MSG_EMCS.CCNIDL	CD917A-MSG.EMCS IDL Definition
CD934A_MSG_EMCS.CCNIDL	CD934A-MSG.EMCS IDL Definition
EMCS_LST_ACFv4.xls	CCN Configuration Request for FAT
EMCS_LCT_ACFv4.xls	CCN Configuration Request for Development Mode

Table 0-2: Sample CCN Configuration Request Forms

C. CLEAN-UP PROCEDURE OF AN EXISTING TA DEPLOYMENT

In order to clean-up an existing TA deployment, follow the steps described below:

1. login in the web logic console from CONFORMANCE;

2. stop servicing all requests for TA application;

3. lock and edit;

4. select deployment TA;

5. delete deployment;

6. release configuration;

7. shutdown admin and managed servers;

8. empty *tmp* contents (but don't delete the folfer itself) from *user_projects/domains/ domain_name/servers/TAAdmin/* and *TAManagedServer/* (this paths defines the usual temporary weblogic folders; please check for any local deviations established for your environment);

9. empty folder *user_projects/domains/domain_name/config/deployments* (but don't delete the folder itself - this path defines the usual weblogic deployments folder; please check for any local deviations established for your environment);

NOTES:

- domain_name may have a specific name on the CONF environment.
- before building, please make sure you do not have backup files for configuration files in pdf folder
- every time, before building the application, please run:

```
ant unix.fix
```

as it is described in Chapter 8.1 - Build the TA Application.

D. UNINSTALL PORTDAEMON

In order to uninstall the TA portdaemon follow the steps described below:

First assure that the PORTDAEMON Service has been cleaned up in case of reinstalling the same service:

(You must use user [Removed])

1) # [Removed]

      to see the servises that are running (e.g. for TA_PORTDAEMON it will show:svc:/network/TA_PORTDAEMON/tcp:default)

2) # inetadm -d svc:/network/TA_PORTDAEMON/tcp:default

      to disable the service

3) # svccfg delete svc:/network/TA_PORTDAEMON/tcp:default

      to delete the service

4) # svcs |grep TA or [Removed]   again

      to see if it has been removed

5a) # cd /var/svc/manifest/network

5b) # ls

      to see the specific service in the list of services

6) # rm -f TA_PORTDAEMON-tcp.xml

      to remove it

7) Edit /etc/inet/services and remove related line

      e.g. TA_PORTDAEMON [Removed]/tcp # TA CSI Portdaemon

8) Edit /etc/inetd.conf and remove related line

      e.g.   TA_PORTDAEMON   stream   tcp   nowait   noaccess /export/home/ta/portdaemon/bin/portdaemon portd /export/home/ta/portdaemon