EUROPEAN COMMISSION

DIRECTORATE-GENERAL INFORMATICS

eDelivery Pilot for BRIS

Quick Start Guide

Author(s) : CEF
Reviewed by :

Approved by :

Version : 1.00

Date: 4/11/2015

CONTENTS

1. INTRODUCTION

CEF e-Delivery provides a set of components to exchange messages over the internet using B2B protocols. See the document concerning the "Introduction to the Connecting Europe Facility eDelivery building block" also included in this package for more information.

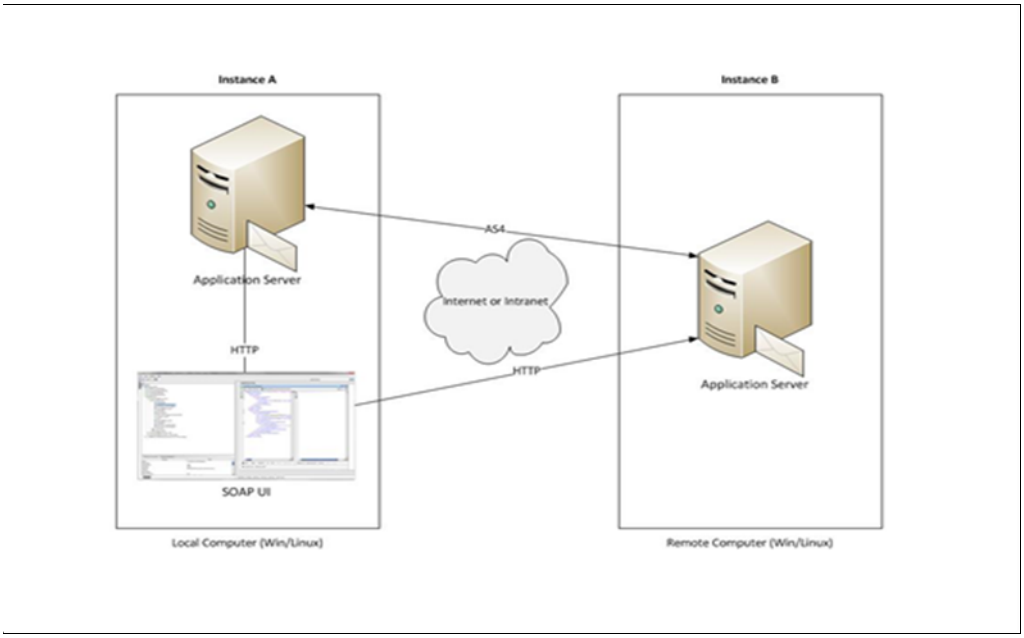
In this particular 'static' deployment context of Business Registers Interconnection System (BRIS), the full set of components (like dynamic discovery, connector) is not required. Business Registers cannot communicate directly with one another. Business Registers must always communicate through the European Central Platform. The required B2B protocol is AS4 (not need of AS2).

Therefore, this specific release (cipa-edelivery-distribution-3.1.0-as4-jboss) provides only an AS4 gateway (CEF e-Delivery component called domibus) running on a JBoss application server and using MySQL database to persist the data.

2. PURPOSE OF THIS GUIDE

In this document, you will find instructions to cover the testing scenario as illustrated in the figure below. In other words, we will guide you to setup 2 standalone instances connected on the same network to exchange B2B documents securely over AS4 by:

- Deploying and configuring both JBOSS instances (A and B)
- Configuring AS4 processing modes files for both gateways
- Using provided AS4 gateways certificates
- Running test cases



Remarks:

- The same procedure can be extended to a third (or more) instance(s).
- This guide doesn't cover the preliminary network configuration allowing communication between separate networks (i.e. infrastructure firewall/Proxy).

3. PREREQUISITES

- Java runtime environment (JRE), version 7 or higher:
  http://www.oracle.com/technetwork/java/javase/downloads/index.html

- JCE Unlimited Strength Policy files, for JRE7:
  http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html
  Copy the jar files from the extracted zip to <JRE_HOME>\lib\security.

- MySQL database server listening on the default port 3306:
  http://dev.mysql.com/downloads/windows/installer/5.6.html

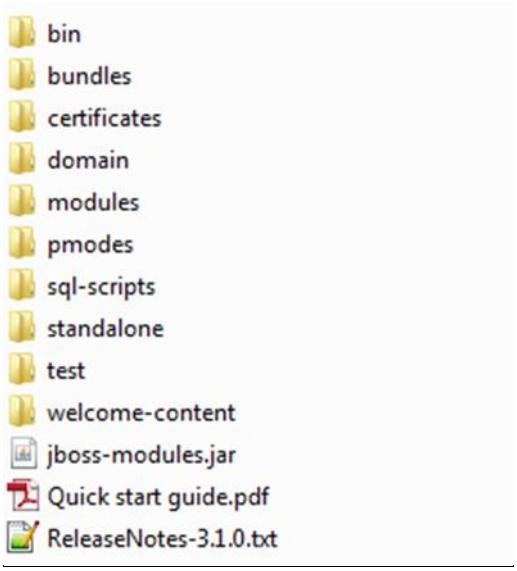
Please install the above software on your host machine. For further information and installation details, we kindly advise you to refer to the manufacturers' websites.

4. CONFIGURE YOUR ENVIRONMENT

4.1. Package Overview

Download the CIPA eDelivery Distribution from the shared drive : https://joinup.ec.europa.eu/nexus/service/local/repositories/snapshots/content/eu/europa/ec/cipa/cipa-edelivery-distribution/3.1.0/cipa-edelivery-distribution-3.1.0-as4-jboss.zip

This package contains the following structure:



- <CEF-eDelivery path>/bin folder contains the executable batch file (windows) and shell script (linux) required to launch the JBoss instance.

- <CEF-eDelivery path>/certificates contains a keystore (including private keys of instance A and instance B) and a trustore (including public keys of Instance A and instance B) that can be used by both instances. For this test release, each instance uses self-signed certificates.

- <CEF-eDelivery path>/modules/eu/europa/ec/cipa/configuration/main/domibus/ contains dombus's configuration files.

- <CEF-eDelivery path>/pmodes contains an AS4 processing mode (pMode-configuration.xml) configured to use compression, payload encryption, message signing and non-repudiation. The provided PMode file must be edited for both instances (cf. chapter 6).

- The <CEF-eDelivery path>/sql-scripts folder contains the required application sql code that needs to be executed on MySQL database.

- The <CEF-eDelivery path>/test folder contains a SOAP UI test project (refer to testing section)

4.2. JBoss Standalone Instance

As described in the purpose of this guide, we need to configure two instances running on two separate machines. Therefore, the procedure below would need to be applied on 'Hostname A' (local machine) and 'Hostname B' (remote machine). Please note that some there are additional steps for 'Hostname B'.

1. Extract the zip file containing the installation package of the CIPA eDelivery to a location on your physical machine, which we will refer to in this document as your "< eDelivery installation path >".

2. Open a command prompt and navigate to this directory:

   < eDelivery installation path >\sql-scripts.

3. Execute the following commands in the command prompt (without ""):

```
"mysql -h localhost -u root --password=root -e "drop schema if exists edelivery;create schema edelivery; create user edelivery identified by 'edelivery';grant all on edelivery.* to edelivery;"
```

```
mysql -h localhost -u root --password=root edelivery < create-mysql.sql
```

Note: if you are using Windows, make sure to have mysql.exe added to your PATH variable.

4. Update default properties of my.ini (Windows) or my.cnf (Linux)

   a. max_allowed_packet property

```
# The maximum size of one packet or any generated or intermediate string, or any parameter sent by the

# mysql_stmt_send_long_data() C API function.

max_allowed_packet = 512M
```

   b. innodb_log_file_size property

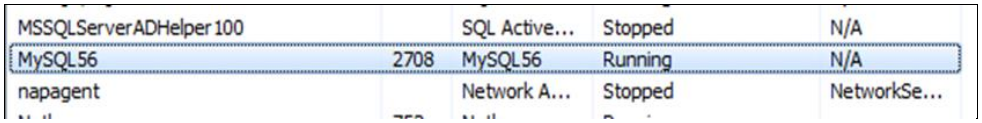
```
# # Size of each log file in a log group. You should set the combined size

# of log files to about 25%-100% of your buffer pool size to avoid

# unneeded buffer pool flush activity on log file overwrite. However,
```

```
# note that a larger logfile size will increase the time needed for the
# recovery process.
innodb_log_file_size = 5120M
```

5. Restart MySQL service:



6. **Only on Hostname B**

Edit the keystore alias to "instanceB" (instead of "instanceA") as indicated below (in domibus-configuration.xml):

```
<!-- The default keystore alias to use, if none is specified. -->
<prop key="org.apache.ws.security.crypto.merlin.keystore.alias">instanceB</prop>
```

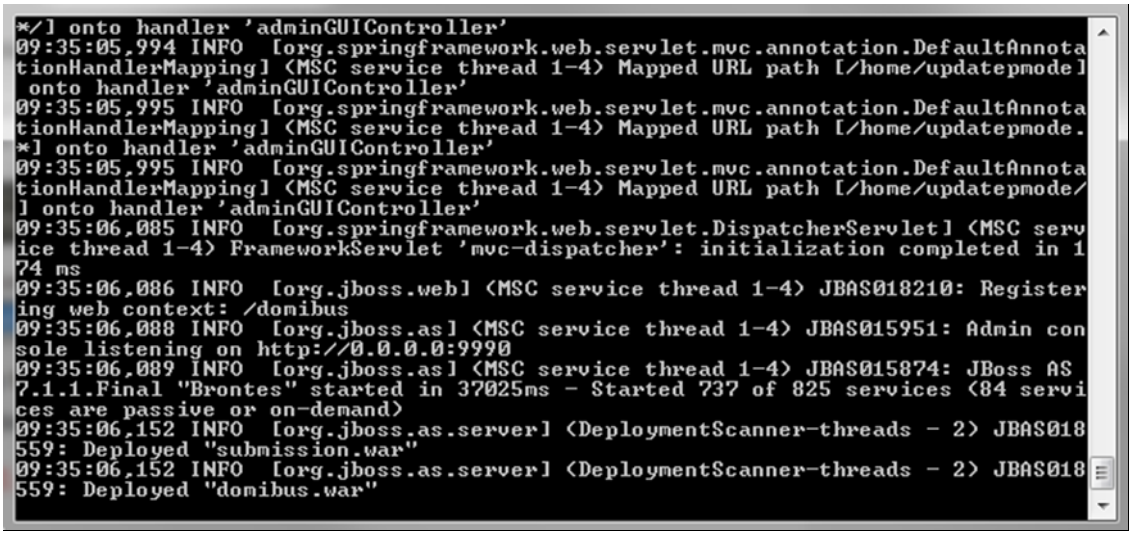
7. You can now start the JBoss standalone instance on your computer.

Execute:

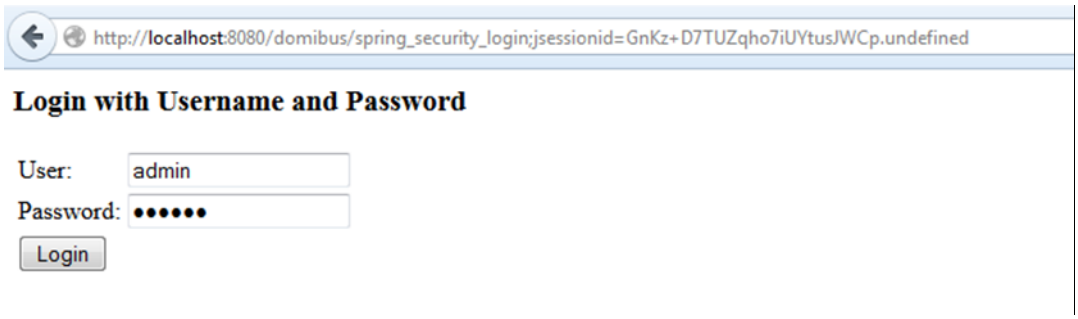
a. bin/standalone.sh (for Linux)

b. bin/standalone.bat (for windows)

Expected result:



Once the application server is started, you can ensure that this server is operational by displaying the administration dashboard (http://localhost:8080/domibus/home) in your browser as below:



Remarks:

- To allow the application server to use the TCP port 8080, it might be necessary to create a dedicated rule (to open this port) on your local firewall (cf. annex)
- In the default configuration, the JVM allocation memory is set to 1024. This parameter has to be reduced if the system cannot reserve enough space during the initializing of the application server (edit the parameter Xmx in the file "bin/standalone.conf.bat"):

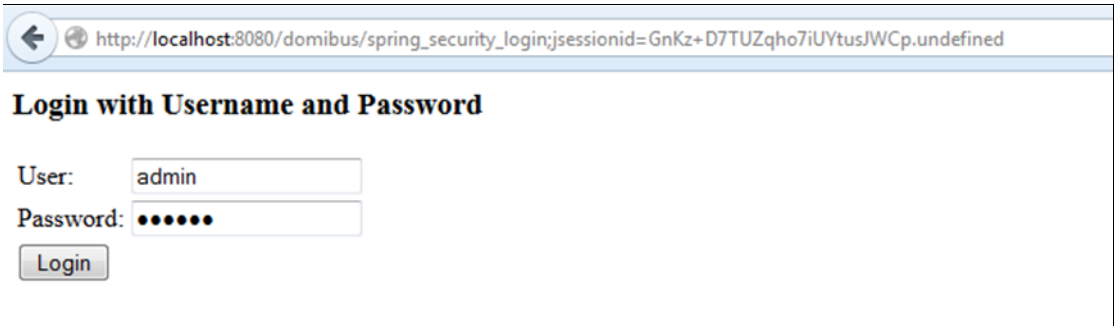
```
rem # JVM memory allocation pool parameters - modify as appropriate.
set "JAVA_OPTS=-Xms128M -Xmx1024M -XX:MaxPermSize=256M"
```

8. Open < eDelivery installation path >\pmodes\pMode-configuration.xml with a text editor and replace 'UndefinedHostnameA' and 'UndefinedHostnameB' with their real hostnames in the lines below (cf. annex):

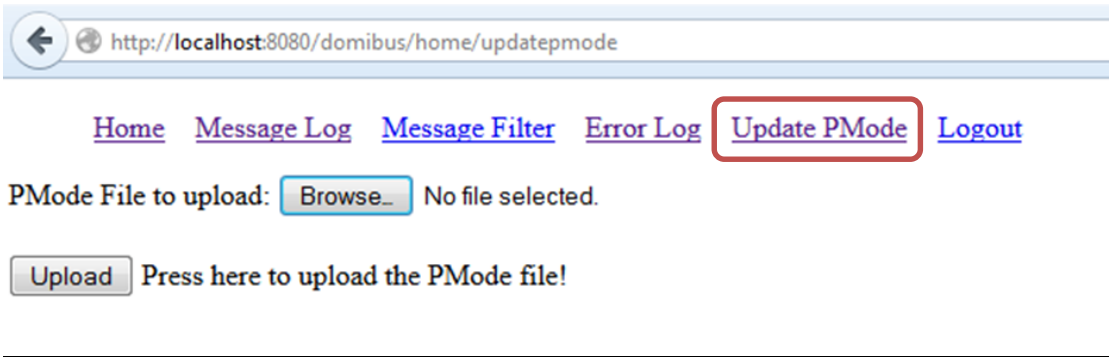
```
<party name="instanceA"
endpoint="http://UndefinedHostnameA:8080/domibus/services/msh">
      <identifier                              partyId="instanceAId1"
partyIdType="exampleType"/>
      <identifier                              partyId="instanceAId2"
partyIdType="exampleType"/>
</party>
<party name="instanceB"
endpoint="http://UndefinedHostnameB:8080/domibus/services/msh">
      <identifier                              partyId="instanceBId1"
partyIdType="exampleType"/>
      <identifier                              partyId="instanceBId2"
partyIdType="exampleType"/>
</party>
```

9. Upload the PMode on both instance A and instance B:

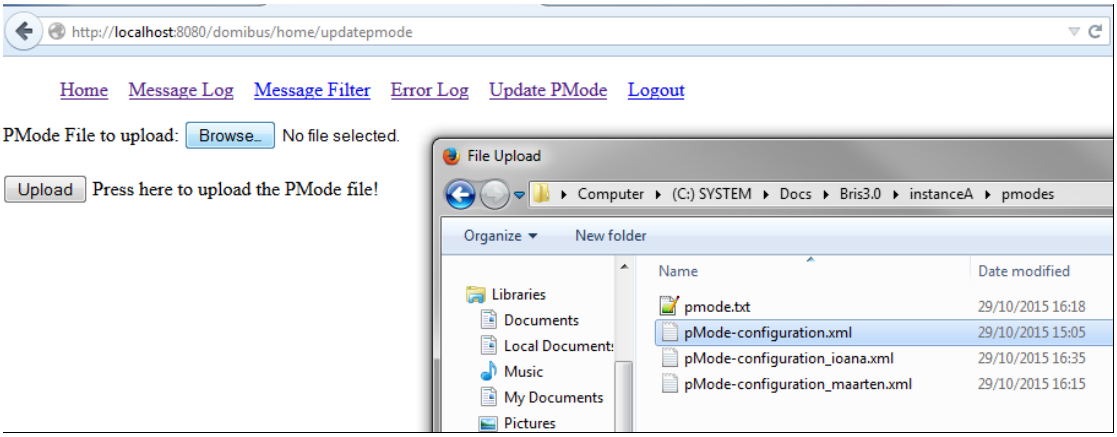
a. To upload a PMode xml file, connect to the administration dashboard using your credentials (by default: login = admin; password = 123456) to http://localhost:8080/domibus/home



b. Click on 'Upload PMode' tab



c. Select your PMode from "< eDelivery installation path >\pmodes" and hit "Upload"



5. TESTING

To send messages, you can follow the instructions of the "Test guide.pdf", in the test folder.

Remark:

> *If you encounter connection timeouts on the test you should increase the Socket Timeout setting of SoapUI. This can be done in the following File -> Preferences.*

ANNEXES

ANNEX 1 PARAMETERS

Parameters	Default value (Instance A)	Value on Instance B
Host Name	Host Name A	Host Name B
Database	MySQL database	MySQL database
Administrator Page	Username: admin Password: 123456 http://HostnameA:8080/domibus/home	Username: admin Password: 123456 http://HostnameB:8080/domibus/home
Database Schema	edelivery	edelivery
Database connector	jdbc:mysql:// "UndefinedHostnameA":3306/edeliver	jdbc:mysql:// "UndefinedHostnameB":3306/edelivery
DB username/passw	edelivery/edelivery	edelivery/edelivery
PModes XML files	pmodes/pMode-configuration.xml	pmodes/pMode-configuration.xml
Keystore location	certificates/keystore.jks	certificates/keystore.jks
Keystore Alias Name	"instanceA"	"instanceB" "to be edited in "domibus-configuration.xml"

ANNEX 2 FIREWALL SETTINGS

Depending on your configuration, the firewall settings might prevent you from exchanging messages from your local JBoss instance and the other one remotely deployed.

To test if a port is blocked or opened, you can use the tool "telnet" and run the command "telnet <server_ip> <port>". If the port is blocked then you need to open it.

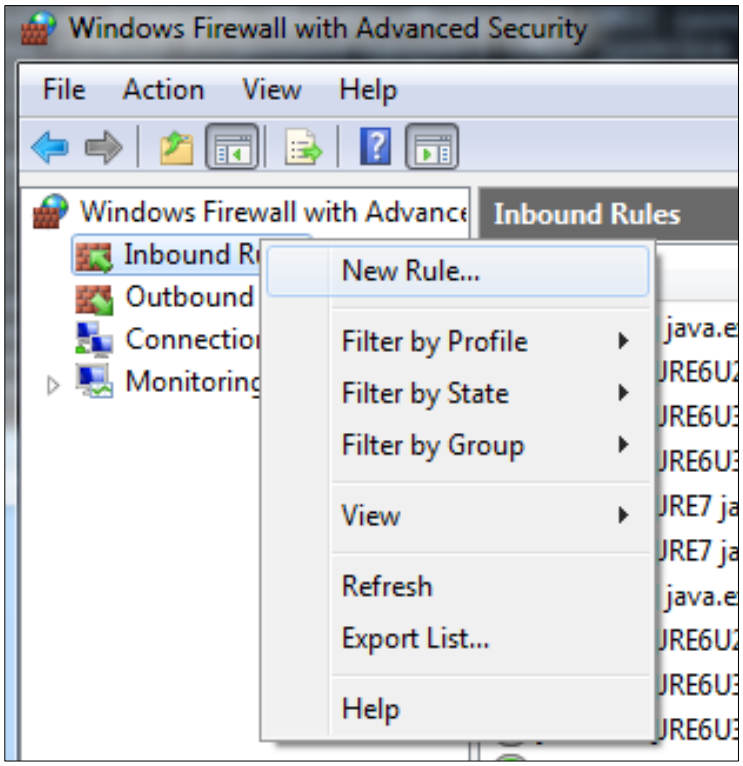
The following ports must be opened on both machines A and B (TCP protocol):

- 8080 (HTTP port)
- 5445 (JMS messaging)
- 5455 (JMS messaging)
- 3306 (MySQL port)
- 9990 (JBoss admin console)

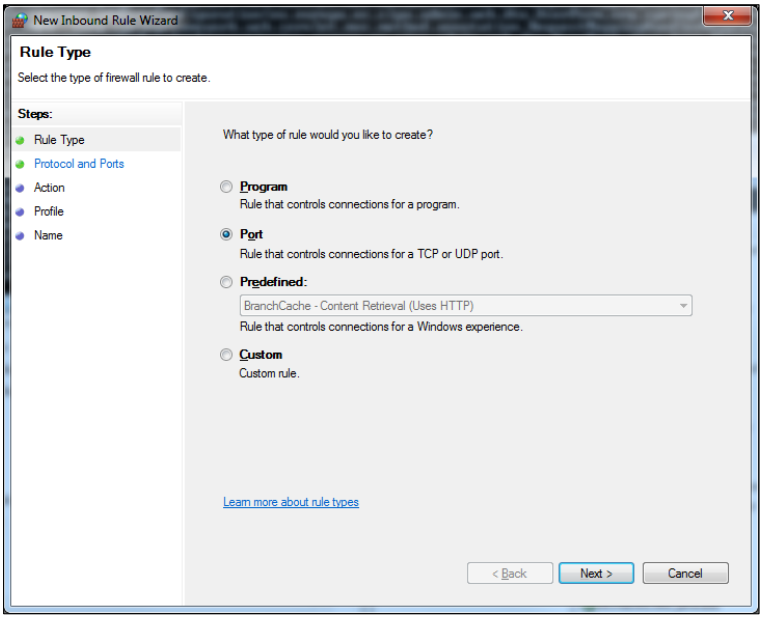
If your computer is protected by the Windows firewall, this is how you can open a port:

1. Open the "Windows Firewall with Advanced Security window": click on Start > Control Panel > System and Security > Windows Firewall and then click on "Advanced Settings".

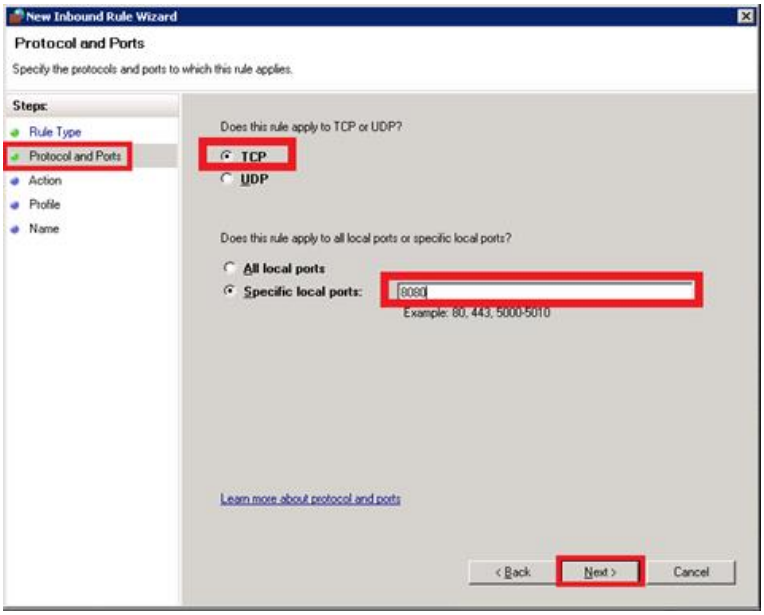
2. Right click on "Inbound Rules > New Rule:



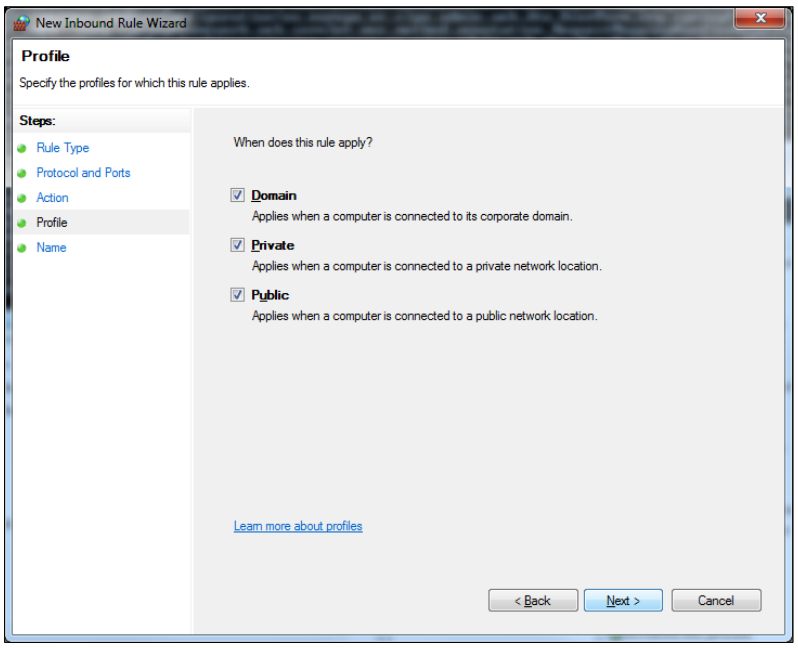
3. Select "Port" and click on "Next":



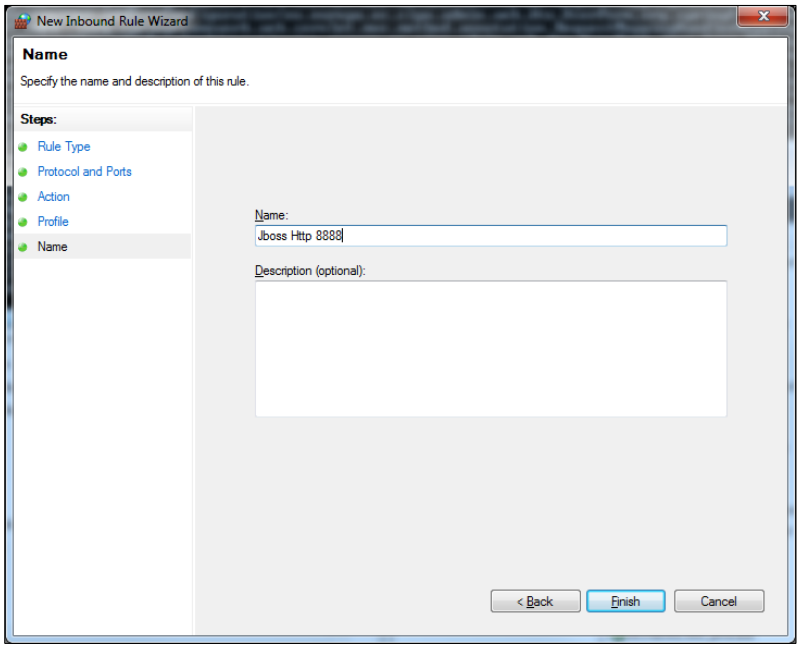
4. Enter a specific local port (for example 8080) and click on "Next":



5. Click on "Next":



6. Name the rule and click on "Finish":



ANNEX 3 DEFAULT PORTS CONFIGURATION

The default package includes an embedded JBoss application server with default ports (as illustrated in the table below).

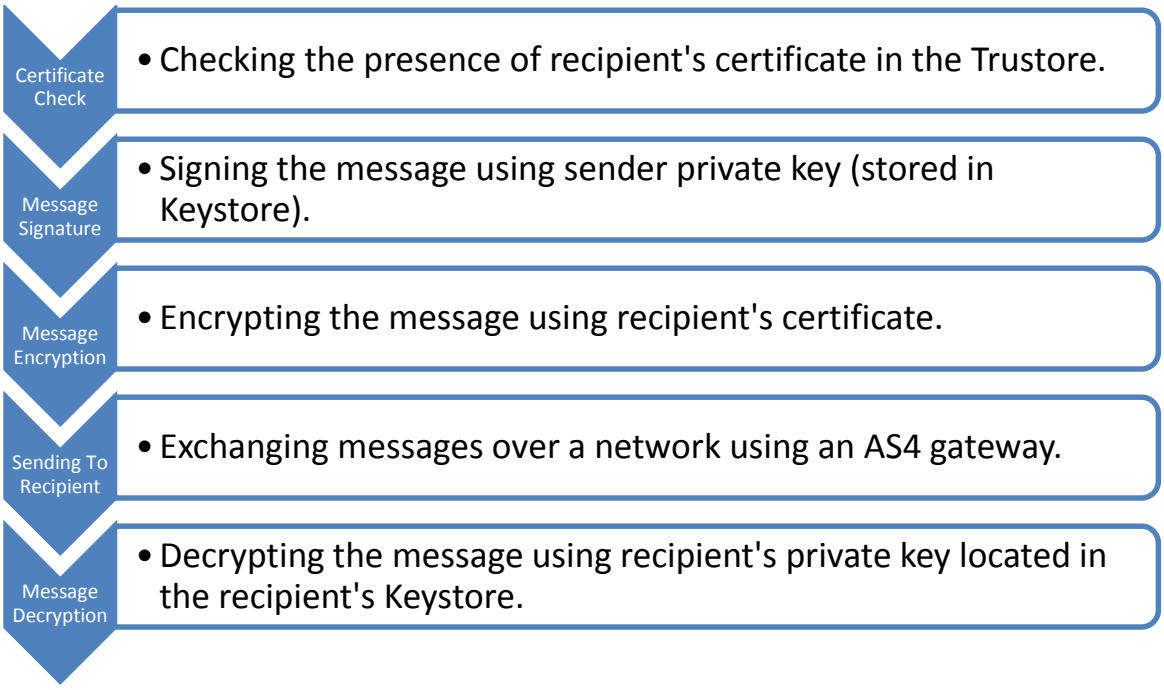
Default parameter	Value
Server listening HTTP port	8080
MySQL Port	3306
JBoss remote port	4447
JBoss admin Console	9990
MySQL Schema	edelivery

These instances can also be deployed on the same machine for internal testing.

In this case, the user will need to change receiver ports to avoid conflicts when starting the servers.

ANNEX 4 THE CERTIFICATES

To secure the exchanges between instances A and B (Instance A is sending a message to Instance B in this example), it is necessary to set up each instance's keystore and trustore accordingly. The diagram below provides a short explanation on the main steps of this process:



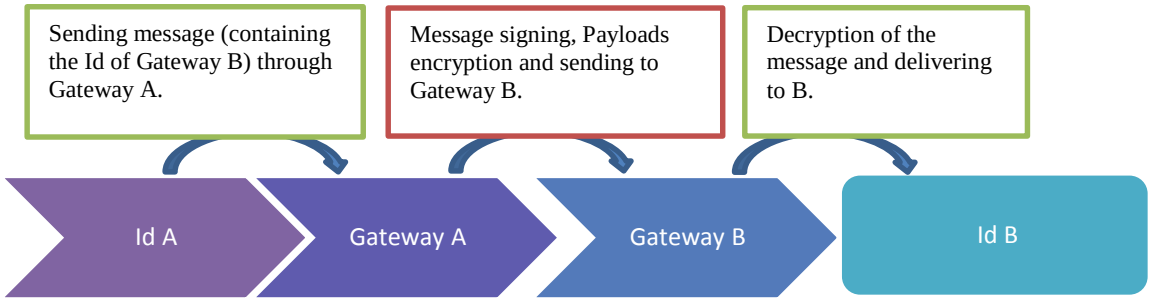
In order to allow B2B messages and documents between instances A and B, it is necessary to check the following:

For Instance A	For Instance B
Check that Instance B certificate (public key of B) is in trustore.jks of A, if not add it.	Check that Instance A certificate (public key of A) is in trustore.jks of B, if not add it.
Check that the name of B private key is in the keystore.jks, if not add it.	Check that the name of A private key is in the keystore.jks, if not add it.
In "domibus-configuration.xml": the keystore alias should be "instanceA", you might edit the keystore password (by default "test"), and the path to keystore.jks (if you change it).	In "domibus-configuration.xml" edit: the alias property to "instanceB", the keystore password (by default "test") if you need to, and the path to keystore.jks (if you change it).

Remark:

using tools sush as "keytool".

Assuming a scenario where a Business Register A (Id A) connected to a Gateway A sends a message to a Business Register B (Id B) connected to a Gateway B, the figure below describes the sending process (sending a message from an instance A to an instance B in P2P mode):



Remark: If Id A or B are behind a local firewall, it is necessary to open the required ports on it. As an example, port 8080 is not opened by default on Windows; we would need to create a dedicated rule on Windows firewall to open TCP 8080 port. See annex "Firewall Settings".

In a production environment, each participant would need a certificate delivered by a certification authority and remote exchanges between business partners would be managed by each partner's PMode (that should be uploaded on each instance).

For testing purposes, this package provides a pre-configured PMode xml file, a trustore.jks file and a keystore.jks file to be added to instances A and B as described in the "JBoss Application Server Configuration" section.

ANNEX 5 PMODE CONFIGURATION

Processing modes (PModes) describe how messages are exchanged between AS4 partners (Instance A and Instance B). These files contain the identifiers of each AS4 gateway (identified as parties in provided PMode file).

InstanceAId1, instanceAId2, instanceBId1, instanceBId2 represent the clients' backend connected to their associated AS4 gateway respectively. Therefore, adding, modifying or deleting a participant imply modifying those PMode files.

In a production environment, you will have an XML file for each instance generated by a plugin (External plugin for Eclipse). This XML file is updated every time a new partner is added or modified. For testing purposes, you will simply need to edit the PMode file dedicated to Instance B.

Here is an example of the content of a PMode XML file (in red, fields which should be adapted according to the user's configuration).

```
<?xml version="1.0" encoding="UTF-8"?>
<db:configuration xmlns:db="http://domibus.eu/configuration"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://domibus.eu/configuration
file:/C:/development/git-repos/domibus/Domibus-MSH/domibus-
configuration.xsd" party="instanceA">
      <mpcs>
            <mpc name="defaultMpc"
                        qualifiedName="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC"
                        enabled="true"
                        default="true"
                        retention_downloaded="0"
                        retention_undownloaded="60"/>
      </mpcs>
      <businessProcesses>
            <roles>
                  <role name="default"
                              value="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole"/>
                  <role name="exampleMessageProducer"
                              value="exampleMessageProducer"/>
                  <role name="exampleMessageReceiver"
                              value="exampleMessageReceiver"/>
```

```
            </roles>


<parties>
                  <partyIdTypes>
                        <partyIdType name="exampleType"
value="http://www.domibus.eu/exampleType"/>
                  </partyIdTypes>
                  <party name="instanceA"

      endpoint="http://UndefinedHostnameA:8080/domibus/services/msh">
                        <identifier partyId="instanceAId1"
partyIdType="exampleType"/>
                        <identifier partyId="instanceAId2"
partyIdType="exampleType"/>
                  </party>
                  <party name="instanceB"

      endpoint="http://UndefinedHostnameB:8080/domibus/services/msh">
                        <identifier partyId="instanceBId1"
partyIdType="exampleType"/>
                        <identifier partyId="instanceBId2"
partyIdType="exampleType"/>
                  </party>
            </parties>
            <meps>
                  <mep name="oneway" value="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay"/>
                  <mep name="twoway" value="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/twoWay"/>
                  <binding name="push" value="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push"/>
                  <binding name="pushAndPush"
value="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/push-and-push"/>
            </meps>
            <properties>
                  <property name="originalSenderProperty"
                              key="originalSender"
                              datatype="string"
                              required="true"/>
                  <property name="finalRecipientProperty"
```

```
                              key="finalRecipient"
                              datatype="string"
                              required="true"/>
                  <propertySet name="listPropertySet">
                        <propertyRef
property="finalRecipientProperty"/>
                        <propertyRef
property="originalSenderProperty"/>
                  </propertySet>
            </properties>
            <payloadProfiles>
                  <payload name="businessContentPayload"
                              cid="BRISPayload"
                              required="true"
                              mimeType="text/xml"/>
                  <payload name="businessContentAttachment"
                              cid="BRISAttachment"
                              required="false"
                              mimeType="application/octet-stream"/>
                  <payloadProfile name="BRISMessageProfile"
                              maxSize="1024">
                        <attachment name="businessContentPayload"/>
                        <attachment
name="businessContentAttachment"/>
                  </payloadProfile>
            </payloadProfiles>
            <securities>
                  <security name="signAndEncrypt"
                              policy="signEncrypt.xml"
                              signatureMethod="RSA_SHA256" />
            </securities>
            <errorHandlings>
                  <errorHandling name="BRISErrorHandling"
                              errorAsResponse="true"
                              businessErrorNotifyProducer="true"
                              businessErrorNotifyConsumer="true"
                              deliveryFailureNotifyProducer="true"/>
            </errorHandlings>
```

```
            <agreements>
                  <agreement name="exampleAgreement"
value="http://domibus.eu/agreement" type=""/>
            </agreements>
            <services>
                  <service name="as4Service" value="AS4"
type="exampleService"/>
            </services>
            <actions>
                  <action name="sendMessage" value="SendMessage"/>
            </actions>
            <as4>
                  <receptionAwareness
name="exampleReceptionAwarenessRetryThreeDuplicateDetectionTrue"
retry="1;6;CONSTANT" duplicateDetection="true"/>
                  <reliability
name="exampleReliabilityNonrepudiationTrueReplypatternResponse"
nonRepudiation="true" replyPattern="response"/>
            </as4>
            <legConfigurations>
                  <legConfiguration name="examplePushLegOne"
                              service="as4Service"
                              action="sendMessage"
                              defaultMpc="defaultMpc"

      reliability="exampleReliabilityNonrepudiationTrueReplypatternRe
sponse"
                              security="signAndEncrypt"

      receptionAwareness="exampleReceptionAwarenessRetryThreeDuplicat
eDetectionTrue"
                              errorHandling="BRISErrorHandling"
                              compressPayloads="false">
                              </legConfiguration>
            </legConfigurations>
            <process name="as4exampleProcess"
                        agreement="exampleAgreement"
                        mep="oneway"
                        binding="push"
                        initiatorRole="exampleMessageProducer"
```

```
                        responderRole="exampleMessageReceiver">
                  <initiatorParties>
                        <initiatorParty name="instanceA"/>
                        <initiatorParty name="instanceB"/>
                  </initiatorParties>
                  <responderParties>
                        <responderParty name="instanceA"/>
                        <responderParty name="instanceB"/>
                  </responderParties>
                  <legs>
                        <leg name="examplePushLegOne"/>
                  </legs>
            </process>
      </businessProcesses>
</db:configuration>
```

Remarks:

- In this setup we have allowed each party (instanceA or instanceB) to initiate the process. If only instanceA is supposed to send messages, we need to put only instanceA in <initiatorParties> and instanceB in <responderParties>.

- SSL mutual authentication is only required if we use HTTPS for endpoint. In that case the <CEF-eDelivery path>/modules/eu/europa/ec/cipa/configuration/main/domibus/clientauthentication.xml file is mandatory.

- The parameter maxSize (in green) represents the maximum size allowed for a message and its value can be edited according to the user's need.