



EUROPEAN COMMISSION

DIGIT
Connecting Europe Facility

Access Point

Quick Start Guide

Domibus 3.2.3

Version [1.00]

Status [Validated]

Date: 30/03/2017

Document Approver(s):

Approver Name	Role
BACIU Cosmin	Technical Office

Document Reviewers:

Reviewer Name	Role
BACIU Cosmin	Technical Office

Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.01	20/01/2017	CEF Support	Creation of the document based on the release 3.2.2 of Domibus
1.00	09/02/2017	Technical Office	Validation of the document

Table of Contents

1. INTRODUCTION	4
1.1. Purpose.....	4
1.2. References.....	5
1.3. Acronyms.....	5
2. PREREQUISITE	6
2.1. Installing JRE.....	6
2.2. Installing MySQL.....	6
3. CONFIGURATION	7
3.1. Overview.....	7
3.1.1. domibus-MSH-X.Y.Z-tomcat-full.zip.....	7
3.1.2. domibus-MSH-X.Y.Z-sample-configuration-and-testing.zip.....	8
4. TESTING	14
4.1. Default plugins.....	14
5. ANNEX 1 - PARAMETERS	15
6. ANNEX 2 - FIREWALL SETTINGS	16
7. ANNEX 3 - PROCESSING MODE	20
8. ANNEX 4 - DOMIBUS PMODE CONFIGURATION TO EBMS3 PMODE MAPPING	23
9. ANNEX 5 - INTRODUCTION TO AS4 SECURITY.....	29
10. LIST OF FIGURES	30
11. LIST OF TABLES	30
12. CONTACT INFORMATION	31

1. INTRODUCTION

1.1. Purpose

This release contains the AS4 Access Point of the CEF eDelivery Digital Service Infrastructure (DSI). It is important to note that this release of the AS4 Access Point contains Domibus 3.2.3. For more information about this release, please refer to CEF Digital.

This release of the CEF eDelivery Access Point is the result of significant collaboration among different EU policy projects, IT delivery teams and the CEF eDelivery DSI. Nevertheless, this eDelivery release is fully reusable by any other policy domain of the EU.

This release supports Tomcat 8, WebLogic 12c and WildFly 9. It is compatible with Oracle 10g+ and MySQL 5.5+. In this guide, we are covering Tomcat/MySQL configuration.

If you want to install Domibus on WildFly or WebLogic or if you want to have more information on Domibus configuration in general, please read the Administration guide available on the release page of Domibus.

Remark:

- *PostgreSQL is not officially supported.*

In other words, we will guide you to setup two Tomcat standalone Access Points, deployed on different machines, to exchange B2B documents securely over AS4 by:

- Deploying and configuring both Access Points (blue and red)
- Configuring processing mode files for both AS4 Access Points
- Using the provided AS4 Access Points certificates
- Setup the Access Points blue and red for running test cases (see §4 - "Testing")

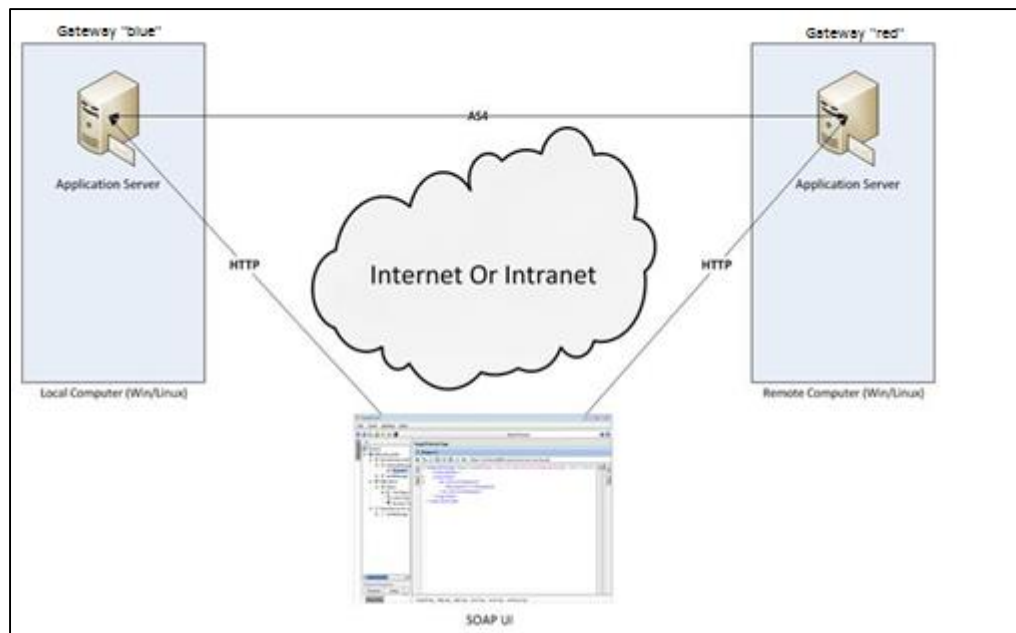


Figure 1 - Installation on two different machines

Remarks:

- *The same procedure can be extended to a third (or more) Access Point.*
- *This guide does not cover the preliminary network configuration allowing communication between separate networks (i.e. Proxy setup).*

1.2. References

Ref.	Document	Content outline
[REF1]		
[REF2]		
[REF3]		

1.3. Acronyms

Acronym	Description

2. PREREQUISITE

2.1. Installing JRE

- Java runtime environment (JRE), version 7 or 8:
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

2.2. Installing MySQL

- MySQL database server listening on the default port 3306:
<http://dev.mysql.com/downloads/>

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.

Remarks:

- *Please ensure that environment variable `JAVA_HOME` is set to JRE but also that the path for JRE and MySQL are set to their respective bin directory.*
- *If you intend to install both Access Points on the same server, you will need to change the ports of the red Access Point but also, create a new database schema, update the `domibus-datasource.xml` and change the ActiveMQ ports before starting the server to avoid conflicts.*

3. CONFIGURATION

3.1. Overview

3.1.1. [domibus-MSH-X.Y.Z-tomcat-full.zip](#)

Download the Domibus 3.2.3 Distribution from CEF Digital:

<https://ec.europa.eu/cefdigital/wiki/x/XwKGAg>

This package has the following structure and contains a naked version of Domibus:

Name	Size
domibus	68 891 766
sql-scripts	91 196
changelog.txt	4 034
upgrade-info.txt	17 451

Figure 2 - Package content

- **<CEF-eDelivery path>/domibus/bin** contains the executable batch file (Windows) and shell script (Linux) which are required to launch the Access Point.
- **<CEF-eDelivery path>/sql-scripts** contains the required application SQL code that needs to be executed on the MySQL database (and scripts for Oracle DB).

Remark:

<CEF-eDelivery path> is the location where you extracted the downloaded package.

- **<CEF-eDelivery path>/domibus** contains:

Name	Size
bin	768 523
conf	6 421 400
lib	7 335 433
logs	0
webapps	54 282 397
LICENSE	58 068
NOTICE	1 489
RELEASE-NOTES	6 913
RUNNING.txt	16 682

Figure 3 - eDelivery path/domibus content

- **conf** folder where you will find the *configuration files* (.xml used to administer your Tomcat and the default domibus configuration files)
- **logs** folder where the logs are stored
- **webapps** folder where the WAR files are stored

Name	Size
domibus.war	54 282 397

Figure 4 - Domibus WAR files

- **<CEF-eDelivery path>/domibus/conf/domibus** contains domibus configuration files.

Name	Size
internal	9 696
plugins	6 172 563
policies	7 221
domibus-configuration.xml	5 497
domibus-datasources.xml	5 561
domibus-datasources.xml.sha256	64
domibus-plugins.xml	2 000
domibus-security.xml	5 309
domibus-security.xml.sha256	64
domibus-transactions.xml	3 258
log4j.properties	1 904
persistence.xml	1 932

Figure 5 - Domibus configuration files

3.1.2. [domibus-MSH-X.Y.Z-sample-configuration-and-testing.zip](#)

Download the Domibus 3.2.3 configuration files sample from Nexus:

<https://ec.europa.eu/cefdigital/wiki/x/XwKGAg>

This package has the following structure and contains pre-configured files for Domibus:

Name	Type
conf	File folder
test	File folder

Figure 6 - Pre-configured files for Domibus

- **<CEF-eDelivery path>/test** contains a SOAP UI test project.
- **<CEF-eDelivery path>/conf/pmodes** contains two AS4 processing mode (xml file, one for blue and one for red Access Point) pre-configured to use compression, payload encryption, message signing and non-repudiation, according to the [eSENS AS4 profile](#).
- **<CEF-eDelivery path>/conf/domibus/keystores** contains a keystore (with the private keys of Access Point blue and Access Point red) and a truststore (with the public keys of Access Point *blue* and Access Point *red*) that can be used by both Access Points. Note that the keystore contains the private keys of both Access Points blue and red. This setup is not secured and is only proposed for convenience purpose. In production, the private key is only known by one participant and only deployed in his keystore. For this test release, each Access Point uses self-signed certificates. Please refer to §9 – "Annex 5 - Introduction to AS4 security" for more information about AS4 security.

Remark:

*The /conf folder in the sample archive should be unzipped in <CEF-eDelivery path>/domibus that already exists by merging it with its content. **Tomcat Standalone Access Point**. As described in the purpose of this guide, we need to configure two Access Points running on two separate machines. Therefore, the procedure below would need to be applied on both machines Hostname "blue" (<blue_hostname>:8080) and Hostname "red" (<red_hostname>:8080).*

1. Unzip the archives:

- a. Unzip **domibus-MSH-X.Y.Z-tomcat-full.zip** to a location on your physical machine, which will be referred in this document as your **<CEF-eDelivery path>**.
- b. The **/conf** folder in the **domibus-MSH-X.Y.Z-sample-configuration-and-testing.zip** should be unzipped in **<CEF-eDelivery path>/domibus**.

2. Prepare the MySQL database:

- a. Update the default properties of my.ini (Windows) or my.cnf (Linux) (MySQL Server File).
 - `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
```

- `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
larger logfile size will increase the time needed for the recovery process
innodb_log_file_size=512M
```

- *Restart MySQL service*
- b. Open a command prompt and navigate to this directory:
<CEF-eDelivery path>/sql-scripts.
 - c. Execute the following commands :

```
mysql -h localhost -u root --password=root -e "drop schema if exists domibus;create
schema domibus;alter database domibus charset=utf8 collate=utf8_bin; create user
edelivery identified by 'edelivery';grant all on domibus.* to edelivery;"
```

This creates a schema named **domibus** and the user named **edelivery** having all the privileges on the schema **Domibus**.

```
mysql -h localhost -u root --password=root domibus < mysql5innoDB-3.2.3.ddl
```

This creates the required tables in the **domibus** schema.

Remarks:

- *If you are using Windows, make sure to have mysql.exe added to your PATH variable.*
- *If you are using a different schema, please adapt your commands but also edit the <CEF-eDelivery path>/conf/domibus/domibus-datasources.xml file*

```
prop key="user">edelivery</prop>
<prop key="password">edelivery</prop>
<prop key="url">
jdbc:mysql://localhost:3306/domibus?pinGlobalTxToPhysicalConnection=true
</prop>
```

- d. Add MySQL JDBC driver (.jar file available on **MySQL official web site**) in the folder **<CEF-eDelivery path>/domibus/lib**.

Remark:

The version of the JDBC driver has to be mysql-connector-java-5.1.40.jar or higher.

3. Set JVM parameters

Domibus expects a single JVM parameter **\$domibus.config.location**, pointing towards the **<CEF-eDelivery path>/domibus/conf/domibus** folder.

You can do this by editing the first command lines of **<CEF-eDelivery path>\domibus\bin\catalina.bat** (Windows) or **<CEF-eDelivery path>/domibus/bin/catalina.sh** (Linux). Set **CATALINA_HOME** equal to the absolute path of the installation **<CEF-eDelivery path>/domibus**

- **For Windows :** Edit **<CEF-eDelivery path>\domibus\bin\catalina.bat** by adding the following lines right after the comments in the beginning of the file:

```
...
set CATALINA_HOME=<your_installation_path>
set JAVA_OPTS=%JAVA_OPTS% -Dfile.encoding=UTF-8 -Xms128m -Xmx1024m -XX:PermSize=64m
-XX:MaxPermSize=256m
set JAVA_OPTS=%JAVA_OPTS% -Ddomibus.config.location=%CATALINA_HOME%\conf\domibus
...
```

- **For Linux :** Edit **<CEF-eDelivery path>/domibus/bin/catalina.sh** by adding the following lines right after the comments in the beginning of the file:

```
...
export CATALINA_HOME=<your_installation_path>
export JAVA_OPTS=$JAVA_OPTS -Xms128m -Xmx1024m -XX:MaxPermSize=256m
export JAVA_OPTS="$JAVA_OPTS -Ddomibus.config.location=$CATALINA_HOME/conf/domibus"
...
```

- You can now start the Tomcat standalone Access Point on your computer.

Execute:

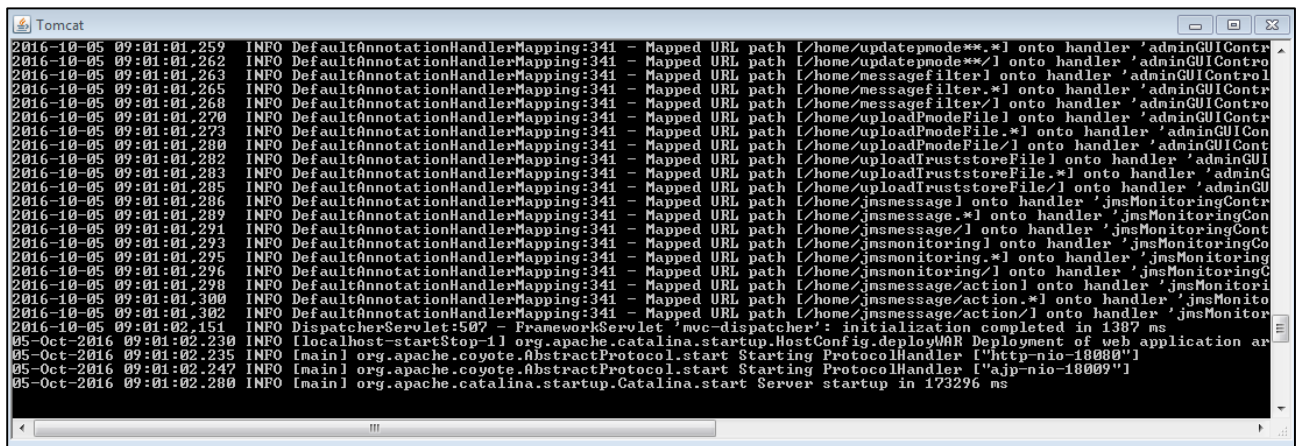
- For Windows :

```
cd <CEF-eDelivery path>\bin\  
startup.bat
```

- For Linux :

```
cd <CEF-eDelivery path>/bin/  
chmod +x *.sh  
./startup.sh
```

Expected result:



```
Tomcat
2016-10-05 09:01:01.259 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/updatepnode**.*] onto handler 'adminGUIContr
2016-10-05 09:01:01.262 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/updatepnode**.*] onto handler 'adminGUIContro
2016-10-05 09:01:01.263 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/messagefilter/] onto handler 'adminGUIControl
2016-10-05 09:01:01.265 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/messagefilter.*] onto handler 'adminGUIContro
2016-10-05 09:01:01.268 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/messagefilter/] onto handler 'adminGUIContro
2016-10-05 09:01:01.270 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/uploadPnodeFile/] onto handler 'adminGUIContro
2016-10-05 09:01:01.273 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/uploadPnodeFile.*] onto handler 'adminGUICon
2016-10-05 09:01:01.280 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/uploadPnodeFile/] onto handler 'adminGUICont
2016-10-05 09:01:01.282 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/uploadTruststoreFile] onto handler 'adminGUI
2016-10-05 09:01:01.283 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/uploadTruststoreFile.*] onto handler 'adminG
2016-10-05 09:01:01.285 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/uploadTruststoreFile/] onto handler 'adminG
2016-10-05 09:01:01.285 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmessage/] onto handler 'jmsMonitoringContr
2016-10-05 09:01:01.289 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmessage.*] onto handler 'jmsMonitoringCon
2016-10-05 09:01:01.291 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmessage/] onto handler 'jmsMonitoringCont
2016-10-05 09:01:01.293 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmonitoring/] onto handler 'jmsMonitoringCo
2016-10-05 09:01:01.295 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmonitoring.*] onto handler 'jmsMonitoringC
2016-10-05 09:01:01.296 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmonitoring/] onto handler 'jmsMonitoringC
2016-10-05 09:01:01.298 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmessage/action] onto handler 'jmsMonitori
2016-10-05 09:01:01.300 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmessage/action.*] onto handler 'jmsMonitori
2016-10-05 09:01:01.302 INFO DefaultAnnotationHandlerMapping:341 - Mapped URL path [/home/jmsmessage/action/] onto handler 'jmsMonitor
2016-10-05 09:01:02.151 INFO DispatcherServlet:507 - FrameworkServlet 'mvc-dispatcher': initialization completed in 1387 ms
05-Oct-2016 09:01:02.230 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web application ar
05-Oct-2016 09:01:02.235 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-18080"]
05-Oct-2016 09:01:02.247 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["ajp-nio-18009"]
05-Oct-2016 09:01:02.280 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in 173296 ms
```

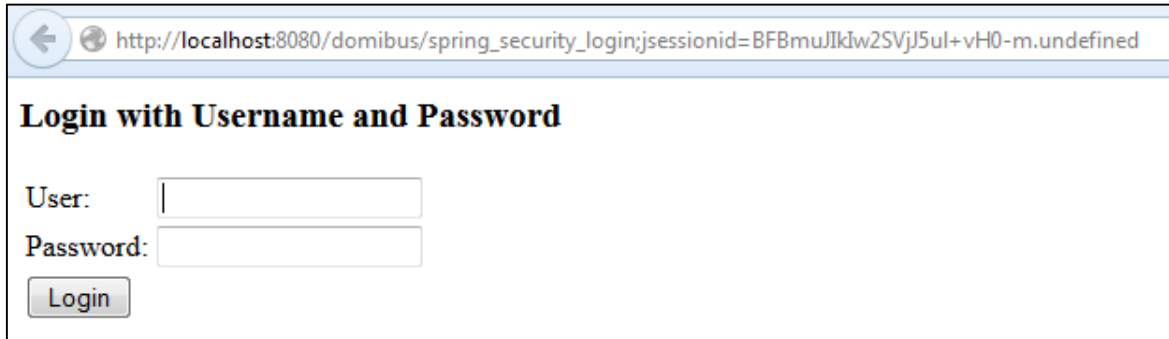
Figure 7 - Tomcat Access Point up and running

Remarks:

- No error message should appear in order to be successful but some warnings may appear.
- If the application server does not start properly, more details about the encountered errors can be found in the log files. Refer to <CEF-eDelivery path>/domibus/logs/

- 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:

To connect to the administration dashboard using your credentials (by default: login = **admin**; password = **123456**)



The screenshot shows a web browser window with the address bar displaying `http://localhost:8080/domibus/spring_security_login;jsessionid=BFBmuJlkw2SVj5ul+vH0-m.undefined`. The page content includes the heading "Login with Username and Password", a "User:" label followed by an input field, a "Password:" label followed by an input field, and a "Login" button.

Figure 8 - Domibus administration page

Remark:

- To allow the remote application to send a message to this machine, you would need to create a dedicated rule (to allow this port) from your local firewall (see §6 – "Annex 2 - Firewall Settings")

6. Upload PModes

Edit the two PMode files `<CEF-eDelivery path>/domibus/conf/domibus/pmodes/domibus-gw-sample-pmode-blue.xml` and `domibus-gw-sample-pmode-red.xml` and replace `<blue_hostname>` and `<red_hostname>` with their real hostnames or IPs:

```
<party name="red_gw"
  endpoint="http://<red_hostname>:8080/domibus/services/msh"
  allowChunking="false">
  <identifier partyId="domibus-red" partyIdType="partyTypeUrn"/>
</party>
<party name="blue_gw"
  endpoint="http://<blue_hostname>:8080/domibus/services/msh"
  allowChunking="false">
  <identifier partyId="domibus-blue" partyIdType="partyTypeUrn"/>
</party>
```

Figure 9 - PMode view

For more details about the provided PMode, see §8 – "Annex 4 - Domibus PMode Configuration to ebMS3 PMode mapping".

Upload the PMode file on both Access Points:

- 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>

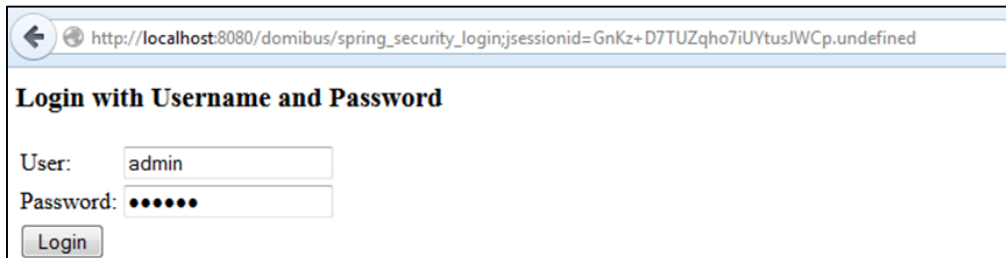


Figure 10 - Login to administration dashboard

- b. Click on the Configuration upload tab:

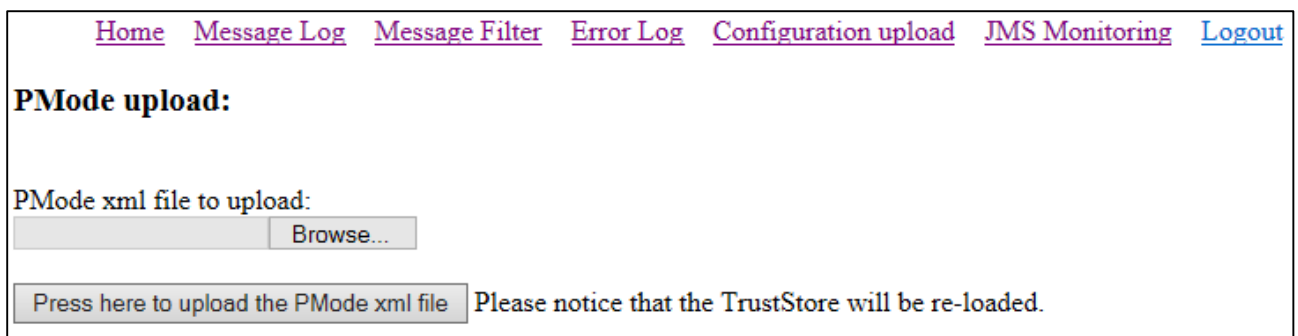


Figure 11 - PMode update

- c. Select your PMode from `<CEF-eDelivery path>domibus/conf/domibus/pmodes/` and click on the Press here to upload the PMode xml file button:

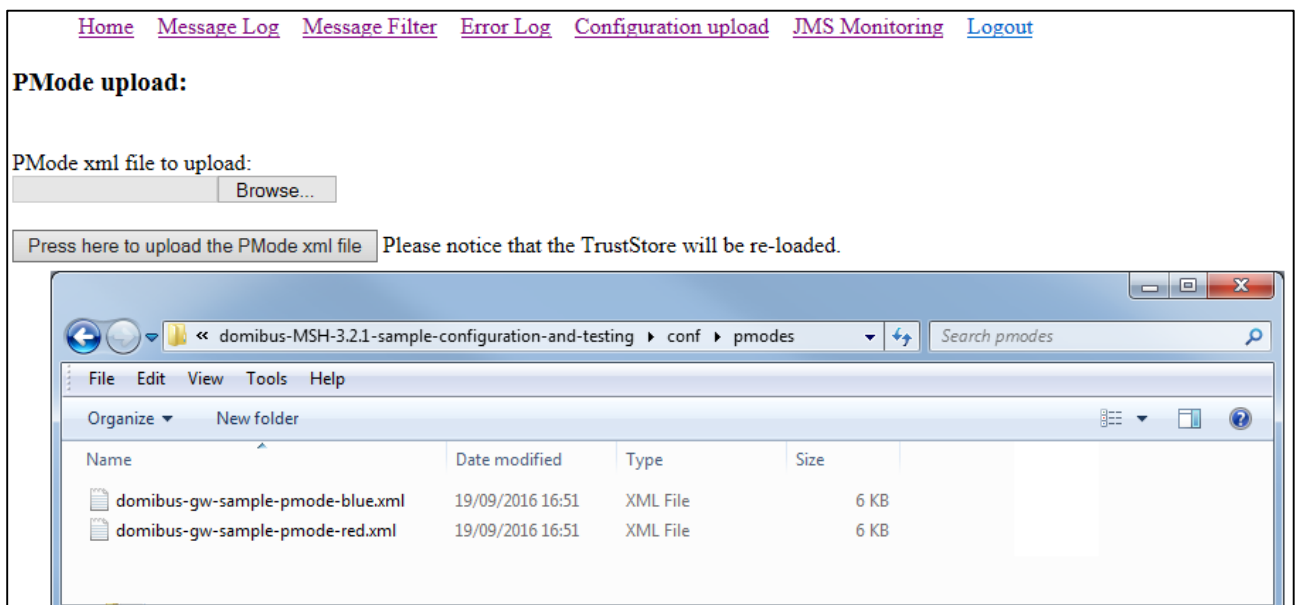


Figure 12 - PMode uploading

Remark:

- Every time a PMode is updated, the truststore is refreshed.

Now your Tomcat Access Points are running and ready to send or receive messages.

4. TESTING

As explained in the Release Notes document and to facilitate testing, we have developed a Reference Web Service endpoint to illustrate how participants can connect and interact with the AS4 Access Point to send messages.

In addition, it is possible for the backends to download received messages from their Access Point using a request (downloadMessage) defined in the same WSDL (Check Interface Control Document for the Default WS Plugin in the Single Web Portal for more details on the WSDL¹).

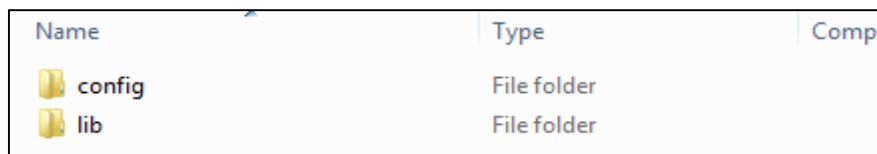
Please refer to the [Test Guide](#) for more detail regarding the Testing with a SoapUI Project

4.1. Default plugins

By default, we provide two plugins for sending and receiving/downloading messages via Domibus, a Web Service plugin and a JMS plugin.

By default, the Web Service plugin is deployed with the tomcat-full distribution.

Default JMS plugin is provided in a different archive, **domibus-MSH-X.Y.Z-default-jms-plugin.zip** including the binaries (domibus-default-jms-plugin-X.Y.Z.jar) and the configuration files (jms-plugin.xml and jms-business-defaults.properties).



Name	Type	Compr
config	File folder	
lib	File folder	

Figure 13 - Default JMS plugin

Unzip **domibus-MSH-X.Y.Z-default-jms-plugin.zip** to your <CEF-eDelivery path>.

An additional step is required to define filters for routing the messages towards each plugin and to configure which plugin is the first to handle the messages. By default the WS plugin is the first one and there are no filters.

Connect to the administration dashboard using your credentials (by default: login = **admin**; password = **123456**) to <http://localhost:8080/domibus/home> and go to MessageFilter tab. Use the arrows to move the preferred plugin to the top and save.

¹ <https://ec.europa.eu/cefdigital/wiki/x/XwKGAq>

5. ANNEX 1 - PARAMETERS

Parameters	Local Access Point (Gateway "blue")	Remote Access Point (Gateway "red")
Hostname	<blue_hostname>:8080	<red_hostname>:8080
Database	MySQL database	MySQL database
Administrator Page	Username: admin Password: 123456 http://localhost:8080/domibus/home	Username: admin Password: 123456 http://localhost:8080/domibus/home
Database Schema	edelivery	edelivery
Database connector	Username: edelivery Password: edelivery jdbc:mysql://localhost:3306/domibus*	Username: edelivery Password: edelivery jdbc:mysql://localhost:3306/domibus*
DB username/password	edelivery/edelivery	edelivery/edelivery
PModes XML files	pmodes/domibus-gw-sample-pmode-blue.xml	pmodes/domibus-gw-sample-pmode-red.xml

Table 1 - Local and Remote Access Points Parameters

* localhost represents the server name that hosts the database and the application server for their respective Access Point.

6. ANNEX 2 - FIREWALL SETTINGS

The firewall settings may prevent you from exchanging messages between your local and remote Tomcat Access Points.

To test the status of a port, run the command `telnet <server_ip> <port>`

Remark:

- *This utility is disabled quite often in Windows 7/8. To enable Telnet command line utilities:*
- *Click Start > Control Panel*
- *Click Programs and Features.*
- *Click Turn Windows features on or off.*
- *In the Windows Features dialog box, check the Telnet Client check box.*
- *Click OK. The system installs the appropriate files.*

Tomcat uses the following ports, make sure those are opened on both machines "blue" and "red" (TCP protocol):

- 8080 (HTTP port)
- 3306 (MySQL port)

This is how you can open a port:

Windows Firewall

1. Click on **Start** then on **Control Panel**
2. Click on **Windows Firewall** and then click on **Advanced Settings**.
3. Right click on **Inbound Rules** then on **New Rule**:

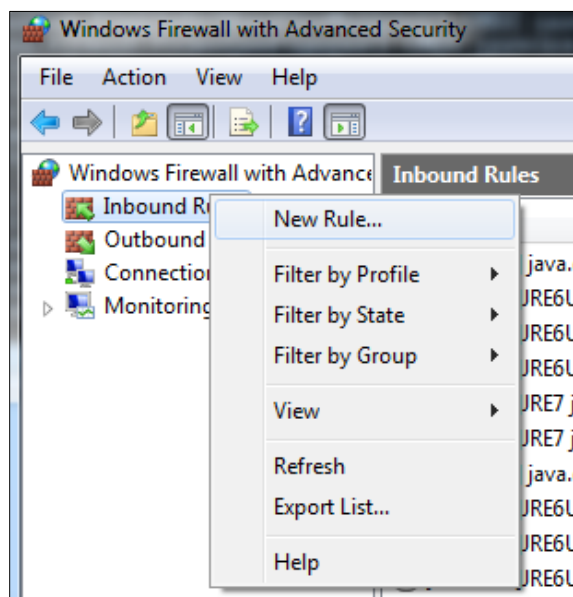


Figure 14 - Opening a port with Windows firewall

4. Select **Port** and click on **Next**:

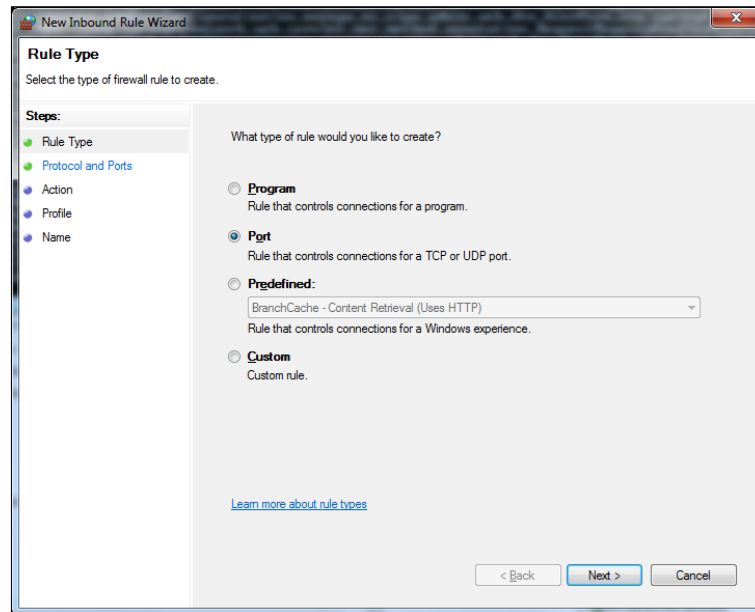


Figure 15 - Opening a port with Windows firewall - redefined rules

5. Enter a specific local port (e.g. 8080) and click on Next:

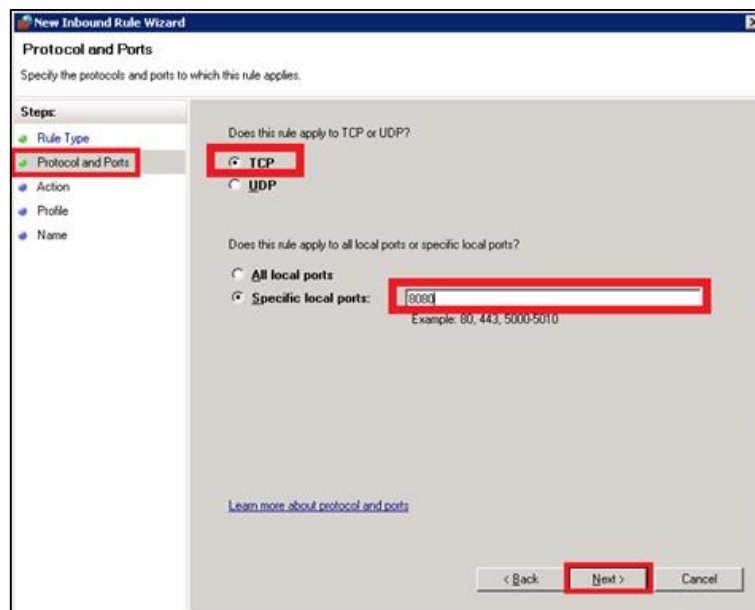


Figure 16 - Opening a port with Windows firewall - TCP

6. Select Allow the connection and click on Next:

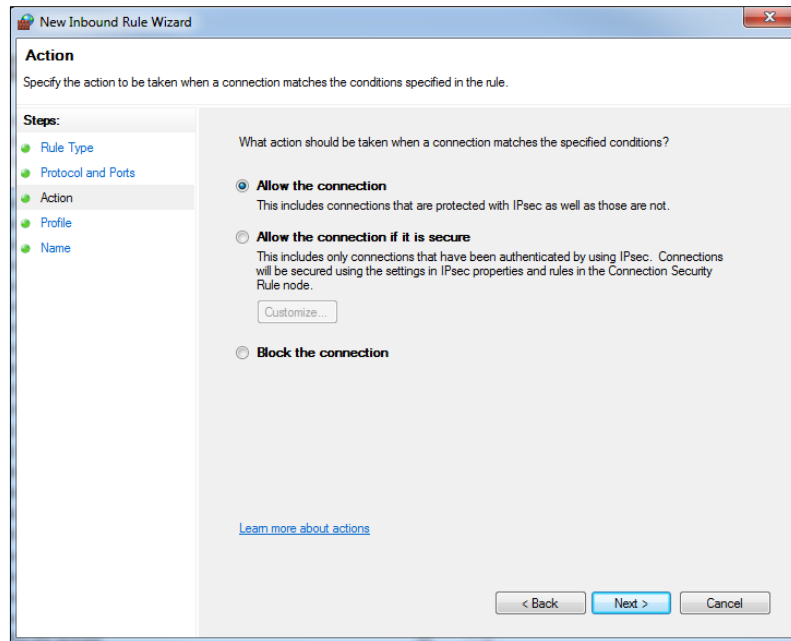


Figure 17 - Opening a port with Windows firewall - Action

7. Click on Next:

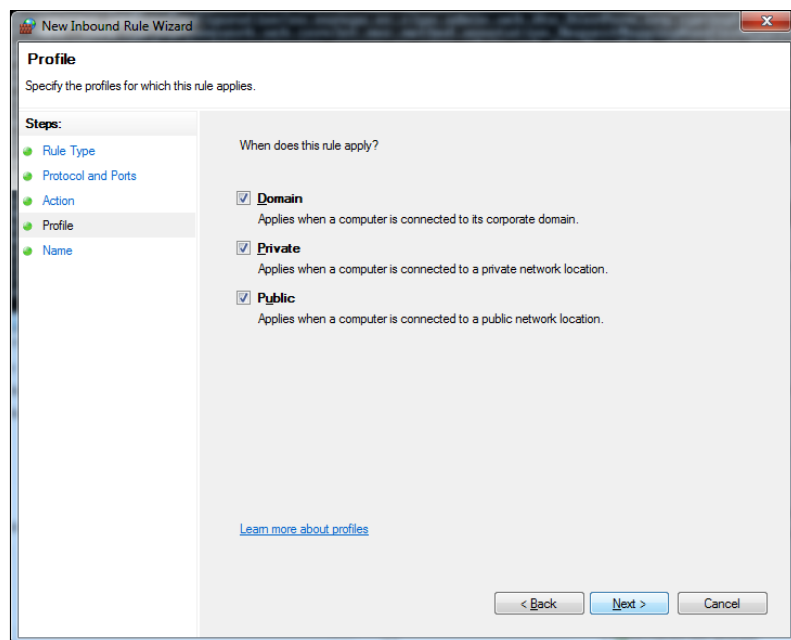


Figure 18 - Opening a port with Windows firewall - Profile

8. Name the rule and click on *Finish*:

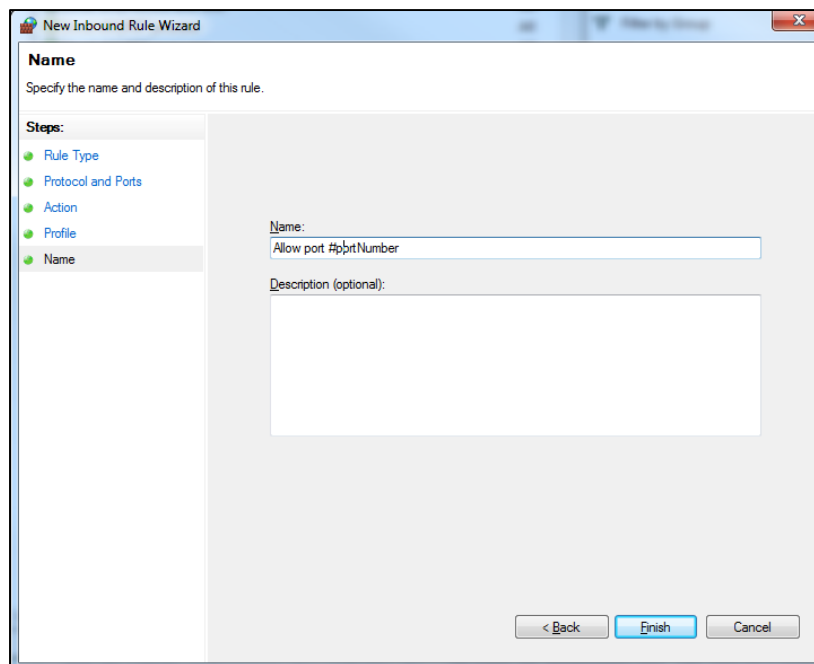


Figure 19 - Opening a port with Windows firewall - Name

Linux Firewall

These commands to open port 8080 need to be executed as **root** or **sudo su**:

```
#open port in firewall
firewall-cmd --zone=public --add-port=8080/tcp --permanent
firewall-cmd --reload

#check if the firewall port is open
firewall-cmd --list-ports | grep 8080
```

Remark:

You can substitute the port number 8080 for any other port.

7. ANNEX 3 - PROCESSING MODE

Processing modes (PModes) describe how messages are exchanged between AS4 partners (Access Point blue and Access Point red). These files contain the identifiers of each AS4 Access Point (identified as parties in the PMode file below).

Sender Identifier and Receiver Identifier represent the organizations that send and receive the business documents (respectively "domibus- blue" and "domibus-red"). They are both used in the authorization process (PMode). Therefore, adding, modifying or deleting a participant implies modifying the corresponding PMode files.

Here is an example of the content of a PMode XML file:

Remark:

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

```
<?xml version="1.0" encoding="UTF-8"?>
<db:configuration xmlns:db="http://domibus.eu/configuration" party="blue_gw">
  <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="14400"/>
  </mpcs>
  <businessProcesses>
  <roles>
    <role name="defaultInitiatorRole"
      value="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/initiator"/>
    <role name="defaultResponderRole"
      value="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/responder"/>
  </roles>
  <parties>
    <partyIdTypes>
      <partyIdType name="partyTypeUrn"
value="urn:oasis:names:tc:ebcore:partyid-type:unregistered"/>
    </partyIdTypes>
    <party name="red_gw"
      endpoint="http://<red_hostname>:8080/domibus/services/msh"
      allowChunking="false">
      <identifier partyId="domibus-red" partyIdType="partyTypeUrn"/>
    </party>
    <party name="blue_gw"
      endpoint="http://<blue_hostname>:8080/domibus/services/msh"
      allowChunking="false">
      <identifier partyId="domibus-blue" partyIdType="partyTypeUrn"/>
    </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="ecodexPropertySet">
    <propertyRef property="finalRecipientProperty"/>
    <propertyRef property="originalSenderProperty"/>
  </propertySet>
</properties>
<payloadProfiles>
  <payload name="businessContentPayload"
    cid="cid:message"
    required="true"
    mimeType="text/xml"/>
  <payload name="businessContentAttachment"
    cid="cid:attachment"
    required="false"
    mimeType="application/octet-stream"/>
  <payloadProfile name="MessageProfile"
    maxSize="40894464">
    <attachment name="businessContentPayload"/>
    <attachment name="businessContentAttachment"/>
  </payloadProfile>
</payloadProfiles>
<securities>
  <security name="eDeliveryPolicy"
    policy="eDeliveryPolicy.xml"
    signatureMethod="RSA_SHA256" />
  <security name="noSigNoEnc"
    policy="doNothingPolicy.xml"
    signatureMethod="RSA_SHA256"/>
  <security name="eSensPolicy"
    policy="eSensPolicy.xml"
    signatureMethod="RSA_SHA256"/>
</securities>
<errorHandlings>
  <errorHandling name="demoErrorHandling"
    errorAsResponse="true"
    businessErrorNotifyProducer="false"
    businessErrorNotifyConsumer="false"
    deliveryFailureNotifyProducer="false"/>
</errorHandlings>
<agreements>
  <agreement name="agreement1" value="A1" type=""/>
  <agreement name="agreement2" value="A2" type=""/>
  <agreement name="agreement3" value="A3" type=""/>
</agreements>
<services>

```

```

    <service name="testService1" value="bdx:noprocess" type="tc1"/>
  </services>
  <actions>
    <action name="tc1Action" value="TC1Leg1"/>
    <action name="tc2Action" value="TC2Leg1"/>
  </actions>
  <as4>
    <receptionAwareness name="receptionAwareness" retry="12;4;CONSTANT"
duplicateDetection="true"/>
    <reliability name="AS4Reliability" nonRepudiation="true"
replyPattern="response"/>
    <reliability name="noReliability" nonRepudiation="false"
replyPattern="response"/>
  </as4>
  <legConfigurations>
    <legConfiguration name="pushTestcase1tc1Action"
      service="testService1"
      action="tc1Action"
      defaultMpc="defaultMpc"
      reliability="AS4Reliability"
      security="eDeliveryPolicy"
      receptionAwareness="receptionAwareness"
      propertySet="ecodexPropertySet"
      payloadProfile="MessageProfile"
      errorHandling="demoErrorHandling"
      compressPayloads="true"/>
    <legConfiguration name="pushTestcase1tc2Action"
      service="testService1"
      action="tc2Action"
      defaultMpc="defaultMpc"
      reliability="AS4Reliability"
      security="eSensPolicy"
receptionAwareness="receptionAwareness"
      propertySet="ecodexPropertySet"
      payloadProfile="MessageProfile"
errorHandling="demoErrorHandling"
      compressPayloads="true"/>
  </legConfigurations>
  <process name="tc1Process"
    agreement=""
    mep="oneway"
    binding="push"
    initiatorRole="defaultInitiatorRole"
    responderRole="defaultResponderRole">
    <initiatorParties>
      <initiatorParty name="blue_gw"/>
      <initiatorParty name="red_gw"/>
    </initiatorParties>
    <responderParties>
      <responderParty name="blue_gw"/>
      <responderParty name="red_gw"/>
    </responderParties>
    <legs>
      <leg name="pushTestcase1tc1Action"/>
      <leg name="pushTestcase1tc2Action"/>
    </legs>
  </process>
</businessProcesses>
</db:configuration>

```

8. ANNEX 4 - DOMIBUS PMode CONFIGURATION TO EBMS3 PMode MAPPING

The following table provides additional information concerning the Domibus PMode configuration (pconf) files.

Domibus pconf	EbMS3 Specification [ebMS3CORE] [AS4-Profile]	Description
MPCs	-	Container which defines the different MPCs (Message Partition Channels).
MPC	PMode[1].BusinessInfo.MPC: The value of this parameter is the identifier of the MPC (Message Partition Channel) to which the message is assigned. It maps to the attribute Messaging/ UserMessage[@type]	Message Partition Channel allows the partition of the flow of messages from a Sending MSH to a Receiving MSH into several flows, each of which is controlled separately. An MPC also allows merging flows from several Sending MSHs into a unique flow that will be treated as such by a Receiving MSH. The value of this parameter is the identifier of the MPC to which the message is assigned.
MessageRetentionDownloaded	-	Retention interval for messages already delivered to/downloaded by the backend.
MessageRetentionUnDownloaded	-	Retention interval for messages not yet delivered to/downloaded by the backend.
Parties	-	Container which defines the different PartyIdTypes, Party and Endpoint.
PartyIdTypes	maps to the attribute Messaging/UserMessage/ PartyInfo/From/PartyId[@type] or to Messaging/UserMessage/ PartyInfo/To/PartyId[@type]	It refers to the type of a party. The value is required.
Party ID	maps to Messaging/UserMessage/ PartyInfo/From/PartyId or to Messaging/UserMessage/ PartyInfo/To/PartyId	The ebCore Party ID type can simply be used as an identifier format and therefore as a convention for values to be used in configuration and – as such – does not require any specific solution building block.

Endpoint	maps to PMode[1].Protocol.Address	The endpoint is a party attribute that contains the link to the MSH. The value of this parameter represents the address (endpoint URL) of the Receiver MSH (or Receiver Party) to which Messages under this PMode leg are to be sent. Note that a URL generally determines the transport protocol (e.g. if the endpoint is an email address, then the transport protocol must be SMTP; if the address scheme is "http", then the transport protocol must be HTTP).
AS4	-	Container
Reliability [@Nonrepudiation] [@ReplyPattern]	Nonrepudiation maps to PMode[1].Security.SendReceipt.NonRepudiation ReplyPattern maps to PMode[1].Security.SendReceipt.ReplyPattern	PMode[1].Security.SendReceipt.NonRepudiation : value = 'true' (to be used for non-repudiation of receipt), value = 'false' (to be used simply for reception awareness). PMode[1].Security.SendReceipt.ReplyPattern: value = 'Response' (sending receipts on the HTTP response or back-channel). PMode[1].Security.SendReceipt.ReplyPattern: value = 'Callback' (sending receipts use a separate connection.)
ReceptionAwareness [@retryTimeout] [@retryCount] [@strategy] [@duplicateDetection]	retryTimeout maps to PMode[1].ReceptionAwareness.Retry=true PMode[1].ReceptionAwareness.Retry.Parameters retryCount maps to PMode[1].ReceptionAwareness.Retry.Parameters strategy maps to PMode[1].ReceptionAwareness.Retry.Parameters duplicateDetection maps to PMode[1].ReceptionAwareness.DuplicateDetection	These parameters are stored in a composite string. <ul style="list-style-type: none"> • retryTimeout defines timeout in minutes. • retryCount is the total number of retries. • strategy defines the frequency of retries. The only strategy available as of now is CONSTANT. • duplicateDetection allows to check duplicates when receiving twice the same message. The only duplicateDetection available as of now is TRUE.
Securities	-	Container
Security	-	Container
Policy	PMode[1].Security.* NOT including PMode[1].Security.X509.Signature.Algorithm	The parameter in the pconf file defines the name of a WS-SecurityPolicy file.
SignatureMethod	PMode[1].Security.X509.Signature.Algorithm	This parameter is not supported by WS-SecurityPolicy and therefore it is defined separately.

BusinessProcessConfiguration	-	Container
Agreements	maps to Messaging/ UserMessage/ CollaborationInfo/ AgreementRef[@type]	This OPTIONAL element occurs zero times or once. The AgreementRef element is a string that identifies the entity or artifact governing the exchange of messages between the parties.
Actions	-	Container
Action	maps to Messaging/ UserMessage/ CollaborationInfo/Action	This REQUIRED element occurs once. The element is a string identifying an operation or an activity within a Service that may support several of these
Services	-	Container
ServiceTypes Type	maps to Messaging/ UserMessage/ CollaborationInfo/ Service[@type]	This REQUIRED element occurs once. It is a string identifying the service that acts on the message and it is specified by the designer of the service. The type attribute is also required.
MEP [@Legs]	-	An ebMS MEP defines a typical choreography of ebMS User Messages which are all related through the use of the referencing feature (RefToMessageId). Each message of an MEP Access Point refers to a previous message of the same Access Point, unless it is the first one to occur. Messages are associated with a label (e.g. request, reply) that precisely identifies their direction between the parties involved and their role in the choreography.
Bindings	-	Container
Binding	-	The previous definition of ebMS MEP is quite abstract and ignores any binding consideration to the transport protocol. This is intentional, so that application level MEPs can be mapped to ebMS MEPs independently from the transport protocol to be used.
Roles	-	Container

Role	<p>maps to PMode.Initiator.Role or PMode.Responder.Role depending on where this is used. In ebMS3 message this defines the content of the following element:</p> <ul style="list-style-type: none"> • For Initiator: Messaging/UserMessage/PartyInfo/From/Role • For Responder: Messaging/UserMessage/PartyInfo/To/Role 	<p>The required role element occurs once, and identifies the authorized role (fromAuthorizedRole or toAuthorizedRole) of the Party sending the message (when present as a child of the From element), or receiving the message (when present as a child of the To element). The value of the role element is a non-empty string, with a default value of http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole. Other possible values are subject to partner agreement.</p>
Processes	-	Container
PayloadProfiles	-	Container
Payloads	-	Container
Payload	<p>maps to PMode[1].BusinessInfo.PayloadProfile</p>	<p>This parameter allows specifying some constraint or profile on the payload. It specifies a list of payload parts.</p> <p>A payload part is a data structure that consists of five properties:</p> <ol style="list-style-type: none"> 1. name (or Content-ID) that is the part identifier, and can be used as an index in the notation PayloadProfile; 2. MIME data type (text/xml, application/pdf, etc.); 3. name of the applicable XML Schema file if the MIME data type is text/xml; 4. maximum size in kilobytes; 5. Boolean string indicating whether the part is expected or optional, within the User message. <p>The message payload(s) must match this profile.</p>
ErrorHandlings	-	Container
ErrorHandling	-	Container

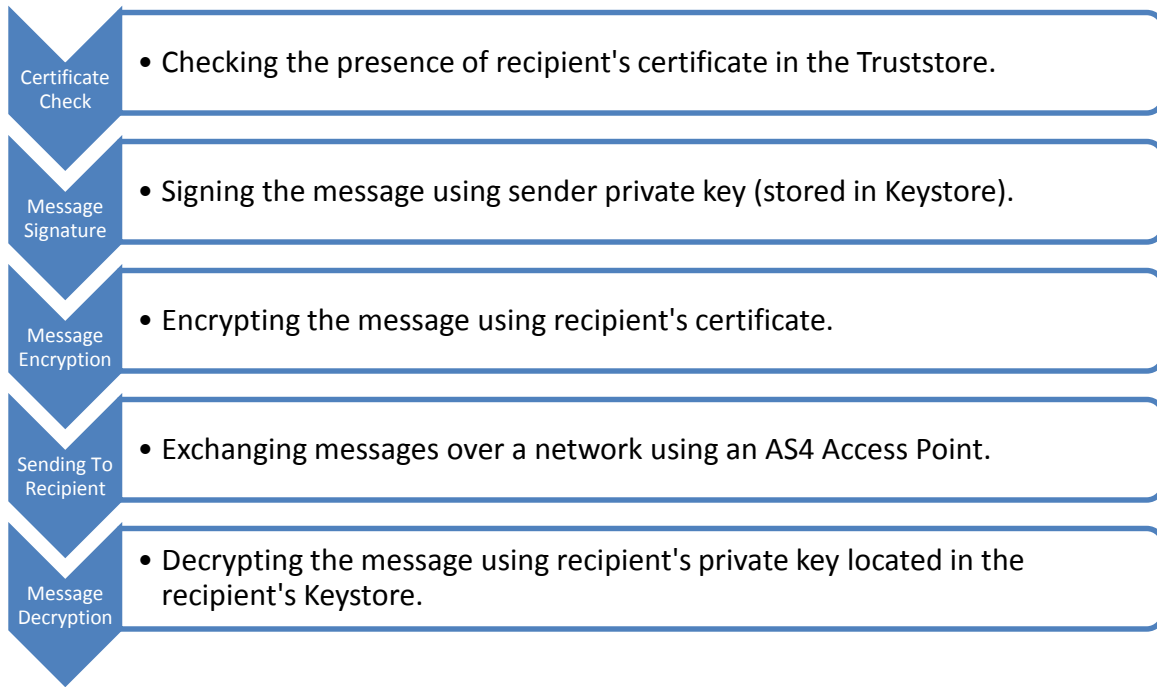
ErrorAsResponse	maps to PMode[1].ErrorHandling.Re port.AsResponse	This Boolean parameter indicates (if true) that errors generated from receiving a message in error are sent over the back-channel of the underlying protocol associated with the message in error. If false, such errors are not sent over the back-channel.
ProcessErrorNotifyProducer	maps to PMode[1].ErrorHandling.Re port.ProcessErrorNotifyProd ucer	This Boolean parameter indicates whether (if true) the Producer (application/party) of a User Message matching this PMode should be notified when an error occurs in the Sending MSH, during processing of the User Message to be sent.
ProcessErrorNotifyConsumer	maps to PMode[1].ErrorHandling.Re port.ProcessErrorNotifyProd ucer	This Boolean parameter indicates whether (if true) the Consumer (application/party) of a User Message matching this PMode should be notified when an error occurs in the Receiving MSH, during processing of the received User message.
DeliveryFailureNotifyProducer	maps to PMode[1].ErrorHandling.Re port.DeliveryFailuresNotifyP roducer	When sending a message with this reliability requirement (Submit invocation), one of the two following outcomes shall occur: - The Receiving MSH successfully delivers (Deliver invocation) the message to the Consumer. - The Sending MSH notifies (Notify invocation) the Producer of a delivery failure.
Legs	-	Container

Leg	-	Because messages in the same MEP may be subject to different requirements - e.g. the reliability, security and error reporting of a response may not be the same as for a request – the PMode will be divided into legs. Each user message label in an ebMS MEP is associated with a PMode leg. Each PMode leg has a full set of parameters for the six categories above (except for General Parameters), even though in many cases parameters will have the same value across the MEP legs. Signal messages that implement transport channel bindings (such as PullRequest) are also controlled by the same categories of parameters, except for BusinessInfo group.
Process	-	In Process everything is plugged together.

Table 2 - Domibus pconf to ebMS3 mapping

9. ANNEX 5 - INTRODUCTION TO AS4 SECURITY

(1) To secure the exchanges between Access Points "blue" and "red" (Access Point "blue" is sending a message to Access Point "red" in this example), it is necessary to set up each Access Point's keystore and *truststore* accordingly. The diagram below shows a brief explanation of the main steps of this process:



In order to exchange B2B messages and documents between Access Points blue and red, it is necessary to check the following:

For blue	For red
Check that the <i>blue_gw</i> private key is in the <i>gateway_keystore.jks</i> , if not add it.	Check that <i>red_gw</i> private key is in the <i>gateway_keystore.jks</i> , if not add it.
In <i>domibus-security.xml</i> : the keystore alias should be <i>blue_gw</i> , you may edit the keystore password (by default <i>test123</i>), and the path to <i>gateway_keystore.jks</i> and <i>gateway_truststore.jks</i> (if you change it).	In <i>domibus-security.xml</i> : the keystore alias should be <i>red_gw</i> , you may edit the keystore password (by default <i>test123</i>) if you need to, and the path to <i>gateway_keystore.jks</i> and <i>gateway_truststore.jks</i> (if you change it).
Check that <i>red_gw</i> certificate (public key of red) is in <i>gateway_truststore.jks</i> of blue, if not add it.	Check that <i>blue_gw</i> certificate (public key of blue) is in <i>gateway_truststore.jks</i> of red, if not, add it.

Table 3 - Checking B2B message exchanges (Access Points blue and red)

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 Access Point).

Remark:

It is necessary to open the required ports when Access Point blue or Access Point red is behind a local firewall. (e.g. port 8080 is not opened by default in Windows; we would need to create a dedicated rule on Windows firewall to open TCP 8080 port). See § 6 – "Annex 2 - Firewall Settings".

10. LIST OF FIGURES

Figure 1 - Installation on two different machines	4
Figure 2 - Package content	7
Figure 3 - eDelivery path/domibus content	7
Figure 4 - Domibus WAR files	7
Figure 5 - Domibus configuration files	8
Figure 6 - Pre-configured files for Domibus	8
Figure 7 - Tomcat Access Point up and running	11
Figure 8 - Domibus administration page	12
Figure 9 - PMode view	12
Figure 10 - Login to administration dashboard	13
Figure 11 - PMode update	13
Figure 12 - PMode uploading	13
Figure 13 - Default JMS plugin	14
Figure 14 - Opening a port with Windows firewall	16
Figure 15 - Opening a port with Windows firewall - redefined rules	17
Figure 16 - Opening a port with Windows firewall - TCP	17
Figure 17 - Opening a port with Windows firewall - Action	18
Figure 18 - Opening a port with Windows firewall - Profile	18
Figure 19 - Opening a port with Windows firewall - Name	19

11. LIST OF TABLES

Table 1 - Local and Remote Access Points Parameters	15
Table 2 - Domibus pconf to ebMS3 mapping	28
Table 3 - Checking B2B message exchanges (Access Points blue and red)	29

12. CONTACT INFORMATION

CEF Support Team

By email: CEF-EDELIVERY-SUPPORT@ec.europa.eu

By phone: +32 2 299 09 09

- Standard Service: 8am to 6pm (Normal EC working Days)
- Standby Service*: 6pm to 8am (Commission and Public Holidays, Weekends)

** Only for critical and urgent incidents and only by phone*