



EUROPEAN COMMISSION

DIGIT  
Connecting Europe Facility

## Service Metadata Publisher

### Administration Guide

#### SMP 4.X

Version [2.6]

Status [Final]

© European Union, 2018

Reuse of this document is authorised provided the source is acknowledged. The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents.

Date: 05/12/2018

## Document Approver(s):

Approver Name	Role
Adrien FERAL	

## Document Reviewers:

Reviewer Name	Role
Joze Rihtarsic	Developer
Caroline AEBY	CEF Support

## Summary of Changes:

Version	Date	Created by	Short Description of Changes
V0.1	22/02/2016	DHENEIN Christophe	Initial Document Creation
V1.0	15/06/2017	Chaouki BERRAH (CEFS), Christophe DHENEIN (CEFS)	Document restructuring and updating.
V1.1	16/06/2016	Chaouki BERRAH (CEFS), Christophe DHENEIN (CEFS)	3.0.0-RC2 changed to 3.X Screens updated.
V1.2	12/02/2018	Chaouki BERRAH	Version 4.0 RC1 changes added
V1.3	16/02/2018	Chaouki BERRAH	Update after test installation
V1.4	21/02/2018	Chaouki BERRAH	Pawel changes included.
V1.5	26/02/2018	Chaouki BERRAH	Links added
V1.6	28/02/2018	Chaouki BERRAH Caroline AEBY	Updates
V1.7	20/03/2018	CEF Support	Reuse notice added
V1.8	11/06/2018	Chaouki BERRAH	Document update
V1.9	28/06/2018	CEF Support	References to nexus updated.
V2.0	01/10/2018	Caroline AEBY	No more standby service
V2.1	18/10/2018	Chaouki BERRAH	Updates
V2.2	23/10/2018	Caroline AEBY	SMP 4.1 RC – SMP admin console
V2.3	25/10/2018	Joze Rihtarsic	SMP 4.1 Updates
V2.4	15/11/2018	Joze Rihtarsic Chaouki BERRAH	Oracle Script Changes for Migration purposes
V2.5	28/11/2018	Joze Rihtarsic Chaouki BERRAH	SMP 4.1 Updates
V2.6	04/12/2018	Chaouki BERRAH	Weblogic and user creation Updates

## Table of Contents

<b>1. INTRODUCTION .....</b>	<b>6</b>
1.1. Purpose.....	6
<b>2. CONVENTION .....</b>	<b>7</b>
Example 1: Sample Oracle Statement:.....	7
Example 2: Sample Configuration File:.....	7
<b>3. PREREQUISITES.....</b>	<b>8</b>
3.1. Binaries repository .....	8
3.2. Source Code Repository .....	8
3.3. Database Scripts .....	9
<b>4. DEPLOYMENT .....</b>	<b>10</b>
4.1. Deployment overview .....	10
<b>5. DATABASE CREATION .....</b>	<b>11</b>
5.1. MySQL.....	11
5.2. Oracle Database .....	11
<b>6. ORACLE WEBLOGIC CONFIGURATION .....</b>	<b>13</b>
6.1. Disabling the Authentication on the WebLogic.....	14
6.2. Configuring the Extra CLASSPATH for WebLogic.....	14
<b>7. TOMCAT CONFIGURATION.....</b>	<b>16</b>
7.1. Configuring the Extra CLASSPATH for Tomcat.....	16
7.2. JDBC Driver .....	17
<b>8. SMP CONFIGURATION .....</b>	<b>18</b>
8.1. Database configuration .....	18
8.1.1. Oracle Database: .....	18
8.1.2. MySQL: .....	18
8.2. SMP Keystore .....	19
8.2.1. XMLDSIG response signing Keystore (DEPRECATED since 4.1.0.FR) .....	19
8.2.2. SML Keystore (DEPRECATED since 4.1.0.FR) .....	20
8.2.3. Initializing and merging new keystore.....	20
<b>9. SMP .WAR FILE DEPLOYMENT .....</b>	<b>22</b>
9.1.1. Tomcat.....	22
9.1.2. Oracle WebLogic.....	22
9.1.3. Verification of the Installation.....	22
<b>10. CONFIGURING THE CEF SMP FOR USE WITH AN SML.....</b>	<b>24</b>
10.1. Configuring the BDMSL Integration.....	24

10.2. Configuring the SML URL.....	24
10.3. SMP authentication to an SML.....	24
10.3.1. Plain Text HTTP.....	24
10.3.2. HTTPS/TLS.....	25
<b>11. SMP USER MANAGEMENT.....</b>	<b>26</b>
11.1. User Roles.....	26
11.2. BCrypt password generation .....	27
11.3. SMP Database User Creation .....	28
11.3.1. SYSTEM_ADMIN SMP User creation .....	28
11.3.2. Admin SMP User Creation.....	29
11.3.3. Admin ServiceGroup User Creation .....	29
<b>12. LOGGING CONFIGURATION .....</b>	<b>30</b>
12.1. Logging properties.....	30
<b>13. SOAPUI TESTING .....</b>	<b>32</b>
13.1. Creation, update and deletion of Service Groups.....	32
13.1.1. Create a Service Group.....	32
13.1.2. Update a Service Group .....	32
13.1.3. Delete a ServiceGroup.....	33
13.2. Creation, update and deletion of Service Metadata.....	33
13.2.1. Create a Service Metadata .....	33
13.2.2. Update Service Metadata.....	34
13.2.3. Delete Service Metadata.....	35
<b>14. THE SWAGGERUI INTERFACE .....</b>	<b>36</b>
14.1. Introduction.....	36
14.2. Downloading the CEF SMP SwaggerUI web application project.....	36
14.3. Configuring the SMP SwaggerUI.....	37
14.4. Generating the Web Application Archive (.war file) .....	38
14.5. Deploy the SMP SwaggerUI war file.....	38
14.5.1. On Tomcat .....	38
14.5.2. On WebLogic: .....	39
<b>15. SMP COMPILATION.....</b>	<b>40</b>
15.1. Compilation prerequisites .....	40
15.1.1. Supported Operating System Platform .....	40
15.1.2. Software Requirements.....	40
15.2. Downloading the source code.....	40
15.3. Compilation .....	41
<b>16. SMP CONFIGURATION FILE AND TABLE.....</b>	<b>43</b>
16.1. Multitenancy and Multidomain Support.....	43
16.2. The smp.config.properties file .....	43

16.2.1. Detailed SMP configuration properties.....	46
16.2.1.1. bdmsl.integration.url.....	51
16.3. smp_domain table configuration .....	51
16.3.1. Example: Update the default single domain smp_domain table record: .....	51
<b>17. SMP ADMIN CONSOLE .....</b>	<b>52</b>
<b>18. CONTACT INFORMATION .....</b>	<b>53</b>

## 1. INTRODUCTION

This Administration Guide is intended for Administrators who are in charge of installing, managing and troubleshooting an eDelivery SMP (Service Metadata Publisher).

### 1.1. Purpose

The purpose of this guide is to provide detailed information on how to deploy and configure an SMP 4.X on either a WebLogic or Tomcat Application Server with either MySQL or Oracle database.

It also provides detailed descriptions of the related Security Configurations (Certificates).

There is also a section on the use of Soap UI to create, update and delete SMP Service Groups and Metadata.

Another section describes an alternative method to perform the creation, update and deletions using Swagger UI.

## 2. CONVENTION

The Commands and Configuration files listed in this document usually contain a mix of reserved words (commands, instructions and system-related special words), user-defined words (chosen by the user) as well as comments and default/preferred values for some fields or variables.

The conventions used in this document, to distinguish between them, are the following:

- **Bold** is used for "reserved" words and commands.
- *Normal italic* together with a short description of the argument is used for user-defined names (chosen by yourself to designate items like users, passwords, database etc.). It normally contains at least 2 words separated by "\_".
- ***Bold and italic*** is used for advisable values which can be changed by the user depending on their infrastructure.
- Comments are sometimes added to describe the purpose of the commands, usually enclosed in brackets ().
- By default, non-OS specific paths will be described using Linux patterns.

### Example 1: Sample Oracle Statement:

```
create user smp_user identified by smp_password;
```

```
grant all privileges to smp_user;
```

(Where *smp\_user* and *smp\_password* are names chosen by the user)

### Example 2: Sample Configuration File:

```
jdbc.driver = com.mysql.jdbc.Driver
```

```
jdbc.url = jdbc:mysql://localhost:3306/smp_database
```

```
jdbc.user = smp_user
```

```
jdbc.password = smp_password
```

```
target-database = MySQL
```

(Where: *smp\_user*, *smp\_database* and *smp\_password* are names chosen by the user.

***localhost:3306*** represents hostname:port parameters of the MySQL database.)

## 3. PREREQUISITES

Please install the following software on the target system. For further information and installation details, please refer to the software owner's documentation.

- Java runtime environment is now (JRE) 8 **only**:  
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>
- **One** of the supported Database Management Systems :
  - MySQL 5,6 or above
  - Oracle 10g+
- **One** of the supported Application Servers:
  - WebLogic 12c
  - Tomcat 8

### 3.1. Binaries repository

The CEF SMP artefacts can be downloaded from the CEF Digital site<sup>1</sup>.

### 3.2. Source Code Repository

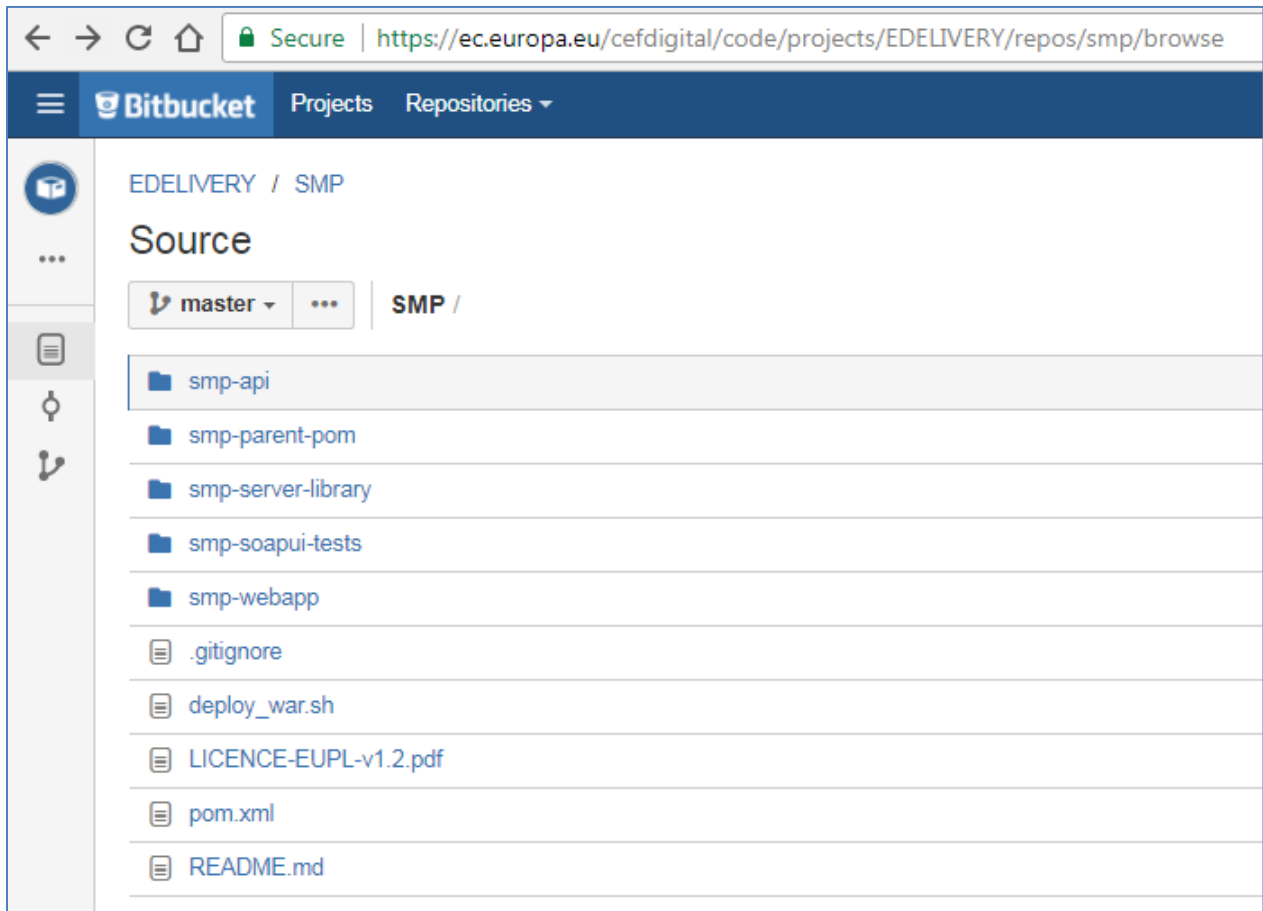
The source code of CEF SMP is available in the **GIT** repository at the following location:

<https://ec.europa.eu/cefdigital/code/projects/EDELIVERY/repos/smp/browse>

---

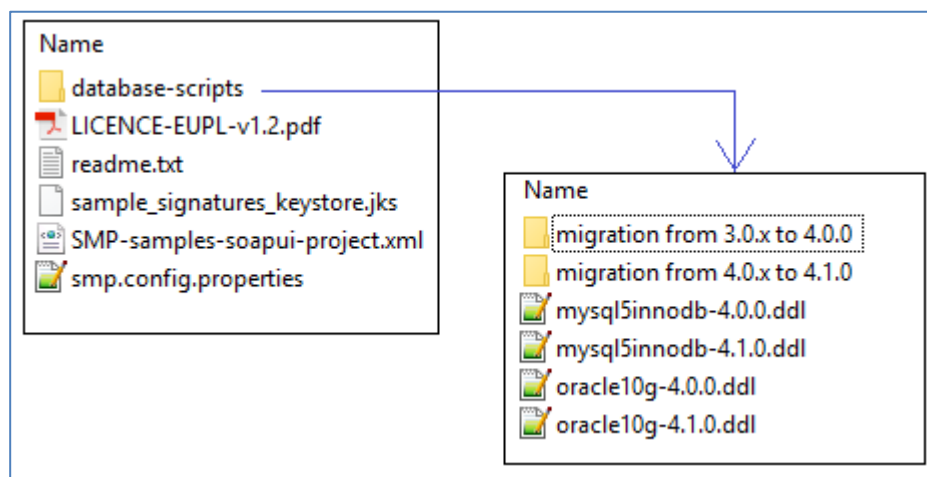
<sup>1</sup> <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP>





### 3.3. Database Scripts

The scripts to create (or migrate) the Oracle or MySQL databases are included in the following downloadable zip file from the CEF Digital site (section §3.1): smp-4.x-setup.zip.



## 4. DEPLOYMENT

### 4.1. Deployment overview

As mentioned in the prerequisites, the deployment of the CEF SMP is only supported on Tomcat or WebLogic application servers.

The deployment of the CEF SMP on both platforms is almost identical but minor platform specific changes will be documented in a dedicated section of this manual.

The deployment of the CEF SMP are summarized in the following mandatory steps:

- Database Configuration
- Application Server Preparation
- SMP Initial Configuration
- SMP .WAR file Deployment

*Remark:*

*The environment variable, **cef\_edelivery\_path**, refers to the name of the folder where the SMP package is installed.*

*For Tomcat, it refers to **CATALINA\_HOME**.*

*For Oracle WebLogic, it refers to **DOMAIN\_HOME**.*

## 5. DATABASE CREATION

This section describes the steps necessary to create the database, tables and the SMP database user (**dbuser** used for database connection purpose).

It also includes the creation of an initial SMP user account that will be used by REST clients to connect to the SMP.

The SMP uses a direct connection to the database, which removes the need to configure a data source within WebLogic.

For this step you need to use the script included in the zip file downloaded in section §3.3.

### 5.1. MySQL

1. Download and copy the `mysql5innoDB-4.x.ddl` script to `cef_edelivery_path/sql-scripts`
2. Open a command prompt and navigate to the `cef_edelivery_path/sql-scripts` folder
3. Execute the following MySQL commands:

```
mysql -h localhost -u root_user --password=root_password -e "drop schema if
exists smp_schema;create schema smp_schema;alter database smp_schema
charset=utf8; create user smp_dbuser@localhost identified by
'smp_password';grant all on smp_schema.* to smp_dbuser@localhost;"
```

This creates an `smp_schema` and an `smp_dbuser` with (all) privileges to the `smp_schema`.

Execute the following command to create the required objects (tables, etc.) in the database:

```
mysql -h localhost -u root_user -p root_password smp_schema < mysql5innoDB-4.x.ddl
```

### 5.2. Oracle Database

1. Download and copy the [oracle10g-4.x.ddl](#) script to `cef_edelivery_path/sql-scripts`
2. Navigate to `cef_edelivery_path/sql-scripts` directory
3. Execute the following commands :

```
sqlplus sys as sysdba (password should be the one assigned during the Oracle
installation )
=====
Once logged in Oracle:
create user smp_dbuser identified by smp_dbpassword;
grant all privileges to smp_dbuser;
connect smp_dbuser
show user; (should return : smp_dbuser)
```

```
@oracle10g-4.x.ddl (run the scripts with the @ sign from the location of the scripts)
```

```
exit
```

```
=====
```

## 6. ORACLE WEBLOGIC CONFIGURATION

This section does not include the installation of a WebLogic application server. It is assumed that the WebLogic Server is installed and a WebLogic domain is created with an administration server and a managed server on which the CEF SMP will be deployed.

Hereafter the domain location will be referred as *DOMAIN\_HOME* (user-defined name).

In the examples below, we will use the following Domain and Server names:

- Domain Name : SMPDOMAIN
- Administration Server : AdminServer
- SMP Managed Server : SMP\_ManagedServer

As shown below:

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled "Summary of Servers" and contains a table of servers. The table has the following data:

Name	Type	Cluster	Machine	State	Health	Listen Port
AdminServer(admin)	Configured			RUNNING	OK	7001
SMP_ManagedServer	Configured			RUNNING	OK	7003

In order to deploy the SMP on the WebLogic Application Server platform, two preliminary steps need to be completed:

- Disabling the Authentication on the Weblogic Server,
- Configuring the Extra CLASSPATH for WebLogic

This is described in the following 2 sections.

## 6.1. Disabling the Authentication on the WebLogic

The CEF SMP has its own authentication mechanism that makes the WebLogic authentication redundant. It is therefore important to disable the WebLogic Authentication to stop it from interfering with the SMP authentication.

To do so, edit the config.xml file (under SMPDOMAIN/config) by adding the following tag before the `</security-configuration>` closing tag:

```
<enforce-valid-basic-auth-credentials>>false</enforce-valid-basic-auth-credentials>
```

Here is an example:

```
../  
<enforce-valid-basic-auth-credentials>>false</enforce-valid-basic-auth-  
credentials>  
</security-configuration>  
/..
```

## 6.2. Configuring the Extra CLASSPATH for WebLogic

Under the DOMAIN\_HOME directory, create the following sub-directories:

- conf
- temp
- logs

Edit the WebLogic DOMAIN\_HOME/bin/setDomainEnv.sh.

### For Linux:

Add the `EXPORT CLASSPATH=${CLASSPATH}:${DOMAIN_HOME}/smp/conf` statement at the end of the CLASSPATH definition as shown below:

```
../  
if [ "${PRE_CLASSPATH}" != "" ] ; then  
    CLASSPATH="${PRE_CLASSPATH}${CLASSPATHSEP}${CLASSPATH}"  
    export CLASSPATH  
fi  
  
    CLASSPATH=${CLASSPATH}:${DOMAIN_HOME}/conf  
    export CLASSPATH  
/..
```

### For Windows:

```
../  
If NOT "%PRE_CLASSPATH%"==" " (  
    set CLASSPATH=%PRE_CLASSPATH%;%CLASSPATH%  
)  
set CLASSPATH=%CLASSPATH%;%DOMAIN_HOME%\conf  
/..
```

## 7. TOMCAT CONFIGURATION

In order to deploy the SMP on Tomcat, the steps below need to be completed.

### 7.1. Configuring the Extra CLASSPATH for Tomcat

In this Tomcat example, a directory called **cef\_edelivery\_path** will be created in the root path of the Tomcat installation (**CATALINA\_HOME**) and the **CLASSPATH** modified to include this new directory using an existing Tomcat batch file (**CATALINA\_HOME/bin/setenv.[sh|bat]**).

Create a **cef\_edelivery\_path** directory in the **CATALINA\_HOME** directory.

Within the **cef\_edelivery\_path/** directory, create new directories:

- conf
- keystores

#### For Linux:

Edit the **CATALINA\_HOME/bin/setenv.sh** file

```
#!/bin/sh
# Set CLASSPATH to include $CATALINA_HOME/cef_edelivery_path/conf
# where the smp 'smp.config.properties' is located
export CATALINA_HOME=cef_edelivery_path
export JAVA_OPTS="$JAVA_OPTS -Dsmp.config.properties=$CATALINA_HOME/conf"
export CLASSPATH=$CATALINA_HOME/conf
```

#### For Windows:

Edit the **%CATALINA\_HOME%/bin/setenv.bat** file

```
REM Set CLASSPATH to include $CATALINA_HOME/cef_edelivery_path/conf
REM where the 'smp.config.properties' is located
set CATALINA_HOME=cef_edelivery_path\cef_edelivery_path
set JAVA_OPTS=%JAVA_OPTS% -Dsmp.config.properties=%CATALINA_HOME%\conf
set classpath=%classpath%;%catalina_home%\conf
```



## 7.2. JDBC Driver

The JDBC driver needs to be downloaded from the manufacturer website:

- For Oracle Database : <http://www.oracle.com/technetwork/apps-tech/jdbc-112010-090769.html>
- For Mysql : <https://www.mysql.com/products/connector/>

The JDBC driver (.jar file) must be copied to the following directory: `cef_edelivery_path/lib`.

## 8. SMP CONFIGURATION

Since **SMP 4.1.0.FR**, configuration properties (except database connection configuration) are stored in the Database **SMP\_CONFIGURATION** table. In order to make the migration easier for existing deployments, the initial database configuration is imported from the existing smp configuration file. Therefore, for a new installation, the initial procedure stays the same.

For this step, use the following resources delivered within the zip file downloaded in section §3.3:

- An smp config file named **smp.config.properties** located in the CLASSPATH
- A keystore file called **sample\_signatures\_keystore.jks** used for XMLDSIG

The **smp.config.properties** file must be copied to the **cef\_edelivery/conf/** folder and referenced by the **CLASSPATH** variable, as explained in the next section.

The **sample\_signatures\_keystore.jks** file must be copied to the **cef\_edelivery/conf/** folder created during the Server preparation phase (see §7.1).

### 8.1. Database configuration

The CEF SMP database back-end configuration is performed within the CEF SMP configuration file (**smp.config.properties** file).

Depending on the selected database back-end, modify the **smp.config.properties** files as indicated below.

#### 8.1.1. Oracle Database:

```
../  
## Sample for Oracle  
#jdbc.driver = oracle.jdbc.driver.OracleDriver  
target-database=Oracle  
jdbc.url=jdbc:oracle:thin:@localhost:1521/xe  
jdbc.user=smp  
jdbc.password=secret123  
..
```

#### 8.1.2. MySQL:

```
../  
## Path pointing to the keystore file with keys used for signing GET  
ServiceMetadata responses.  
## Keystore must keep exactly 1 key if single-domain setup is used
```

```
## For more than 1 domain setup, aliases of each key have to be configured
in SMP_DOMAIN table

## Keystore password must be equal for every key within this keystore
xmldsig.keystore.classpath=/keystores/sample_signatures_keystore.jks
xmldsig.keystore.password=secure123

## Database access
target-database = MySQL
jdbc.driver = com.mysql.jdbc.Driver
jdbc.url = jdbc:mysql://localhost:3306/smp
jdbc.user =smp
jdbc.password=secret123
```

## 8.2. SMP Keystore

From SMP 4.1.0. FR on, the eDelivery SMP application uses only one keystore with the following default name: smp-keystore.jks. Keystore is automatically created by eDelivery SMP 4.1.0.FR. Initialization is triggered at start-up of the eDelivery SMP when the database *SMP\_CONFIGURATION* table is empty. Managing keystore (adding/deleting entries) on SMP 4.1.0. FR is done by the eDelivery SMP Admin console on the Domain page with the SYSTEM\_ADMIN role (see also §17).

Before SMP 4.1.0.FR, the eDelivery SMP used two distinct keystores for different purposes:

- One **mandatory** keystore is used for signing the responses to **GET** requests (XMLDSIG response signing);
- One **optional** (SML) keystore is used to authenticate SMP using 2-way-SSL when it is calling SML via HTTPS.

For migration purposes, please follow the description of deprecated/obsolete keystores described in the next sections.

### 8.2.1. XMLDSIG response signing Keystore (DEPRECATED since 4.1.0.FR)

This keystore contains keys for signing the SMP responses. A keystore with at least one entry is required.

A sample keystore is included in the zip file downloaded in section §3.3.

Details of the sample keystore:

- *xmldsig.keystore.classpath*: `/{path}/sample_signatures_keystore.jks`
- *xmldsig.keystore.password*: `secure123`.

*Remark:*

The value of the `xmlldsig.keystore.password` (=secure123) also acts as the password for the `SML_CLIENT_KEY_ALIAS` field in the `smp_domain` table described later.

This keystore must be copied to the `smp` or any other folder in the SMP server, and then configured in the `smp.config.properties` file as shown in the following example:

```
../
## XMLDSIG response signing:
xmlldsig.keystore.classpath    =cef_edelivery_path/sample_signature_keys.jks
xmlldsig.keystore.password     =secure123
/..
```

### 8.2.2. SML Keystore (DEPRECATED since 4.1.0.FR)

The SML keystore is **optional** and only needs to be deployed and configured if the SMP will be accessing an SML using HTTPS.

The SML keystore should be deployed in a server location and then configured in the `smp.config.properties`, using a relative or an absolute location.

```
../
# BDMSL URL
bdmsl.integration.url=http://localhost:8080/manageparticipantidentifier

## Keystore JKS file path (optional). Used for X509 client 2-way-SSL
authentication in SML integration
## If there is more than one domain configured, alias of each key must be set up
in SMP_DOMAIN table
## Password must be equal for every key within the keystore and for keystore
itself
bdmsl.integration.keystore.path=
bdmsl.integration.keystore.password=
```

### 8.2.3. Initializing and merging new keystore.

The initial deployment of the eDelivery SMP 4.1,0 FR version automatically creates a new keystore with the following filename:

- `smp-keystore.jks`.

The keystore is created in the folder where the existing keystore, `xmlldsig.keystore.classpath`, is located.

A random keystore password and symmetric encryption key (AES 256) are also generated.

The Symmetric encryption key is stored in a file named:

- `encryptionPrivateKey.private`

The Symetric key is used to encrypt the keystore password, which is then stored in the corresponding database field property:

- **smp.keystore.password** ( example value: 7css/uqZRFBeiKavrzzB1A==)

The Decrypted password is also stored in the database. The Decrypted value is not used by the application. You need to store the password in a safe location and remove it from the database.

- **smp.keystore.password.decrypted**

The Application will import the keys and certificate from the existing keystores. First from **xmlsig.keystore.classpath** and then, if it exists, from **bdmsl.integration.keystore.path**, keeping the same aliases for keys used in the old keystore. If the aliases are the same in both keystores, then the aliases from sml keystore are appended with a 3-digit number (starting at 001).

Example:

If the duplicate alias is *myBestCertificate*, then the second imported certificate will have alias: *myBestCertificate\_001*.

If the migration fails, the migration/initialization can be relaunched after clearing the **SMP\_CONFIGURATION** table.

Example:

```
SQL> DELETE FROM SMP_CONFIGURATION;
```

After a successful migration, the old keystores can be backed up and then removed from the property file.

## 9. SMP .WAR FILE DEPLOYMENT

The CEF SMP is deployed using the steps described in the next sections.

### 9.1.1. Tomcat

Copy the `cef_edelivery/temp/smp-4.X.war` file to the Tomcat **webapps** directory (`cef_edelivery/webapps`).

### 9.1.2. Oracle WebLogic

Deploy the **.war** file within WebLogic using the Oracle Weblogic deployer feature or using the Weblogic Administration Console.

An example of using the Oracle the **weblogic.deployer**, is shown below:

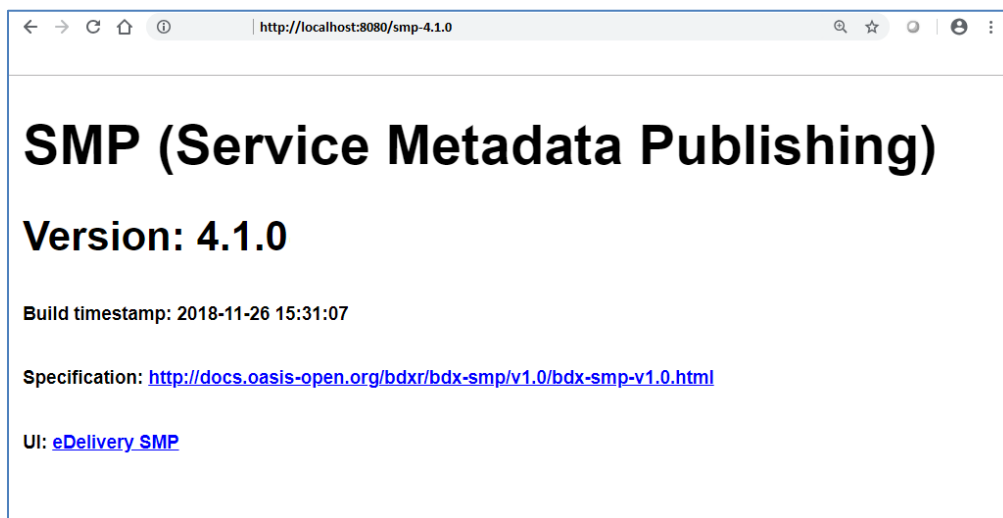
```
java weblogic.Deployer -adminurl
t3://${WebLogicAdminServerListenAddress}:${WebLogicAdminServerPort} \
-username ${WebLogicAdminUserName} \
-password ${WebLogicAdminUserPassword} \
-deploy -name smp-4.X.war \
-targets ${SMP_ManagedServer} \
-source $TEMP_DIR/ smp-4.X.war
```

### 9.1.3. Verification of the Installation

Verify the installation by navigating with your browser to the following address:

**`http://[hostname]:[port]/smp-4.X`**

If the deployment is successful, the following page is displayed:



Important: Context path (example above: `/smp-4.1.0`) should be the same as is deployment WAR file. If the war file is called **smp.war** then the URL will be **`http://[hostname]:[port]/smp`**.



## 10. CONFIGURING THE CEF SMP FOR USE WITH AN SML

The SMP can be registered in an SML, using two identification mechanisms:

- Using HTTP and plain text with metadata embedded into the header of the REST request,
- Using HTTPS/TLS and a keystore containing a certificate.

### 10.1. Configuring the BDMSL Integration

The first step is to configure the SMP so that it can be used with an SML.

This is achieved by setting the database property: **bdmsl.integration.enabled** parameter to **true**, default is **false**.

```
Execute the following sql command for Oracle database:UPDATE
SMP_CONFIGURATION SET VALUE='true', LAST_UPDATED_ON=systemdate WHERE
PROPERTY='bdmsl.integration.enabled';
```

### 10.2. Configuring the SML URL

The configuration of the SML URL endpoint is achieved by configuring the **bdmsl.integration.url** property in the **smp.config.property** file as follows:

```
UPDATE SMP_CONFIGURATION SET VALUE= http://localhost:8080/edelivery-sml/,
LAST_UPDATED_ON=systemdate WHERE PROPERTY= bdmsl.integration.url';
```

### 10.3. SMP authentication to an SML

Once registered in an SML, the SMP needs to authenticate against the SML during normal operations. For authentication, the client key/certificate must be installed in the keystore and an alias defined for the domain. The configuration is either done using the eDelivery SMP Admin console (see also §17) or by entering the values directly into the database.

SML supports two ways of authentication

- BlueCoat: HTTP client certificate header. This is used behind a bluecoat reverse proxy.
- HTTPS/TLS: Standard mutual TLS authentication.

#### 10.3.1. Plain Text HTTP

**SML\_CLIENT\_CERT\_HEADER** contains the SMP certificate needed if accessing SML directly through HTTP. The configured "Client-Cert" HTTP header will be added to each SML request bypassing SSL certificate verification made normally by SSL terminators.



**SML\_CLIENT\_CERT\_HEADER** is the configuration attribute (column) in the **SMP\_DOMAIN** table described in section §16.3.

### **10.3.2. HTTPS/TLS**

When using HTTPS/TLS, as mentioned in the **bdmsl.integration.url** covered earlier, all information related to the Keystore containing the SMP certificate must be configured under the SMP Keystore and the corresponding certificate alias must be set in column **SML\_CLIENT\_KEY\_ALIAS** in the **SMP\_DOMAIN** table described in section §16.3.

## 11. SMP USER MANAGEMENT

Only **Admin SMP** and Admin **ServiceGroup** users, who connect to the CEF SMP, need to be created in the SMP database.

Anonymous users or public users can access the SMP to retrieve only. They are not registered and therefore not added to the database.

There are no restrictions on the number of users that can be created to access the CEF eDelivery SMP.

The (MYSQL or ORACLE) Database script provided creates an **smp\_admin** user with password=**changeit**, by default. This password must be immediately changed for the purpose of using the **SMP in Acceptance or Production**.

### 11.1. User Roles

The CEF SMP users can be of three types, as briefly described below:

Actor	UC	Short description	Oper.	Data
Admin SMP	Create or Update Service Group	Create a new ServiceGroup for a new receiver participant. This service stores the Service Group and links it to the specified duplet participantIdentifier + participantIdentifierScheme. Information is stored into ServiceGroup table. This same service is used to create and update a ServiceGroup.	PUT	ServiceGroup
Admin SMP	Erase Service Group	Erases the service group definition AND the list of services for the specified receiver participant.	DELETE	ServiceGroup
Admin Service Group	Create or Update Service Metadata	Publish detailed information about one specific document service (multiple processes and endpoints). This same service is used to create and update ServiceMetaData.	PUT	ServiceMetadata
Admin Service Group	Erase Service Metadata	Remove all information about one specific service (i.e. all related processes and endpoints definitions).	DELETE	ServiceMetadata
User	Retrieve Service Group	Obtain the list of services provided by a specific receiver participant (collection of references to the ServiceMetaData's). This service provides the information related to the Service Group according to the input duplet participantIdentifier + participantIdentifierScheme. Returns information	GET	ServiceGroup

Actor	UC	Short description	Oper.	Data
		from the ServiceMetadata table only (references to actual MetaData).		
User	Retrieve Service Metadata	Obtain detailed definition about one specific service of a specific participant for all supported transports. This service retrieves the SignedServiceMetadata according to the input quadruplet participantIdentifier+participantIdentifierScheme+documentIdentifier+documentIdentifierScheme. Returns information from the Endpoint table.	GET	SignedServiceMetadata
System admin		Create, modify and delete users and domains. System admin can be only used in the edelivery SMP UI.		

**Note:** For a complete description of the SMP user management, please consult the SMP Interface Control Document (ICD) document available at <https://ec.europa.eu/cefdigital/wiki/x/OwvNAG>.

Users can be added, modified and deleted using the SMP Admin console or directly by executing sql commands. Below are instructions on how to modify users in the database.

## 11.2. BCrypt password generation

The SMP v4.X uses the BCrypt algorithm to hash users' passwords. A BCrypt-hashing tool is bundled into the SMP WAR file. To get the hashing code, follow the steps below.

Place a copy of the **smp-4.X.war** file into a temporary directory of your choice.

Extract the war file using the **jar** command:

```
jar -xvf smp-4.X.war
```

Obtain one or multiple hashes at once, using the following command:

```
java -cp "WEB-INF/lib/*"
eu.europa.ec.edelivery.smp.utils.BCryptPasswordHash password_to_be_hashed
```

The result will be a BCrypt hash of the specified password (listed below in *italic*):

```
java -cp "WEB-INF/lib/*"
eu.europa.ec.edelivery.smp.utils.BCryptPasswordHash password_to_be_hashed
$2a$10$6nYTSUSH2BQfbOLiYcXn8eUViBcnn.WcjUrW0tJLMND0dAtI85zMa
```

The next command shows the hashing of several passwords at once, separated by a space in the command.

```
java -cp "WEB-INF/lib/*" eu.europa.ec.edelivery.smp.BCryptPasswordHash
password_to_be_hashed_1 password_to_be_hashed_2
$2a$10$6nYTSUSH2BQfbOLiYcXn8eUViBcnn.WcjUrWotJLMNDodAtI85zMa
$2a$107zNzSeZpxiHeqY2BRKkHE.HknfIe3aiu6XzU.qHHnnPbUHktfcmDG
```

### 11.3. SMP Database User Creation

Adding an SMP user is done by adding a new entry in the SMP database **SMP\_USER** table either directly or via the Administration console.

The User role is set in the SMP\_USER table ROLE column as follows:

User Role	Role value
Admin SMP	SMP_ADMIN
Admin Service Group	SERVICE_GROUP_ADMIN
System Administrator	SYSTEM_ADMIN
AnonymousUser (Not defined in the SMP User database)	N/A

In the following two examples, an **Admin SMP** and an **Admin ServiceGroup** users are created.

#### 11.3.1. SYSTEM ADMIN SMP User creation

**Remark:**

- In order to logon on the Administration Console **for the first time**, it is necessary to, first create a user with **SYSTEM\_ADMIN** privileges by entering the details directly into the **SMP\_USER** table. This initial user's password is generated using the **BCRYPT** utility described previously.
- *If **PASSWORD\_CHANGED** is not set, the user will be asked to change the password at first logon.*

Example of a SYSTEM\_ADMIN user creation:

```
Username           : smp_admin
Password (Hashed)  : $2a$10$6nYTSUSH2BQfbOLiYcXn8eUViBcnn.WcjUrWotJIMNDodAtI85zMa
Role               : SYSTEM_ADMIN
```

Execute the following database command using the database user/password created in the Database Configuration section of this guide.

MySql example:

```
INSERT into SMP_USER (ID, USERNAME, PASSWORD, ROLE, ACTIVE,
CREATED_ON, LAST_UPDATED_ON, PASSWORD_CHANGED) values ((select max(next_val) from
SMP_USER_SEQ), 'smp_user',
```

```
'$2a$10$o1cGeWKGEoRia2DPuFqRNeca0IEdRSmOrljLz57BAjf1jLC9SohrS',
'SYSTEM_ADMIN',1,SYSDATE(), SYSDATE(),SYSDATE() );
update SMP_USER_SEQ set next_val=next_val+1;
```

Oracle example:

```
SQL> INSERT into SMP_USER (ID, USERNAME, PASSWORD, ROLE, ACTIVE,
CREATED_ON, LAST_UPDATED_ON) values (SMP_USER_SEQ.NEXTVAL, 'smp_user',
'$2a$10$o1cGeWKGEoRia2DPuFqRNeca0IEdRSmOrljLz57BAjf1jLC9SohrS',
'SYSTEM_ADMIN',1,SYSDATE, SYSDATE );
update SMP_USER_SEQ set next_val=next_val+1;
```

### 11.3.2. Admin SMP User Creation

Username : smp\_user1  
 Password (Hashed) : \$2a\$10\$6nYTSUSH2BQfbOLlyCXn8eUViBcnn.WcjUrWotJIMNDOdAtI85zMa  
 IsAdmin : SERVICE\_GROUP\_ADMIN

Example: Oracle database command.

```
SQL> insert into smp_user (ID, username, password, ROLE, ACTIVE,
CREATED_ON, LAST_UPDATED_ON) values (SMP_USER_SEQ.NEXTVAL, 'smp_user1',
'$2a$10$6nytsush2bqfboliycxn8euviBcnn.wcjurwotjlmndodati85zma',
'SMP_ADMIN',1,SYSDATE, SYSDATE);
```

### 11.3.3. Admin ServiceGroup User Creation

Username : smp\_user2  
 Password (Hashed) : \$2a\$10\$6nYTSUSH2BQfbOLlyCXn8eUViBcnn.WcjUrWotJIMNDOdAtI85zMa  
 IsAdmin : SERVICE\_GROUP\_ADMIN

Example: Oracle database command.

```
SQL> insert into smp_user (ID, username, password, ROLE, ACTIVE,
CREATED_ON, LAST_UPDATED_ON) values (SMP_USER_SEQ.NEXTVAL, 'smp_user1',
'$2a$10$6nytsush2bqfboliycxn8euviBcnn.wcjurwotjlmndodati85zma',
'SERVICE_GROUP_ADMIN',1,SYSDATE, SYSDATE);
```

## 12. LOGGING CONFIGURATION

### 12.1. Logging properties

The SMP logging properties are defined in the `./WEBINF/log4j.properties` file embedded in the SMP `.war` file.

It is possible to modify the configuration of the logs by editing the embedded **log4j properties**.

Name	Date modified	Type	Size
internal	20/04/2016 10:38	File folder	
keystores	25/04/2016 16:13	File folder	
plugins	20/04/2016 10:38	File folder	
policies	20/04/2016 10:38	File folder	
temp	27/04/2016 10:41	File folder	
work	20/04/2016 16:44	File folder	
domibus-configuration.xml	26/04/2016 10:11	XML File	5 KB
domibus-datasources.xml	20/04/2016 15:31	XML File	6 KB
domibus-plugins.xml	19/04/2016 10:26	XML File	2 KB
domibus-security.xml	19/04/2016 10:26	XML File	5 KB
domibus-transactions.xml	19/04/2016 10:26	XML File	4 KB
log4j.properties	19/04/2016 10:26	PROPERTIES File	2 KB
persistence.xml	19/04/2016 10:26	XML File	2 KB

In the example below, a **log4j.properties** file is shown:

```
# Direct log messages to stdout
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.Target=System.out
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%d{ABSOLUTE} %5p %c{1}:%L - %m%n

log4j.appender.file=org.apache.log4j.FileAppender
log4j.appender.file.file=${catalina.home}/logs/domibus.log
log4j.appender.file.layout=org.apache.log4j.PatternLayout
log4j.appender.file.layout.ConversionPattern=%d{ABSOLUTE} %5p %c{1}:%L - %m%n

log4j.appender.atomikos=org.apache.log4j.FileAppender
log4j.appender.atomikos.file=${catalina.home}/logs/atomikos.log
log4j.appender.atomikos.layout=org.apache.log4j.PatternLayout
log4j.appender.atomikos.layout.ConversionPattern=%d{ABSOLUTE} %5p %c{1}:%L - %m%n

# In order to enable logging of request/responses please change the loglevel to INFO
log4j.logger.org.apache.cxf=WARN
# Root logger option
log4j.rootLogger=INFO, file, stdout

log4j.logger.com.atomikos=WARN, atomikos
```

In red: the parameters can be edited to modify the location of the log file, and the layout.

In **green**: the parameters can be edited to change the level of logging (3 levels defined: INFO, WARN, and ERROR).

## 13. SOAPUI TESTING

Soap UI can be used to create, update and delete Service Groups and Metadata.

An SMP SoapUI project contains sample requests and is included in the zip file already downloaded.

The procedure to create, update or delete a Service Group is described in the next steps.

### 13.1. Creation, update and deletion of Service Groups.

#### 13.1.1. Create a Service Group

In the left navigation pane of the SoapUI interface, browse to the REST PUT method as shown below:

The screenshot displays the SoapUI 5.4.0 interface. The left-hand 'Navigator' pane shows a project tree with 'SMP Samples' expanded to 'SMP 4.0 Sample Requests', then 'ServiceGroup [/{ParticipantIdentifierScheme}:/ParticipantIdentifier]', and finally 'UC02 - PUT' selected. The main workspace shows the configuration for this REST PUT request. The 'Method' is set to 'PUT' and the 'Endpoint' is 'http://localhost:8080/smp'. The 'Resource' is '/{ParticipantIdentifierScheme}'. A table below lists parameters:

Name	Value	Style	Level
ParticipantIdentifierSch...	ehealth-participantid-qns	TEMPLATE	RESOURCE
ParticipantIdentifier	urn:poland:ncpb	TEMPLATE	RESOURCE

The 'Raw' tab is active, showing the following XML payload:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<ServiceGroup xmlns="http://docs.oasis-open.org/bdxx/ns/SMP/2016/05">
  <ParticipantIdentifier scheme="{=request.getProperty('ParticipantIdentifier')}" />
  <ServiceMetadataReferenceCollection />
</ServiceGroup>
```

At the bottom, the 'Request Properties' tab is visible, showing details like Name (simple request), Description, Encoding (UTF-8), Endpoint (http://localhost:8080/smp), and Username (smp\_admin).

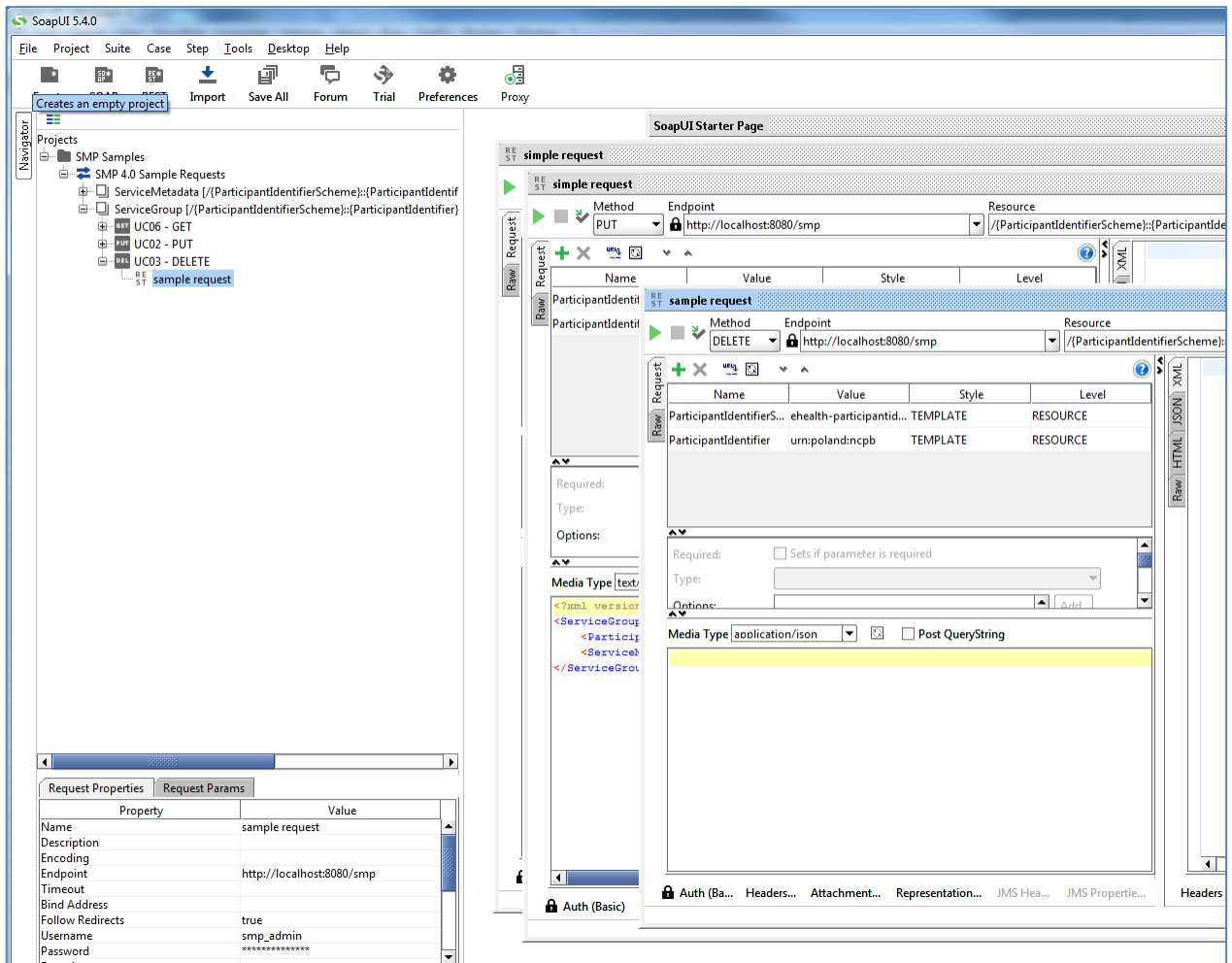
#### 13.1.2. Update a Service Group

The REST method to update the **ServiceGroup** is the same as the one used for creating **ServiceGroup** described in the previous section.



### 13.1.3. *Delete a ServiceGroup*

On the SoapUI interface on the left navigation panel, browse to the REST DELETE method as indicated below:



## 13.2. Creation, update and deletion of Service Metadata.

### 13.2.1. *Create a Service Metadata*

In the left navigation pane of the SoapUI interface, browse to the REST PUT method as shown below:

The screenshot shows the SoapUI 5.4.0 interface. The main window displays a REST client configuration for a PUT request. The endpoint is `http://localhost:8080/smp` and the resource is `/ParticipantIdentifierScheme`. The request body is an XML document representing Service Metadata.

Name	Value	Style	Level
ParticipantIdentifierScheme	ehealth-participantid-qns	TEMPLATE	RESOURCE
ParticipantIdentifier	urn:poland:ncpb	TEMPLATE	RESOURCE
DocTypeIdentifierScheme	ehealth-docid-qns	TEMPLATE	RESOURCE
DocTypeIdentifier	urn:epsos##services:ext...	TEMPLATE	RESOURCE

The XML body is as follows:

```
<ServiceMetadata xmlns="http://docs.oasis-open.org/bdxc/ns/SMP/2016/05">
  <ServiceInformation>
    <ParticipantIdentifier scheme="{=request.getProperty('ParticipantIdentifierScheme')}">urn:poland:ncpb</ParticipantIdentifier>
    <DocumentIdentifier scheme="{=request.getProperty('DocTypeIdentifierScheme')}">urn:epsos##services:ext...</DocumentIdentifier>
    <ProcessList>
      <Process>
        <ProcessIdentifier scheme="cenbii-procid-ubl">urn:www.cenbii.eu:ubl:1:1:1</ProcessIdentifier>
      </Process>
    </ProcessList>
    <ServiceEndpointList>
      <Endpoint transportProfile="busdox-transport-start">
        <EndpointURI>https://poland.pl/theService</EndpointURI>
        <RequireBusinessLevelSignature>true</RequireBusinessLevelSignature>
        <ServiceActivationDate>2003-01-01T00:00:00</ServiceActivationDate>
        <ServiceExpirationDate>2020-05-01T00:00:00</ServiceExpirationDate>
        <Certificate>MIICUTCCAbggAwIBAgIEW0KxxzANBgkqhkiG9w0BAQ0F...</Certificate>
        <ServiceDescription>Sample description of invoicing se...</ServiceDescription>
        <TechnicalContactUrl>https://example.com/TechnicalContact</TechnicalContactUrl>
      </Endpoint>
    </ServiceEndpointList>
  </ServiceInformation>
</ServiceMetadata>
```

The 'Request Properties' tab shows the following configuration:

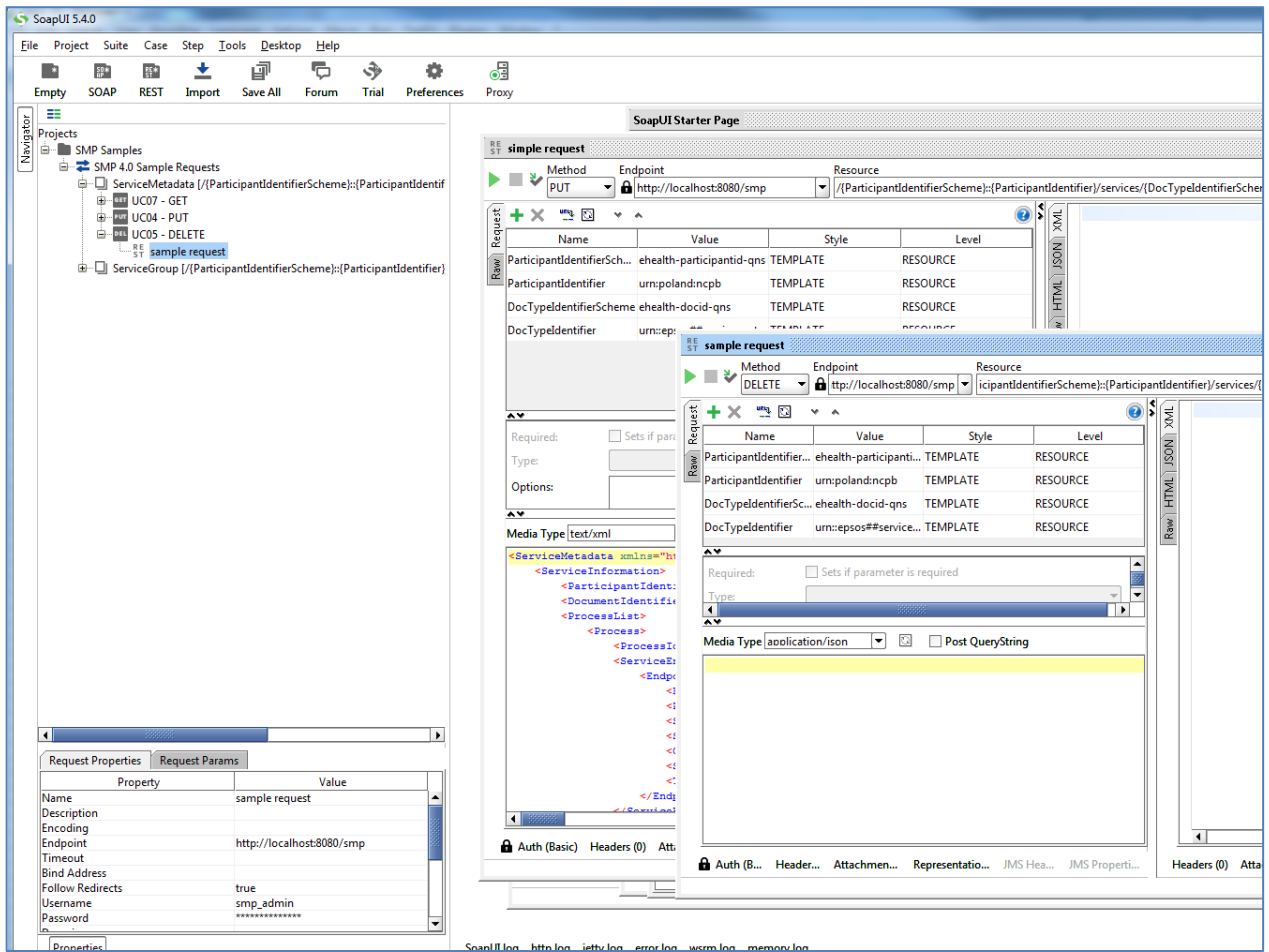
Property	Value
Name	simple request
Description	
Encoding	UTF-8
Endpoint	http://localhost:8080/smp
Timeout	
Bind Address	
Follow Redirects	true
Username	smp_admin
Password	*****

### 13.2.2. Update Service Metadata

The REST method to update **ServiceMetadata** is the same as the one use for creating **ServiceMetadata** as described in the previous section.

### 13.2.3. Delete Service Metadata

In the left navigation pane of the SoapUI interface, browse to the **REST DELETE** method as indicated below:



## 14. THE SWAGGERUI INTERFACE

### 14.1. Introduction

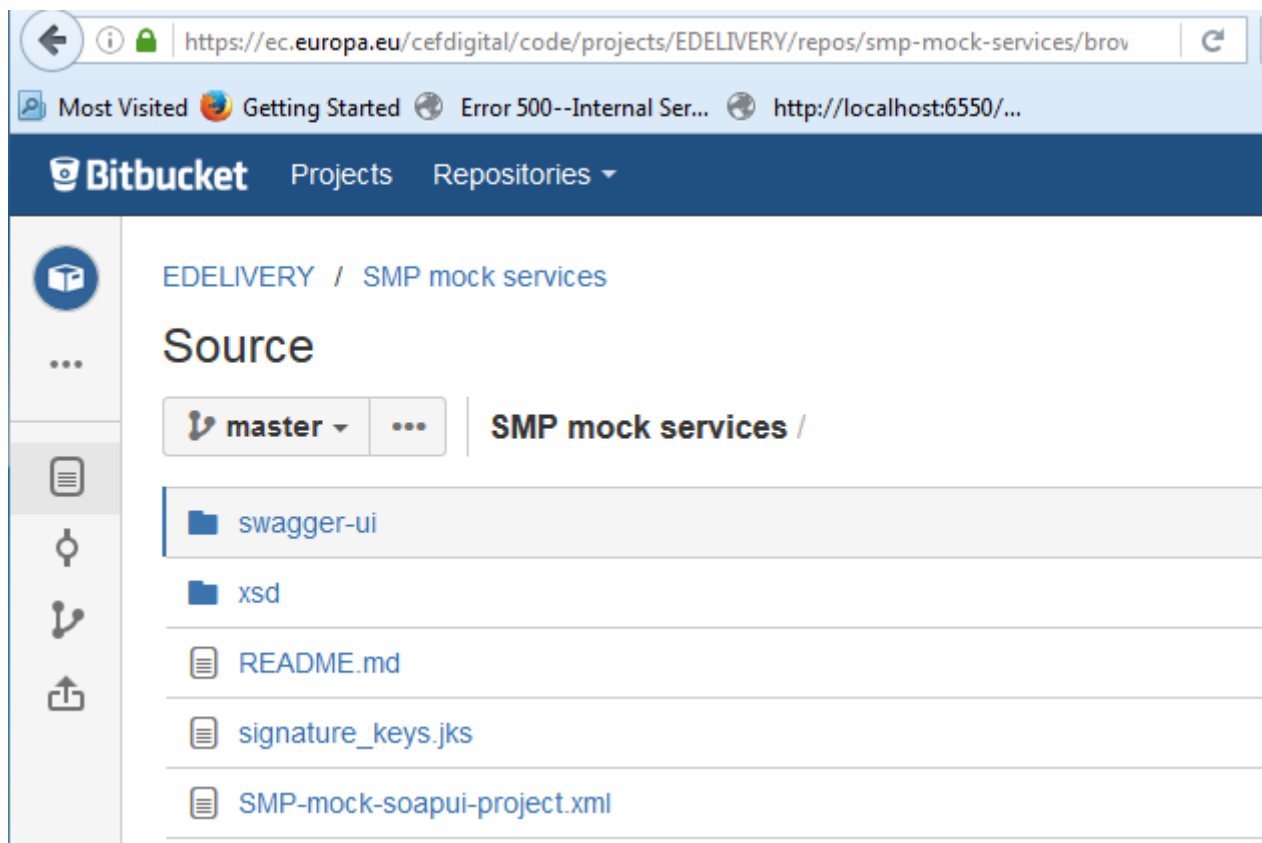
"Swagger is an API developer tools for the OpenAPI Specification (OAS). It allows anyone (developers or end-users) to interact with the API's resources"<sup>2</sup>.

The SMP Web Client can be tested at: <http://130.206.118.4/smp-swagger-ui> and, as explained, is a WEB client configured to shoot (PUT, GET or DELETE) at the mocked SMP implementation Metadata.

### 14.2. Downloading the CEF SMP SwaggerUI web application project

The CEF SMP SwaggerUI web application project can be freely downloaded from the following location:

<https://ec.europa.eu/cefdigital/code/projects/EDELIVERY/repos/smp-mock-services/browse>



Create a new **swagger\_temp** temporary directory.

Within the previously created **swagger\_temp** directory, execute the following command:

---

<sup>2</sup> Quote from: <http://swagger.io/>.

```
git clone https://ec.europa.eu/cefdigital/code/scm/edelivery/smp-mock-
services.git
Cloning into 'smp-mock-services'...
remote: Counting objects: 133, done.
remote: Compressing objects: 100% (130/130), done.
remote: Total 133 (delta 50), reused 0 (delta 0)
Receiving objects: 100% (133/133), 823.54 KiB | 0 bytes/s, done.
Resolving deltas: 100% (50/50), Done.
```

The SMP **SwaggerUI** project is downloaded and saved the **smp-mock-services** directory:

```
ls
smp-mock-services
```

### 14.3. Configuring the SMP SwaggerUI

Navigate to the **swagger-ui** directory located under the **smp-mock-services** directory.

The contents is listed below:

```
ls
css  fonts  images  index.html  lib  smp.json  swagger-ui.js
```

Edit the **smp.json** file and modify it to target your SMP:

**Replace:**

```
{
  "swagger": "2.0",
  "info": {
    "description": "This WEB client is configured to shoot at the [mocked SMP
implementation](http://smp-digit-
mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu/ehealth-actorid-
qns%3A%3Aurn%3Apoland%3Ancpb). After a few improvements (both on client and
server side) it might be used also for shooting at TEST / PROD environments. You
can find out more about Swagger at [http://swagger.io](http://swagger.io)",
    "version": "1.0.0",
    "title": "SMP 3.X WEB client (based on Swagger-UI)"
  },
  "host": "smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu",
  "basePath": "/",
  "externalDocs": {
    "description": "Find out more about SMP 3.X mock services",
```

With:

```
"url": "https://ec.europa.eu/cefdigital/code/projects/EDELIVERY/repos/smp-
mock-services"
{
  "swagger": "2.0",
  "info": {
    "description": "This WEB client is configured to shoot at
[http://localhost:7003/ smp-4.X](http://localhost:7003/ smp-4.X). After a few
improvements (both on client and server side) it might be used also for shooting
at TEST / PROD environments. You can find out more about Swagger at
[http://swagger.io](http://swagger.io)",
    "version": "1.0.0",
    "title": "SMP 4.X WEB client (based on Swagger-UI)"
  },
  "host": "localhost:7003",
  "basePath": "/ smp-4.X",
  "externalDocs": {
  },
}
```

## 14.4. Generating the Web Application Archive (.war file)

To generate the CEF SMP SwaggerUI Web Application archive (.war file), just create a zip file of the content of the swagger-ui directory and rename it as **swagger.war**.

This can be performed using any **zip** utility (**winzip** on Windows or **zip** on Linux).

Example on Linux:

```
zip -r swagger.war swagger-ui/*
```

## 14.5. Deploy the SMP SwaggerUI war file

### 14.5.1. On Tomcat

Copy the **swagger.war** file to *cef\_edelivery\_path* /webapps.

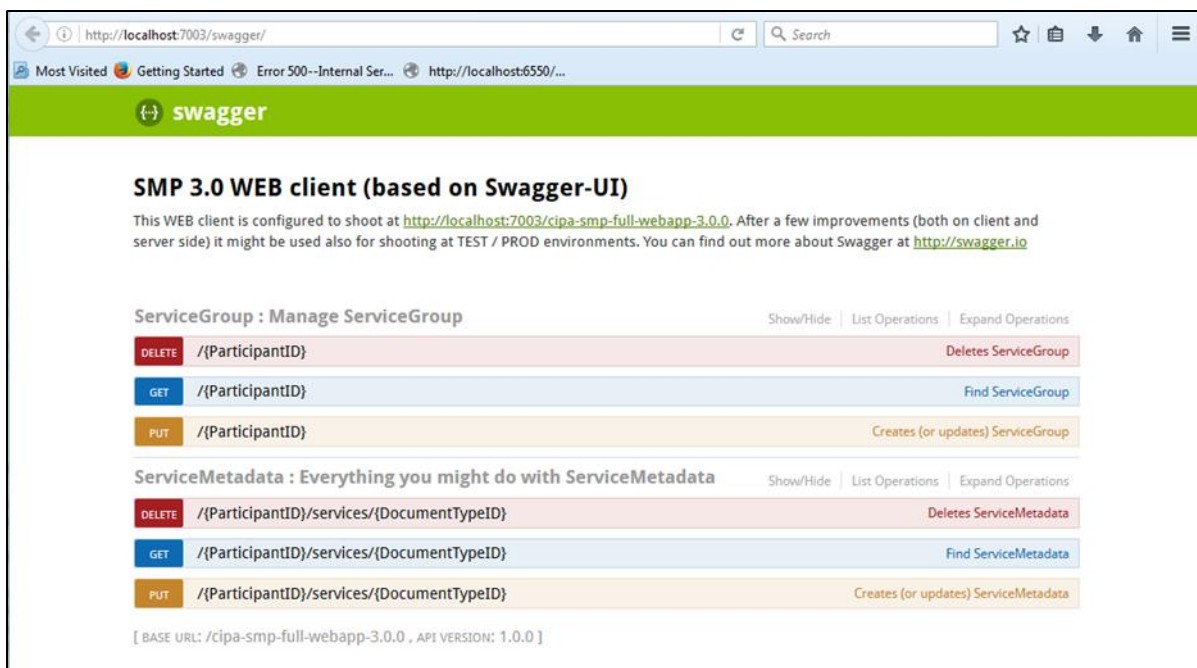
### 14.5.2. On WebLogic:

Deploy the .war file within WebLogic:

```
java weblogic.Deployer -adminurl
t3://${WebLogicAdminServerListenAddress}:${WebLogicAdminServerPort} \
-username ${WebLogicAdminUserName} \
-password ${WebLogicAdminUserPassword} \
-deploy -name swagger.war \
-targets ${SMP_ManagedServer} \
```

After starting the application, connect to <http://localhost:7003/swagger>.

A successful deployment should display the following page:



## 15. SMP COMPILATION

### 15.1. Compilation prerequisites

#### 15.1.1. Supported Operating System Platform

The CEF SMP can be built on the following OS platforms:

- Windows Workstation & Server
- Linux platform

#### 15.1.2. Software Requirements

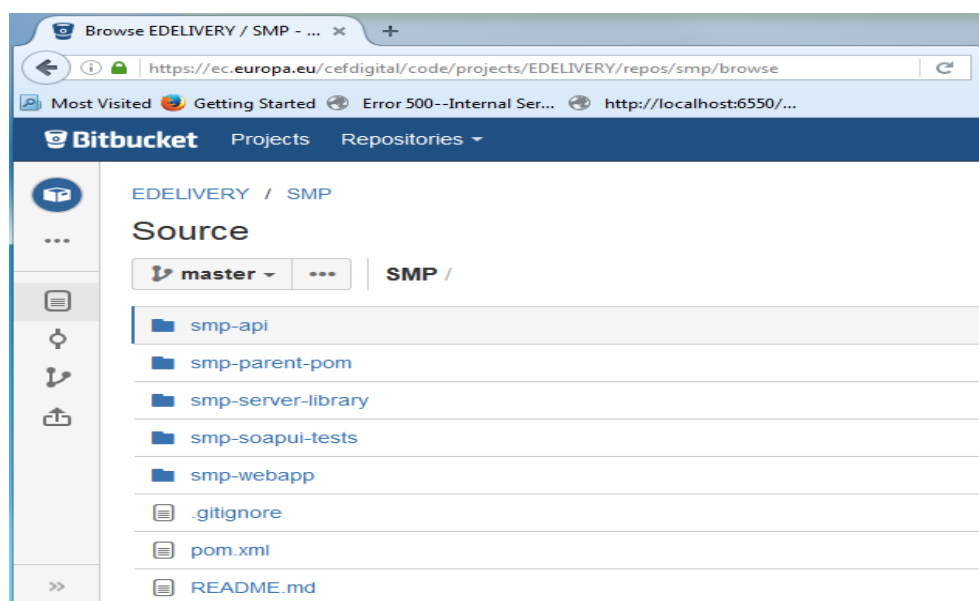
The following software components on the target system:

- Java Development Kit environment (JDK), version 7 or 8:  
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>
- Maven 3.0 and above (<https://maven.apache.org/download.cgi>)
- GIT (optional: Git is only used to download the project sources but these sources can be downloaded from any system having Git installed and then just copied manually on the compilation platform).

### 15.2. Downloading the source code

The source code of SMP is freely available and can be downloaded from the following location:

<https://ec.europa.eu/cefdigital/code/scm/edelivery/smp.git>





## 15.3. Compilation

Create a new **comp\_dir** temporary directory.

Within the previously created **comp\_dir** directory, execute the following command:

```
git clone https://ec.europa.eu/cefdigital/code/scm/edelivery/smp.git
Cloning into 'smp'...
remote: Counting objects: 52788, done.
remote: Compressing objects: 100% (15640/15640), done.
remote: Total 52788 (delta 25293), reused 47993 (delta 23387)
Receiving objects: 100% (52788/52788), 637.14 MiB | 2.06 MiB/s, done.
Resolving deltas: 100% (25293/25293), done.
```

Go to the newly created **smp** directory.

The directory contains the following:

```
ls
pom.xml  README.md  smp-api  smp-parent-pom  smp-server-library  smp-soapui-
tests  smp-webapp
```

Start the compilation by executing the following command:

```
mvn clean install -DskipTests
```

A successful compilation will result with the following:

```
mvn clean install -DskipTests
[INFO] Scanning for projects...
/..
../
[INFO] Installing /home/smpcomp/smp/smp/pom.xml to
/home/smpcomp/.m2/repository/eu/europa/ec/smp/3.X/smp-3.X.pom
[INFO] -----
[INFO] Reactor Summary:
[INFO]
[INFO] smp-parent-pom ..... SUCCESS [ 0.120 s]
[INFO] smp-angular ..... SUCCESS [132.375 s]
[INFO] smp-api ..... SUCCESS [ 32.375 s]
[INFO] smp-server-library ..... SUCCESS [02:01 min]
[INFO] smp-webapp ..... SUCCESS [ 23.314 s]
[INFO] SMP Builder POM ..... SUCCESS [ 2.222 s]
```

```
[INFO] -----  
[INFO] BUILD SUCCESS  
[INFO] -----  
[INFO] Total time: 03:00 min  
[INFO] Finished at: 2017-06-08T11:35:27+02:00  
[INFO] Final Memory: 61M/726M  
[INFO] -----
```

The resulting will be a Web application Archive (.war file) named **smp-4.X.war** located in the **smp-webapp/target/** directory:

```
ls ./smp-webapp/target  
smp-4.X  smp-4.X.war  classes  generated-sources  generated-test-sources  maven-  
status  test-classes  webapp-classes
```

## 16. SMP CONFIGURATION FILE AND TABLE

### 16.1. Multitenancy and Multidomain Support

The SMP is able to support multiple certificates in the same SMP. This is very useful in the Acceptance environment where multiple domains like ISA ITB, eHealth and others are hosted.

The SMP has the capability of keeping a relationship between a particular **Service Group** and its related **domain**.

As a result of this feature, the SMP Administration has the option, if need be, to define extra domains for newly created **Service Groups** meaning that the SMP is able to handle multiple domains environments.

**Remark:**

*In normal circumstances, when any one SMP is used for only one Domain, the domain used is then considered as the "domain by default" (or "default domain") for configuration purposes. The domain, in this case, does not need to be specified in the **Service Group** definitions or other configurations of the SMP as in previous versions of SMP.*

### 16.2. The smp.config.properties file

The CEF SMP configuration is performed via the **smp.config.properties** file.

This file is delivered by default embedded within the SMP war file.

```
#
# Copyright 2017 European Commission | CEF eDelivery
#
# Licensed under the EUPL, Version 1.2 or - as soon they will be approved
# by the European Commission - subsequent versions of the EUPL (the
# "Licence");
# You may not use this work except in compliance with the Licence.
#
# You may obtain a copy of the Licence attached in file: LICENCE-EUPL-
# v1.2.pdf
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the Licence is distributed on an "AS IS" basis,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the Licence for the specific language governing permissions and
# limitations under the Licence.
#
```

```
# Blue Coat reverse-proxy authentication, by default disabled (false)
# Be careful with switching it to 'true' - do it only if you know what you
# are doing.
# Authentication with Blue Coat means that all HTTP requests having
# 'Client-Cert' header will be authenticated
# as username placed in the header.
# Never expose SMP to the WEB without properly configured reverse-proxy
# and active blue coat.
authentication.blueCoat.enabled=false

## Only set to false in PRODUCTION mode. This variable is used to clear
## the context path of the SMP
contextPath.output=true

## Most Java libraries and J2EE containers block encoded slashes in URL -
## For security reasons.
## Theoretically there are no restrictions on slash "/" characters in
## document or participant identifiers,
## but by default we block them as well.
## If slash "/" characters must be supported, then switch this property to
## "true".
## Remember that in such case the relevant change should be also applied
## on J2EE level
## I.e. for Tomcat it is handled by property:
org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true
encodedSlashesAllowedInUrl=false

## Participant Identifier Schema of each PUT ServiceGroup request is
## validated against this schema
## I.e this regex: ^(?!^.{26})([a-z0-9]+-[a-z0-9]+-[a-z0-9]+)
## - limits length of scheme to 25 characters
## - forces pattern to consist of 3 alpha-numeric segments delimited with
## "-", i.e: aa1-bb2-cc3
## To turn validation OFF, set regex to "match all": .*
identifiersBehaviour.ParticipantIdentifierScheme.validationRegex=^(?!^.{26}
)([a-z0-9]+-[a-z0-9]+-[a-z0-9]+)

## All Identifiers by default are CASE-INSENSITIVE.
## Specifies schemes of participant/document identifiers that must be
## considered CASE-SENSITIVE.
## List values (delimited by pipe character: "|" ) placed here are checked
## against runtime (request) schemes in the CASE-INSENSITIVE way
```

```
identifiersBehaviour.caseSensitive.ParticipantIdentifierSchemes=casesensitive-participant-scheme1|casesensitive-participant-scheme2
identifiersBehaviour.caseSensitive.DocumentIdentifierSchemes=casesensitive-doc-scheme1|casesensitive-doc-scheme2

# Switches ON/OFF the BDXL client - integrationwith with SML
bdmsl.integration.enabled=false

# SML URL (incl. the service name)
#bdmsl.integration.url=https://sml.peppolcentral.org/manageparticipantidentifier
#
bdmsl.integration.url=https://smk.peppolcentral.org/manageparticipantidentifier
bdmsl.integration.url=http://localhost:8080/manageparticipantidentifier
bdmsl.integration.keystore.path=
bdmsl.integration.keystore.password=

bdmsl.integration.proxy.server=
bdmsl.integration.proxy.port=
bdmsl.integration.proxy.user=
bdmsl.integration.proxy.password=

## XMLDSIG response signing:
xmlsig.keystore.classpath = ../keystore/keystore.jks
xmlsig.keystore.password = peppol

## JDBC configuration for DB
jdbc.driver = oracle.jdbc.OracleDriver
jdbc.url =
jdbc:oracle:thin:@olrdev3.cc.cec.eu.int:1597/EX1UDIGD_TAF.cc.cec.eu.int
jdbc.user = CIPA_ADMIN
jdbc.password = the_password
target-database = Oracle
jdbc.read-connections.max = 10
```

### 16.2.1. Detailed SMP configuration properties

Attributes are stored in the database and the filesystem property file. If a property is located on both locations then the database property value takes precedence.

The following table describes them briefly:

Parameter	Default Value	Location	Comment
authentication.blueCoat.enabled	false	Database/Property file	Authentication with Blue Coat means that all HTTP requests having <b>Client-Cert</b> header will be authenticated as username placed in the header.  # Never expose an SMP to the WEB without properly configured reverse-proxy and active blue coat.
contextPath.output	true	Database/Property file	PRODUCTION mode. This variable is used to clear the context path of the SMP
encodedSlashesAllowedInUrl	false	Database/Property file	Most Java libraries and J2EE containers block encoded slashes in URL, for security reasons.  ## Theoretically there are no restrictions on slash "/" characters in document or participant identifiers, ## but by default we block them as well.  ## If slash "/" characters must be supported, then switch this property to "true".  ## Remember that in such case the relevant change should be also applied on J2EE level  ## I.e. for Tomcat it is handled by property: org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true

Parameter	Default Value	Location	Comment
bdmsl.integration.enabled	false	Database/Property file	BDMSL (SML) integration ON/OFF switch
identifiersBehaviour.caseSensitive.ParticipantIdentifierSchemes	casesensitive-participant-scheme1   casesensitive-participant-scheme2	Database/Property file	## All Identifiers by default are CASE-INSENSITIVE. ## Specifies schemes of participant/document identifiers that must be considered CASE-SENSITIVE.
identifiersBehaviour.caseSensitive.DocumentIdentifierSchemes	casesensitive-doc-scheme1   casesensitive-doc-scheme2	Database/Property file	## List values (delimited by pipe character: " " ) placed here are checked against runtime (request) schemes in the CASE-INSENSITIVE way
bdmsl.integration.url	# <a href="https://sml.peppolcentral.org/manageparticipantidentifier">https://sml.peppolcentral.org/manageparticipantidentifier</a>  http://localhost:8080/manageparticipantidentifier	Database/Property file	The URL of the targeted SML (incl. the service name)
bdmsl.integration.logical.address	<a href="http://localhost:8080/smp/">http://localhost:8080/smp/</a>	Database/Property file	SMP logical address. Value is used when registering new domain to SML.
bdmsl.integration.physical.address	0.0.0.0	Database/Property file	SMP physical address. Value is used when registering new domain to SML.
smp.keystore.password	Generated	Database/Property file	Encrypted password for keystore generated at initialization database properties.
smp.keystore.password.decrypted	Generated	Database/Property	Generated password for keystore. Password should be stored on save located and then the entry should be

Parameter	Default Value	Location	Comment
		file	deleted. Purpose of decrypted password is for system administrator to open/edit keystore with other tools if needed.
smp.keystore.filename	smp-keystore.jks	Database/Property file	Keystore for SMP.
configuration.dir	Parent of (xmldsig.keystore.classpath)	Database/Property file	Configuration folder
encryption.key.filename	Generated	Database/Property file	Symetric encryption key for keystore password encryption. Password is stored in database (smp.keystore.password) and encryption key is stored on server's file system.
bdmsl.integration.keystore.path (Deprecated)		Database/Property file	The location of the keystore. At initialization database propertis keystore is imported to smp-keystore.jks
bdmsl.integration.keystore.password(Deprecated)		Database/Property file	The password of the keystore
xmldsig.keystore.classpath (Deprecated)	../keystore/keystore.jks	Database/Property file	The location of the xmldsig keystore (Deprecated)
xmldsig.keystore.password(Deprecated)	peppol	Database/Property file	The password of the xmldsig keystore
jdbc.driver	com.mysql.jdbc.Driver	Property file	Database Configuration: Driver MySQL:



Parameter	Default Value	Location	Comment
			com.mysql.jdbc.Driver Oracle Database: oracle.jdbc.OracleDriver
jdbc.url	jdbc:mysql://localhost:3306/smp	Property file	Database Configuration: url MySQL : jdbc:mysql://dbhost:dbport/smp_database Oracle Database: jdbc:oracle:thin:@dbhost:dbport:smp_database jdbc:oracle:thin:@dbhost:dbport/smp_service
jdbc.user	smp	Property file	Database User/Password Configuration: User
jdbc.password	The_password	Property file	Database User/password Configuration: Password
target-database	MySQL	Property file	Target Database Backend type/Brand: For MySQL, use: MySQL For Oracle Database, use: Oracle
jdbc.read-connections.max	10	Property file	Database Configuration: Max Read Connection
bdmsl.integration.proxy.server		Database/Property file	When an SMP calls the SML and the SML is behind a proxy, then standard proxy settings need to be specified. Proxy server hostname
bdmsl.integration.proxy.port		Database/Property file	Proxy server port

Parameter	Default Value	Location	Comment
bdmsl.integration.proxy.user		Database/Property file	Proxy server user
bdmsl.integration.proxy.password		Database/Property file	Proxy server password

### 16.2.1.1. *bdmsl.integration.url*

Only used if SML/DNS integration has been selected.

In case the integration with the SML/DNS is needed, this value has to be set as the address of the SML or the loadBalancer/proxy tagetting these SML instance(s).

## 16.3. smp\_domain table configuration

This table is used to support the multi-tenancy feature of the SMP. Its parameters/fields are:

- **SML\_SMP\_ID**: This is the SMP ID that must match the SMP ID registered within the SML.
- **SML\_CLIENT\_CERT\_HEADER**: The SMP's certificate - needed only when accessing BDMSL directly through HTTP. The configured "Client-Cert" HTTP header will be added to each BDMSL request (bypassing SSL certificate verification made normally by SSL terminator) .
- **SML\_CLIENT\_KEY\_ALIAS**: This is the Domain scoped alias of the keystore private key used for authentication with the SML. The password is the same as `xmlsig.keystore.password` defined in the SMP configuration file.
- **SIGNATURE\_KEY\_ALIAS**: This field points to the **Domain scoped** alias of the Keystore private key certificate, used by the SMP to sign GET Signed Service Metadata responses.

### 16.3.1. Example: Update the default single domain smp\_domain table record:

```
update smp_domain set SML_SMP_ID='SMP-MCB-ID14', SML_CLIENT_KEY_ALIAS= 'smp_mock';
```

or

```
update smp_domain set SML_SMP_ID='SMP-MCB-ID14', SML_CLIENT_CERT_HEADER=  
'serial=000000000000000000000000000000009A195D2DD88C&subject=CN=SMP_1000000000,O=DG-  
DIGIT,C=BE&validFrom=Oct 21 02:00:00 2014 CEST&validTo=Oct 21 01:59:59 2016  
CEST&issuer=CN=Issuer Common Name,OU=Issuer Organization Unit,O=Issuer Organization,C=BE'  
where domainId='default';
```

## 17. SMP ADMIN CONSOLE

The SMP Admin console has two purposes:

- Enable anonymous users to search and explore published data in the SMP. Anonymous users can search for participants by participant ID, schema or domain.
- Enable Service Group administrators to manage owned Service groups, SMP administrators to manage Service groups registered on SMP, and System Administrators to manage users and domains.

The administration dashboard is reachable via the following URLs:

[http://\[host\]:\[port\]/smp\[-version\]/iu/](http://[host]:[port]/smp[-version]/iu/)

If the deployment package (war file) filename changed in order to simply upgrade the old SMP version as for example “smp-4.0.0.war” to “cipa-smp-full-webapp.war”, than application root context might change as well.

Example:

[http:// \[host\]:\[port\]/cipa-smp-full-webapp/ui/](http://[host]:[port]/cipa-smp-full-webapp/ui/) .

Three types of roles are defined in the SMP admin console:

- **System Administrator:** this is a “super admin” who can manage SMP users and domains
- **SMP Administrator:** the SMP administrator can create/delete Service Groups, manage users and domains for service groups and its extensions and metadata. The SMP administrator has access to all Services Groups registered in the SMP.
- **Service Group Administrator:** this user can administer only the metadata for the Service Groups that he owns. He cannot change ownerships or the domains for the existing Service Group.

When users are logged, their role is displayed in read-only mode (as a label). Only the System Administrator can change the role of another user including an SMP Administrator and a Service group Administrator. They, however, cannot change the role of another System Administrator.

## 18. CONTACT INFORMATION

CEF Support Team

By email: [CEF-EDELIVERY-SUPPORT@ec.europa.eu](mailto:CEF-EDELIVERY-SUPPORT@ec.europa.eu)

Support Service: 8am to 6pm (Normal EC working Days)