



**Submitted to the EC on XX/10/2017**

**Justice Action Grant**

## **Me-CODEX**

***Maintenance of e-Justice Communication via Online Data Exchange***

Call identifier: JUST-2015-JACC-AG-1

Topic: JUST-2015-JACC-AG-E-JU Support for national or transnational e-Justice projects

Project full title: Maintenance of e-Justice Communication via Online Data Exchange

Grant agreement n°: 721334

### **e-Delivery Configuration Management Tool**

**Abstract:**

e-Delivery allows for multiple configuration management techniques (SML/SMP and or PModes), while also having to support multiple implementations of the e-Delivery specification. As the network configuration continuously changes a generic way to update multiple heterogeneous implementations is proposed.



## History

Version	Date	Changes made	Modified by
0.1	2017-12-08	First Version	B. Riedler T. Nowosadtko
0.5	2018-07-03	Update structure New sections added describing the former process, the new CMT and a FAQ	T. Nowosadtko



## Table of contents

<b>HISTORY</b> .....	<b>2</b>
<b>TABLE OF CONTENTS</b> .....	<b>3</b>
<b>LIST OF ABBREVIATIONS</b> .....	<b>4</b>
<b>1 INTRODUCTION</b> .....	<b>5</b>
<b>2 PROCESS BEFORE CMT</b> .....	<b>6</b>
2.1.1 RELEASE OF A NEW VERSION .....	7
<b>3 CONFIGURATION MANAGEMENT TOOL (CMT)</b> .....	<b>8</b>
3.1 REQUIREMENTS .....	8
3.1.1 NCP REQUIREMENTS .....	8
3.1.2 MS REQUIREMENTS.....	8
3.1.3 ARCHITECTURAL REQUIREMENTS .....	8
3.2 ARCHITECTURE .....	9
3.3 PROCESS.....	10
3.3.1 ACTORS:.....	10
3.3.2 USE CASES .....	11
3.4 CONFIGURATION CHANGE WORKFLOW .....	13
<b>4 USING THE CMT</b> .....	<b>14</b>
4.1 CREATE A NEW PARTY .....	14
4.2 INVITE A USER.....	14
4.3 USER REGISTRATION .....	15
4.4 UPLOAD CONFIGURATION PARAMETER .....	16
4.5 DOWNLOAD CONFIGURATION FILES.....	17
<b>5 FAQ</b> .....	<b>18</b>
<b>6 GLOSSARY</b> .....	<b>21</b>
<b>7 ANNEX</b> .....	<b>22</b>
7.1 TEMPLATE FOR CONFIGURATION.PROP .....	22



## List of abbreviations

MS	Member State
CMT	Configuration management tool
NCP	National contact point
CfC	Coordinator for configuration
GW	Gateway

Figure 1 - Structure on BSCW .....	6
Figure 2 - MS directory .....	7
Figure 3 - Elements of the solution .....	9
Figure 4: Main use cases .....	11
Figure 5 -Workflow .....	13
Figure 6 - Invite a User .....	14
Figure 7 - Registration of a new user .....	15
Figure 8 – Upload environment specific parameters .....	16
Figure 9 - Download configuration files .....	17
Figure 10 - One-Way-SSL .....	19
Figure 11 - Two-Way-SSL .....	20
Figure 12 - Template for configuration.xml file .....	22



## 1 Introduction

The overall goal of the Me-CODEX project is to ensure a swift and sustainable transition of the e-CODEX project towards long-term sustainability. It is planned that an agency shall take responsibility for the daily maintenance of the building blocks, ongoing development and support to EU Member States, making use of the building blocks deployed. In doing so, it will be of the utmost importance to respect and ensure the independence of the judiciary. Until this goal could be reached, the current pilot projects developed under the e-CODEX project will be supported and the building blocks will be maintained, but no new pilot project will be initiated.

As more and more piloting member states use the e-Delivery Gateway Domibus to connect their national case management systems the need for an effective way to manage project configurations has emerged. Because of the ineffective currently used process for the configuration management and the limited usability of the underlying tools, there is a need for a new configuration management tool (CMT).

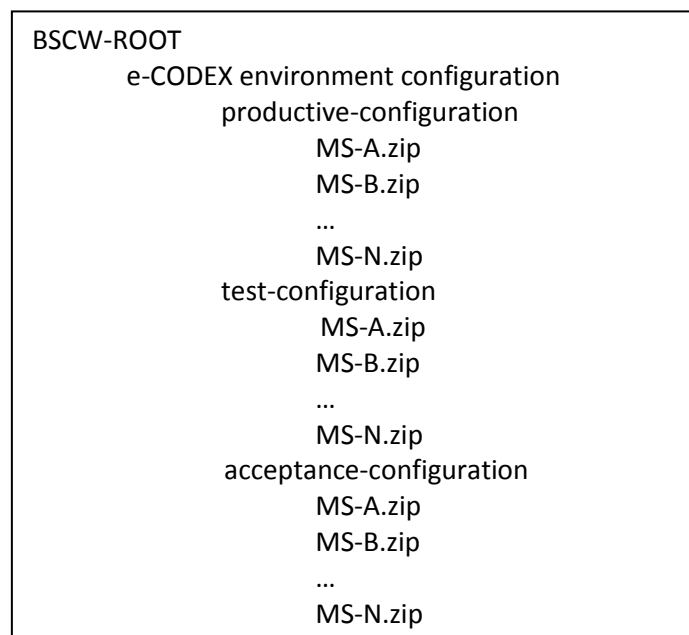
This document describes the procedure before the CMT by using existing collaboration tools and standardized configuration files. Moreover it describes the CMT, an effective solution for handling configuration creation, maintenance and distribution for the configuration management team and the piloting member states in Me-CODEX.

## 2 Process before CMT

The complexity of the distribution of member state specific information<sup>1</sup> between the national contact points<sup>2</sup> (NCP) and the Coordinator for Configuration (CfC) for the e-CODEX environments<sup>3</sup> raised the necessity for a standardized process.

The key element of this process is the use of the BSCW server, a collaboration tool which fulfils the needs of a secure exchange of configuration parameters and public keys.

The NCP uses the following structure on the [BSCW](#)<sup>4</sup> to upload the national specific information:



**Figure 1 - Structure on BSCW**

Each MS's ZIP-file contains a properties file for the configuration parameters and directories for the public keys<sup>5</sup> of Gateway (GW), Connector and SSL-Connection<sup>6</sup>. If a certificate is used multiple times, e.g. for Connector and GW, it should also be uploaded to all corresponding directories. A template of this properties file can be found in Annex *Template for configuration.prop*.

<sup>1</sup> configuration parameter and public keys for p-Modes, gateway truststore, connector truststore and SSL truststore

<sup>2</sup> See National contact persons in WP3 Tech mailing list

<sup>3</sup> test, acceptance and productive environment

<sup>4</sup> <https://www.jol.nrw.de/bscw/bscw.cgi/5390849>

<sup>5</sup> In pem format and using naming scheme pub.pem (public cert), RootCA.pem (cert root CA), SubCA[1-9].pem (cert sub CA [1-9])

<sup>6</sup> for Server and Client Authentication. Client-Authentication is just necessary if this is a requirement of one of the supported Use Cases



If a MS is running more than one GW in one environment, for each GW an extra ZIP-file must be provided.

```
MEMBER_STATE
configuration.prop
GW_public_key
Con_public_key
SSL_client_public_key
SSL_public_key
```

*Figure 2 - MS directory*

The property file **configuration.prop**<sup>7</sup> contains the MS specific parameters. This property file is already available in all MS directories and is specified in the Annex of this document.

The access to the test and production specific folders is only allowed for the NCPs. The responsible national contact person<sup>8</sup> uploads the information, which the CfC uses to create a new set of configuration files.

Finally the national contact person has to inform the CfC<sup>9</sup> via e-mail that a change on the BSCW has been made.

### 2.1.1 Release of a new version

After the release of new versions on the Nexus repository server, all piloting MS will be informed about the new release using the old WP3.tech mailing list from the e-CODEX project (wp3.tech@lists.e-codex.eu).

If you are not part of this list please contact the CfC.

---

<sup>7</sup> See Annex: Template for configuration.prop

<sup>8</sup> Also more than one person is possible

<sup>9</sup> cfc@lists.e-codex.eu

## 3 Configuration management tool (CMT)

The Configuration management tool (CMT) gives the responsible person for a local environment the opportunity to either upload their configuration parameter to the web frontend and to download the released configuration files for their specific environment.

### 3.1 Requirements

A variety of requirements can be considered that a configuration management solution may support. This includes user requirements but also other requirements related to architecture, implementation options, degree of standardization and market traction.

These requirements are specific for the Me-CODEX and it is foreseen to support also other e-Delivery based projects in the justice domain.

#### 3.1.1 NCP requirements

It must be given, that the NCPs of each participant is getting access to a centralized solution to be able to upload and edit the MS's configuration.

Via authentication the NCP is getting access to the configuration of only his MS's files and data and is not able to see and/or edit other MS's configurations.

#### 3.1.2 MS requirements

A MS must have access to be able to download and use the configuration files for the installed systems. Configuration files must be prepared to be ready for use for the specific MS.

#### 3.1.3 Architectural requirements

The CMT solution must be accessible by the user out of the user's environment. In particular this means that the CMT solution must run on a centralized portal which is accessible over the public internet. Anyway, as mentioned in the requirements above, access must be restricted for the user's role. It is also required that the communication between the CMT portal and the user's client must be via a secure connection (https).

Since the suggested implementation has an iterative approach the architecture should be aware of possible enhancements from the beginning. It is advised, that the data provided and shared will be kept in a secure storage of no deeper specification (e.g. secure filesystem storage, secure database storage).



### 3.2 Architecture

The architecture of the CMT consists of two different elements:

1. Frontend: Web interface

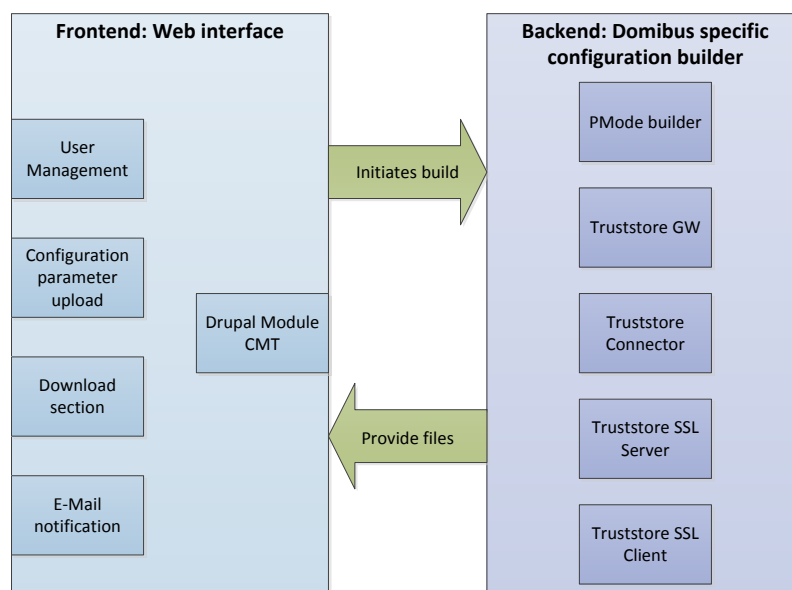
Users interact with the solution through a browser based interface, built with standard technologies based on a Java framework. The NCP can upload the specific configuration parameter for the national environment he/she is responsible for. He/she can also download configuration data for the pilots the MS is participating in. The web interface provides different roles for user and administrators.

Users participating in a specific service are automatically notified of changes in the configuration which require a participant side configuration update.

2. Backend: Domibus specific configuration builder

The application generates an Domibus specific configuration containing a full set of e-Delivery PModes and jks trust stores for

- a. ebMS message signing and encryption in the Domibus GW
- b. certificate for signing of trust-OK-token and the ASIC-S container in the connector
- c. certificates for SSL-Handshake (Server and Client authentication will be supported)



**Figure 3 - Elements of the solution**

The development of this solution is done in an iterative approach to guarantee the 100% support and generation of configuration files for the pilot activities in the different projects.

The following iterative stages are planned:

1. Development of a new library based on the current Eclipse Plug-In. The Library contains different smaller updates to support also new versions of the Domibus Gateway
2. Update of the projects for PMode generation using this library.
3. Integration of the library into the Configuration Tool. This CMT will support the complete Workflow for the creation of configuration files containing PModes, truststores GW, connector and SSL. The developed CMT in this stage can be used as the backend of the upcoming solution.
4. Development of a portal as frontend for the CMT. It is foreseen to use a Java based website framework.
5. Move all projects to the CMT.

A possible function extension of the CMT can be:

6. Development of a web service interface for an automated exchange of configuration file releases between the national environments and the CMT.
7. Integration of the web service interface into the Domibus e-CODEX plug-in and the Webadmin interface of the connector.

## 3.3 Process

### 3.3.1 Actors:

- CMT Administrator  
The administrator of the configuration management tool is responsible for the CMT and service configuration and administration.
- Project Participant  
A Project Participant is responsible for managing the configuration of one or more project servers participating in one or more projects.

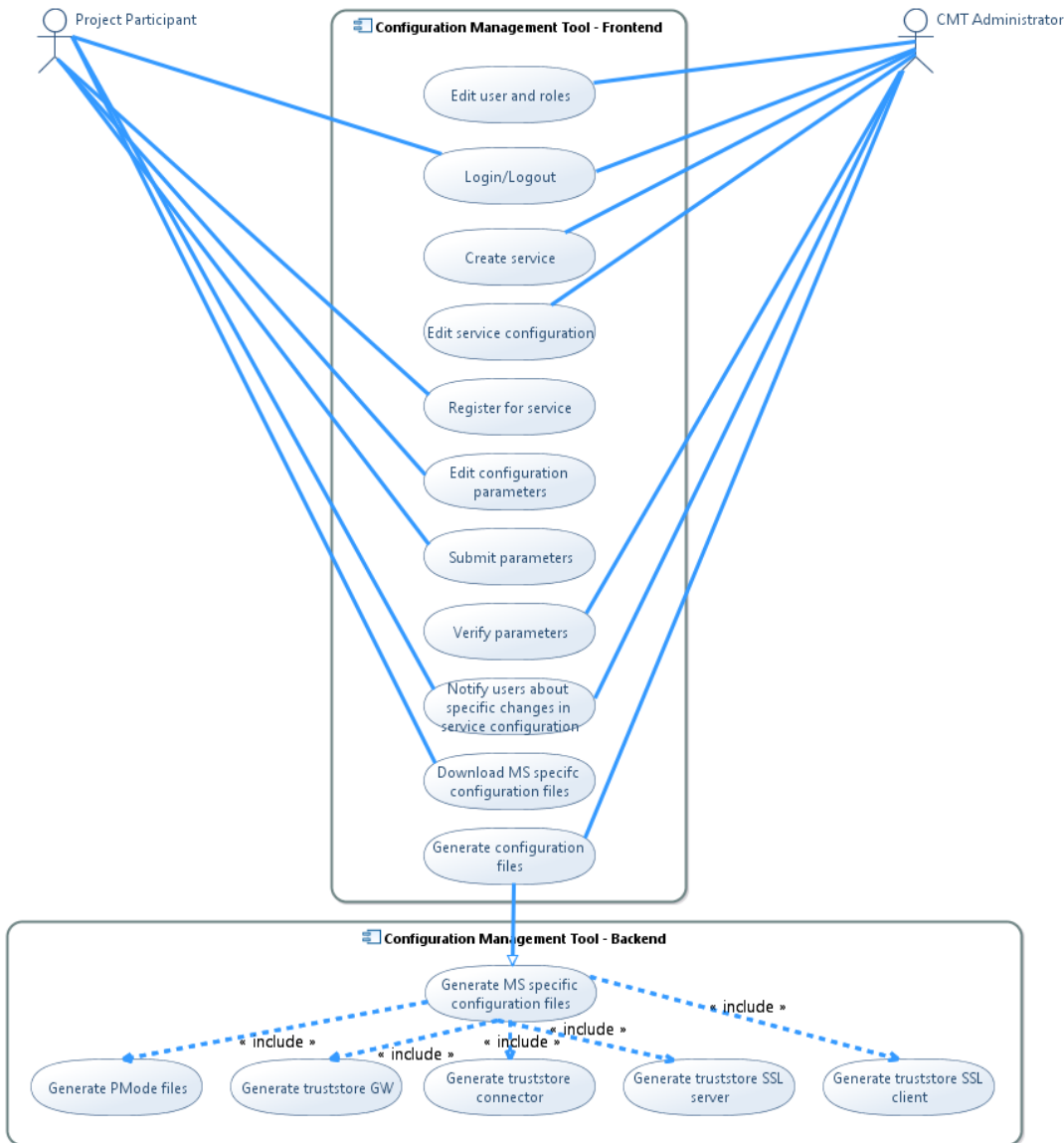


Figure 4: Main use cases

### 3.3.2 Use cases

Note:

Basic web application use cases like account creation and user management have been omitted.

- Edit user and roles  
Add or remove user and roles and modify their permissions.
- Login/Logout  
The user can login to the system. A two factor authentication (username/certificate/password) is preferred.

- **Create service**  
A new service is created. Detailed service configuration is done in the “Edit service configuration” use case.
- **Edit service configuration**  
Edit detailed service configuration like reliability, policy.
- **Register for service**  
A project participant signs up to participate in a service. This signup can be accepted/rejected by the project CMT Administrator.
- **Edit configuration parameters**  
A project participant uploads the MS configuration parameters, e.g. endpoint address and certificates.
- **Submit parameters**  
A project participant submits updated the MS configuration parameters, e.g. endpoint address and certificates.
- **Verify parameters**  
The CMT Administrator gets notified about changes to MS configuration parameters made by project participants. Those changes can be reviewed and either be accepted or rejected. Accepting the changes triggers the “Generate configuration files” use case.
- **Notify users about specific changes in service configuration**  
Whenever there are new configuration files available, either through service or participant configuration changes, project participants are notified about the availability of new configuration files.
- **Download MS specific configuration files**  
A project participant downloads configuration files for the services they participating in.
- **Generate configuration files**  
Triggers the uses case “Generate MS specific configuration files” in the component “Configuration Management Tool – Backend”
- **Generate PMode files**  
Generate a new set of PMode files either through project or participant configuration changes.
- **Generate truststore GW**  
Generate a new version of the truststore for the GW initiated by participant configuration changes.
- **Generate truststore connector**  
Generate a new version of the truststore for the connector initiated by participant configuration changes.
- **Generate truststore SSL server**  
Generate a new version of the truststore for the SSL server authentication initiated by participant configuration changes.
- **Generate truststore SSL client**  
Generate a new version of the truststore for the SSL client authentication initiated by participant configuration changes.

### 3.4 Configuration Change Workflow

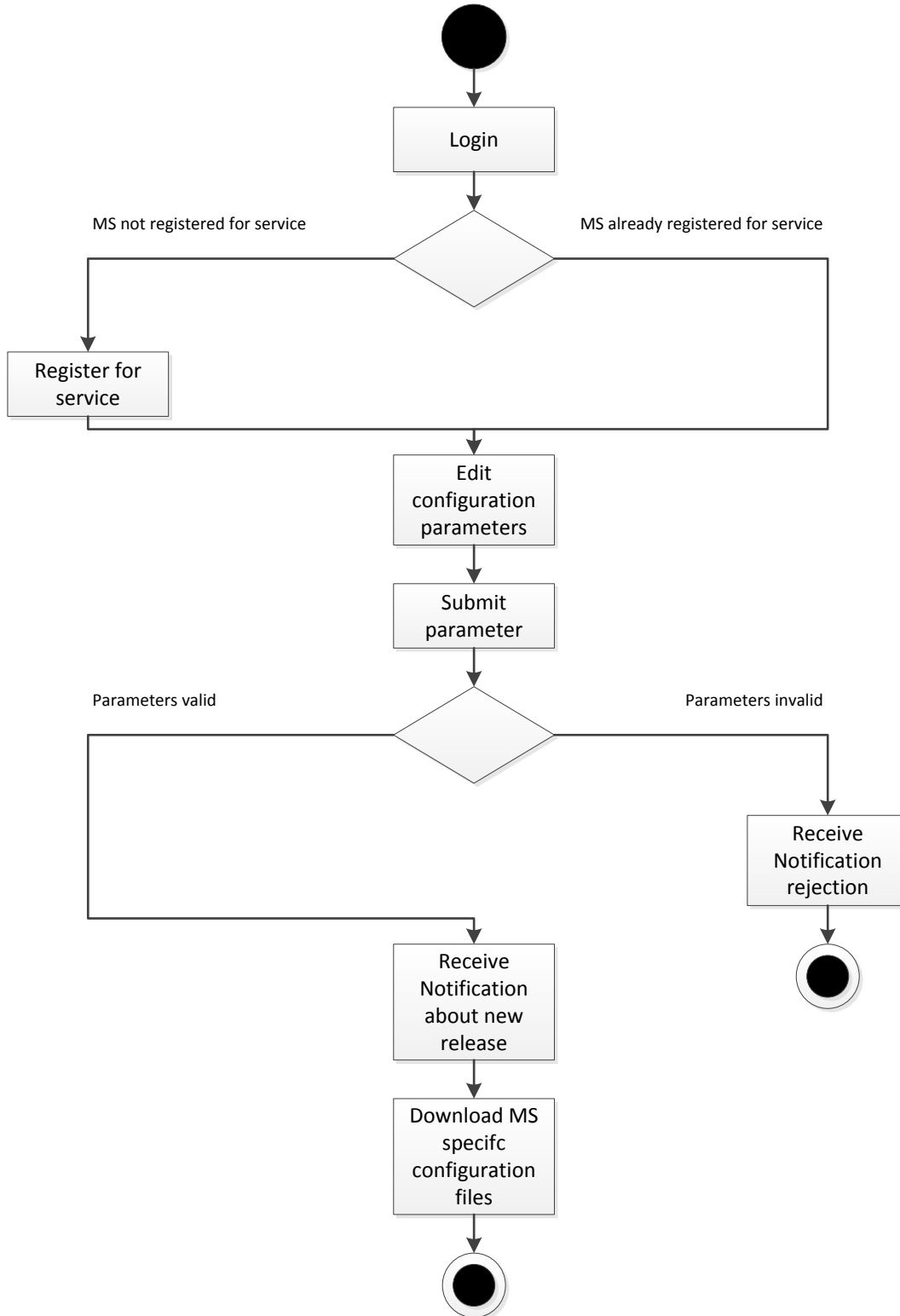


Figure 5 -Workflow

## 4 Using the CMT

### 4.1 Create a new party

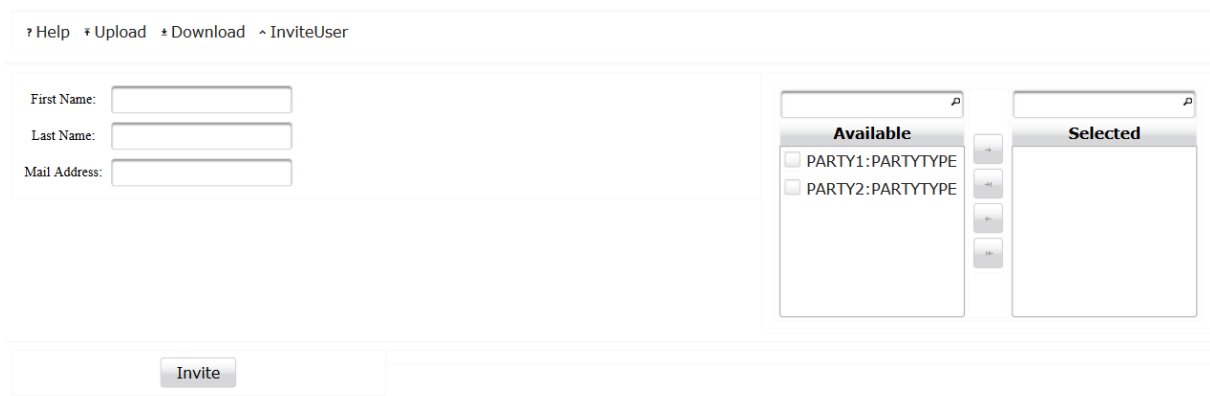
A new MS which become part of the pilot family must be represented by a specific party. Each party must have a unique identifier.

The CMT administrator must create this party with the following parameters:

- Party ID
- Party ID Type

### 4.2 Invite a user

The CMT administrator can invite new NCPs to the CMT. For this the full name and mail address must be set. Additionally the new user must assign to a specific party which is already set up by the CTP administrator.



The screenshot shows a web interface for inviting a user. At the top, there is a navigation bar with links for Help, Upload, Download, and InviteUser. Below this, there are three input fields for 'First Name', 'Last Name', and 'Mail Address'. To the right of these fields is a selection interface with two columns: 'Available' and 'Selected'. The 'Available' column contains two entries: 'PARTY1:PARTYTYPE' and 'PARTY2:PARTYTYPE', each with a checkbox. Between the columns are four buttons: a right-pointing arrow, a left-pointing arrow, a plus sign, and a minus sign. At the bottom of the form is a large 'Invite' button.

**Figure 6 - Invite a User**

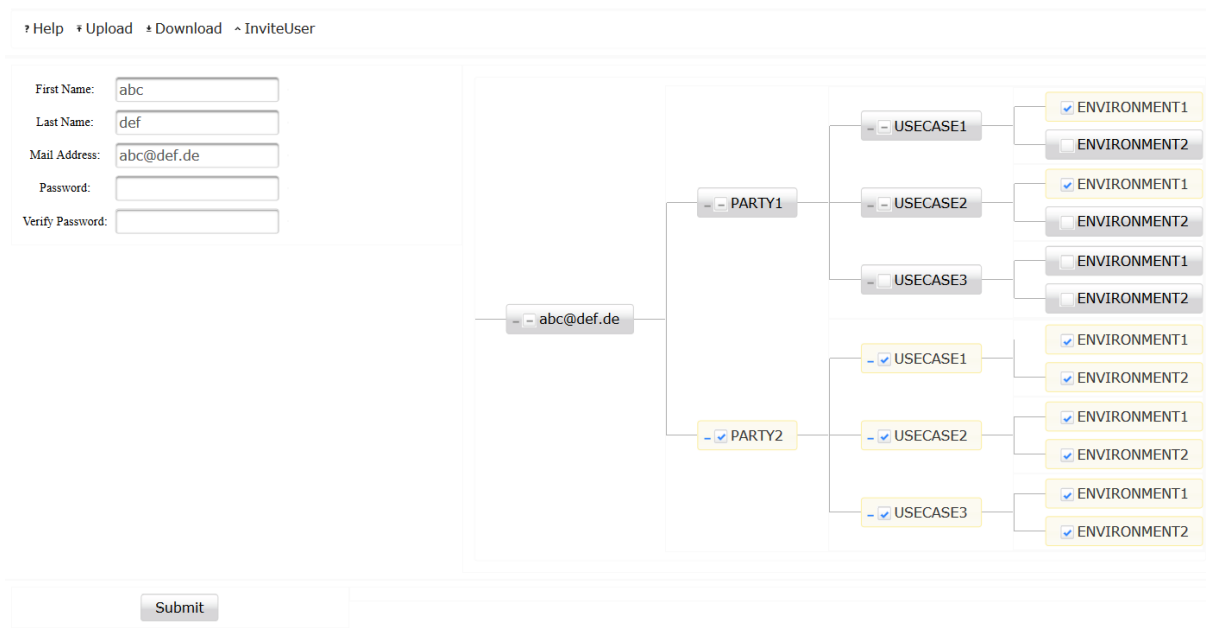
The invited user will receive an invitation mail which contains an invitation link to the registration page.



### 4.3 User registration

To complete the registration process the user gets an invitation link within the received invitation mail. The link contains a unique one-time hash so it can be used only once by the user.

On the registration page the user can set a personal password, change the full name and make a selection of the environments in which his/her party will participate in.




**Figure 7 - Registration of a new user**

Once the user has been successfully registered to the CTP, the user can change these user parameters by using the same interface.

## 4.4 Upload configuration parameter

After the user is logged in to the CMT the configuration parameters for the environments he/she is responsible for can be uploaded by using the following interface.

### Sample Layout



The screenshot shows the eCODEX Configuration Management Tool interface. On the left, there are two environment selection buttons: "PARTY1:PARTYTYPE ENVIRONMENT1" and "PARTY2:PARTYTYPE ENVIRONMENT2". On the right, there are input fields for "Endpoint URL" (https://test.de), "IP Range" (10-20), and "Port" (8080). Below these are four "Choose" buttons for "Gateway Certificate(s)", "SSL Server Certificate(s)", "SSL Client Certificate(s)", and "Connector Certificate(s)". A "Save" button is at the bottom.

**Figure 8 – Upload environment specific parameters**

Required elements in this interface are:

- Endpoint URL  
The URL to the Message Service Handler (MSH) Webservice of the Domibus Gateway
- IP Range  
IP Address Range for incoming and outgoing communication with/to the Domibus Gateway
- Port  
The Port for incoming and outgoing communication with/to the Domibus Gateway
- Gateway Certificate  
The Gateway certificate containing the complete certificate chain (CA-Certificates) in X.509 format
- SSL Server Certificate  
The SSL Server certificate containing the complete certificate chain (CA-Certificates) in X.509 format
- SSL Client Certificate  
The SSL Client certificate containing the complete certificate chain (CA-Certificates) in X.509 format



- Connector Certificate

The Connector certificate containing the complete certificate chain (CA-Certificates) in X.509 format

The uploaded parameters will be verified during the upload process. If an issue with the parameters occurs a specific error message will be displayed.

## 4.5 Download configuration files

The CMT gives the NCP the possibility to download the current and former configuration files releases for the specific parties which the NCP is responsible for.



The screenshot displays the eCODEX Configuration Management Tool interface. At the top left is the eCODEX logo. To its right are navigation links: ? Help, ¶ Upload, ± Download, and ^ InviteUser. Below the logo, there are two menu items: 'Current Releases' and 'Release History'. The main content area is titled 'Current Releases' and lists two configurations: 'config1' and 'config2'. Under 'config1', it says 'Latest version for config1' and provides a 'Download' button. Similarly, under 'config2', it says 'Latest version for config2' and provides a 'Download' button.

*Figure 9 - Download configuration files*

## 5 FAQ

### Which parameters must be provided by the NCP?

*Former process (BSCW/Nexus):*

- *Party ID*  
*A unique party ID for the Gateway*
- *Endpoint URL*  
*The URL to the Message Service Handler (MSH) Webservice of the Domibus Gateway*
- *IP Range*  
*IP Address Range for incoming and outgoing communication with/to the Domibus Gateway*
- *Port*  
*Port for incoming and outgoing communication with/to the Domibus Gateway*
- *Supported services*  
*A list of the supported e-Justice services*
- *Gateway Certificate*  
*The Gateway certificate containing the complete certificate chain (CA-Certificates) in X.509 format*
- *SSL Server Certificate*  
*The SSL Server certificate containing the complete certificate chain (CA-Certificates) in X.509 format*
- *SSL Client Certificate*  
*The SSL Client certificate containing the complete certificate chain (CA-Certificates) in X.509 format*
- *Connector Certificate*  
*The Connector certificate containing the complete certificate chain (CA-Certificates) in X.509 format*

*Process using the CMT:*

- *Endpoint URL*  
*The URL to the Message Service Handler (MSH) Webservice of the Domibus Gateway*
- *IP Range*  
*IP Address Range for incoming and outgoing communication with/to the Domibus Gateway*
- *Port*  
*Port for incoming and outgoing communication with/to the Domibus Gateway*
- *Gateway Certificate*  
*The Gateway certificate containing the complete certificate chain (CA-Certificates) in X.509 format*
- *SSL Server Certificate*  
*The SSL Server certificate containing the complete certificate chain (CA-Certificates) in X.509 format*

- *SSL Client Certificate*  
The SSL Client certificate containing the complete certificate chain (CA-Certificates) in X.509 format
- *Connector Certificate*  
The Connector certificate containing the complete certificate chain (CA-Certificates) in X.509 format

### Who should be informed about configuration changes of your party?

First the CfC must be informed about the changes to create a new release of configuration files for the affected use cases (services).

Once a new release is available all NCPs will be informed via the WP3.tech mailing list.

### Are there any requirements on the used certificates?

The certificates for the Gateway and Connector must support encryption and signing (KeyUsage).

The certificate for the SSL handshake must support signing (KeyUsage).

### What is the difference between the SSL Server certificate and the SSL Client certificate?

Both certificates are used during the SSL handshake.

During the standard SSL handshake, the recipient of the HTTP request (Server) provides his certificate to identify himself and to give the client the opportunity to decrypt the received packages. The provided certificate is the SSL Server certificate.

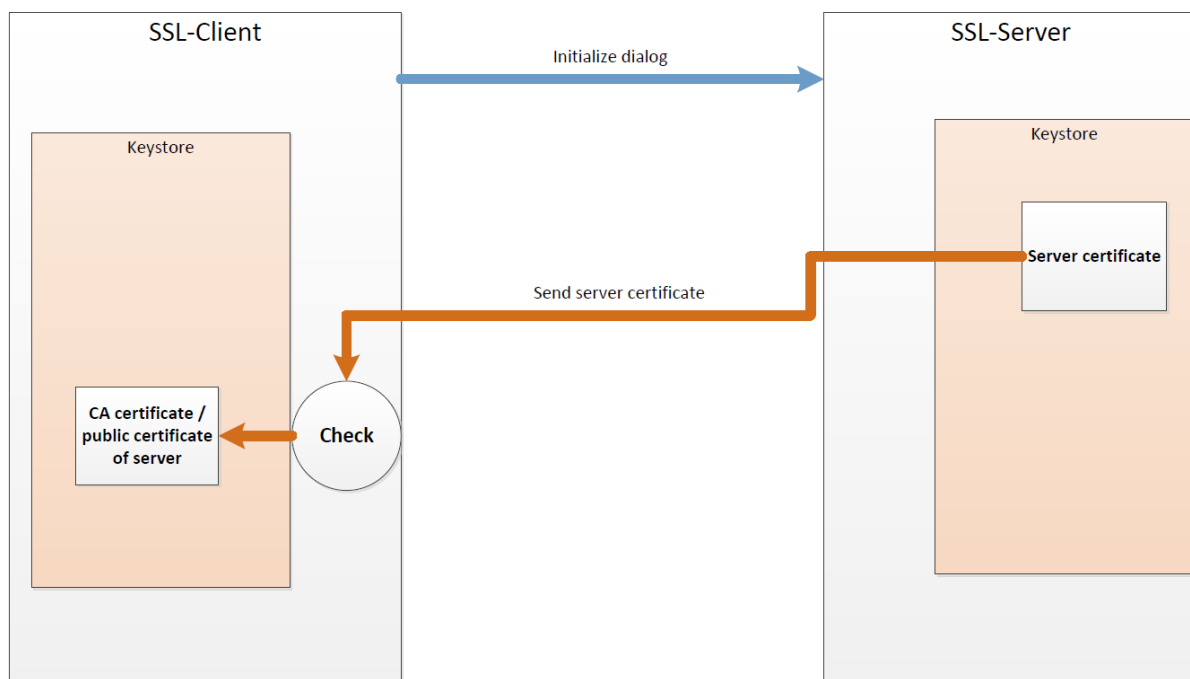


Figure 10 - One-Way-SSL

Based on the agreed policy of the use case (service) it could be required to support so called mutual authentication.

Different to the standard One-Way-SSL handshake the client provides also a certificate to identify him during the handshake and to give the server the opportunity to decrypt the received packages too.

The provided certificate is the SSL Client certificate.

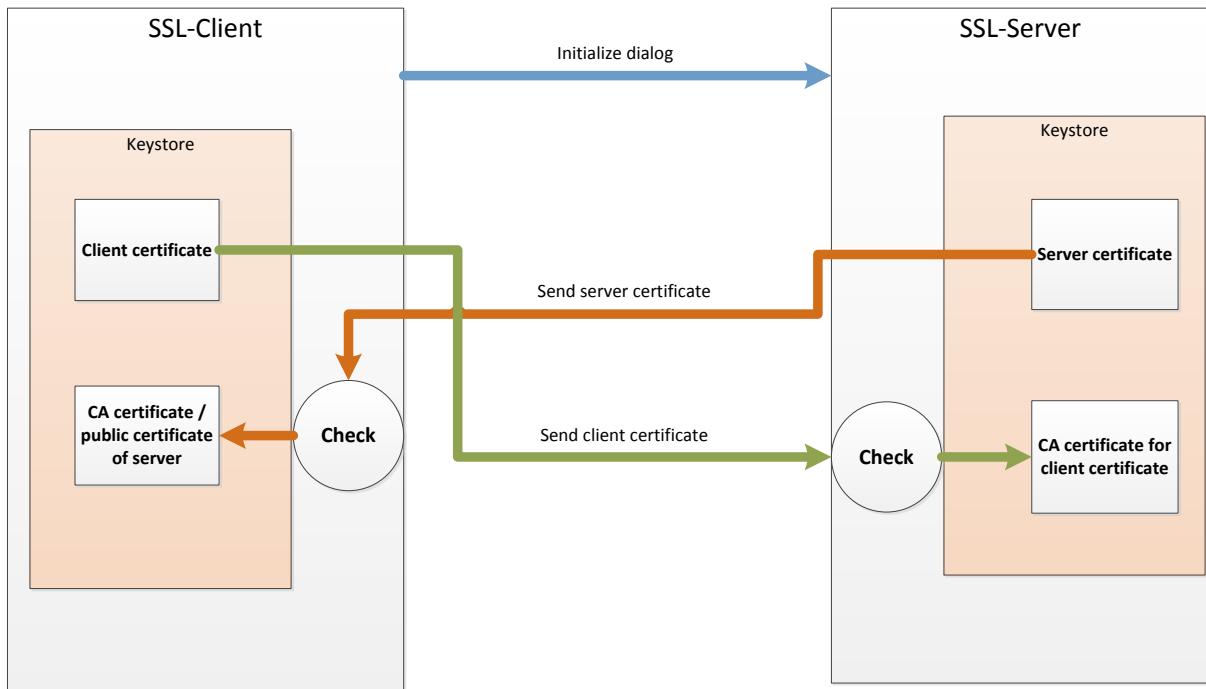


Figure 11 - Two-Way-SSL

## 6 Glossary

**Configuration Management Tool (CMT):**

Web based tool for the configuration management of different projects.

**Service:**

A Service is a self-contained set of dependent message exchange agreements e.g. EUCEG, BRIS.

**Gateway:**

The Gateway software product provides the eDelivery functionality based on the corresponding specification.

**Certificate:**

Electronic document used in cryptography.

## 7 Annex

### 7.1 Template for configuration.prop

```
*****  
#EXAMPLE STRUCTURE FOR CONFIGURATION EXCHANGE  
*****  
  
# Country Code for your Country. Example EE for Estonia.  
partyId = country_code  
# Use Cases(Services) you wish to participate. Example EPO, MLA, SMALL_CLAIMS  
services = service  
# Endpoint address for your GW webservice  
endpoint.uri = endpoint_uri  
#Port for endpoint  
port = port  
# Endpoint IP address used for the message outflow FROM this party. (Multiple IPs or IP  
range)  
endpoint.outflow.ip = endpoint_outflow_ip  
# Endpoint IP address used for the message inflow TO this party. (Multiple IPs or IP range)  
endpoint.inflow.ip = endpoint_inflow_ip
```

*Figure 12 - Template for configuration.xml file*