



EUROPEAN COMMISSION

DIGIT  
Digital Europe Programme

# Software Architecture Document

© European Union, 2022

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: 29/04/2022

Document Approver(s):

| Approver Name   | Role            |
|-----------------|-----------------|
| Bogdan DUMITRIU | Project Manager |
|                 |                 |

Document Reviewers:

| Reviewer Name                    | Role                     |
|----------------------------------|--------------------------|
| Cosmin BACIU                     | Domibus Technical leader |
| Caroline AEBY and Chaouki BERRAH | Technical Writer         |
| Catalin-Emanuel ENACHE           | Developer                |

Summary of Changes:

| Version | Date       | Created by                               | Short Description of Changes  |
|---------|------------|--|---|
| 0.1     | 21.07.2016 | Christian KOCH                           | Initial draft   |
| 0.2     | 27.09.2016 | Christian KOCH,<br>Stefan MÜLLER         | Changes according to comments   |
| 0.3     | 30.09.2016 | Stefan MÜLLER                            | Chapters about logging and caching added  |
| 0.4     | 05.10.2016 | Federico Martini                         | Added information about<br>TB_MESSAGE_LOG and TB_ERROR_LOG  |
| 0.5     | 06.10.2016 | Christian KOCH,<br>Stefan MÜLLER         | Information about certificate handling and<br>retry mechanism added. Graphics updated.                            |
| 1.0     | 10.10.2016 | Adrien FERIAI                            | First published version   |
| 1.1     | 13.01.2017 | Cosmin BACIU                             | Documented new Domibus logging<br>framework   |
| 1.2     | 29.06.2017 | Cosmin BACIU                             | Documented the domibus-ext-services-api   |
| 1.3     | 03.10.2017 | Cosmin BACIU                             | Documented the messageStatusChanged<br>method and updated the diagrams for the<br>outgoing/incoming message flows |
| 1.4     | 09.10.2017 | CEF Support                              | Update list of reviewers  |
| 1.5     | 24/11/2017 | CEF Support                              | Updates for Domibus 3.3.1   |
| 1.6     | 03/01/2018 | Tiago MIGUEL                             | Update Log Codes for Domibus 3.3.2  |
| 1.7     | 20/03/2018 | CEF Support                              | Reuse notice added, e-Sens AS4 profile<br>replaced by eDelivery AS4 profile                                       |
| 1.8     | 21/06/2018 | CEF Support                              | Updated for Domibus 3.3.4 link to REST<br>api)  |
| 1.9     | 30/07/2018 | Cosmin BACIU & CEF<br>Support            | Documented multi-tenancy; moved the<br>External API documentation in the Plugin<br>Cookbook                       |
| 1.10    | 04/09/2018 | CEF Support                              | Domibus 4.0   |
| 1.11    | 17/09/2018 | Caroline AEBY                            | Multi-tenancy => Multitenancy   |
| 1.12    | 18/09/2018 | Chaouki BERRAH<br>Catalin-Emanuel ENACHE | Update<br>UIReplication added   |
| 1.13    | 26/09/2018 | Caroline AEBY                            | CEF Support contact information added   |
| 1.14    | 07/12/2018 | Caroline AEBY                            | Domibus 4.0.1 update  |
| 1.15    | 11/02/2019 | Caroline AEBY                            | Domibus 4.0.2 update  |
| 1.16    | 16/04/2019 | Caroline AEBY                            | Domibus 4.1-RC1 update  |
| 1.17    | 15/07/2019 | Caroline AEBY                            | Version 4.1-RC1 => 4.1  |
| 1.18    | 09/09/2019 | Caroline AEBY                            | Domibus 4.1 => 4.1.1  |
| 1.19    | 29/11/2019 | Caroline AEBY                            | Domibus 4.1.1 => 4.1.2  |

|     |            |   |   |
|-----|------------|---|---|
| 1.2 | 04/02/2020 | Caroline AEBY   | Domibus 4.1.2 => 4.1.3  |
| 1.3 | 04/09/2020 | Caroline AEBY   | Domibus 4.1.5 + Domibus version agnostic  |
| 1.4 | 10/09/2020 | Caroline AEBY<br>Ion PERPEGEL<br>Sebatian TINCU<br>Arun VENUGOPAL | Domibus 4.2:<br>Section 9.1.1 Data auditing added<br>Section 14.5: properties with multimode<br>Domibus log codes added |
| 1.5 | 21/09/2020 | Caroline AEBY   | Domibus 4.2 RC version release  |
| 1.6 | 21/10/2020 | Arun VENUGOPAL<br>Caroline AEBY                                   | Domibus 4.2. FR – updates in BUS log codes  |
| 1.7 | 25/02/2021 | Caroline AEBY   | Domibus 4.2.1 version   |
| 1.8 | 25/02/2021 | Caroline AEBY   | Domibus 4.2.2 version   |
| 1.8 | 29/04/2022 | Caroline AEBY   | Domibus 4.2.9 version + no more CEF references +links update  |
| 2.0 | 29/04/2022 | Caroline AEBY   | Domibus 5.0 version   |

## Table of Contents

|   |           |
|---|-----------|
| <b>1. INTRODUCTION .....</b>                          | <b>6</b>  |
| 1.1. Purpose.....                                     | 6         |
| 1.2. Scope .....                                      | 6         |
| 1.3. References.....                                  | 6         |
| 1.4. Document Content Overview.....                   | 8         |
| <b>2. ARCHITECTURAL REPRESENTATION .....</b>          | <b>9</b>  |
| <b>3. ARCHITECTURAL GOALS AND CONSTRAINTS .....</b>   | <b>10</b> |
| <b>4. SECURITY.....</b>                               | <b>11</b> |
| 4.1. Introduction.....                                | 11        |
| 4.2. Corner 1 - Corner 2 Communication .....          | 11        |
| 4.3. Corner 2 – Corner 3 Communication .....          | 11        |
| 4.3.1. Certificate Configuration .....                | 11        |
| 4.3.2. Client Certificate.....                        | 11        |
| 4.4. Corner 3 – Corner 4 Communication .....          | 11        |
| 4.5. Administrative Sites.....                        | 12        |
| <b>5. USE-CASE VIEW.....</b>                          | <b>13</b> |
| <b>6. LOGICAL VIEW .....</b>                          | <b>15</b> |
| 6.1. Overview .....                                   | 15        |
| 6.2. Architecturally Significant Design Packages..... | 15        |
| 6.2.1. Back office system (Corner 1/4).....           | 15        |
| 6.2.2. Domibus plugin implementation.....             | 15        |
| 6.2.3. Domibus default plugins .....                  | 16        |
| 6.2.4. Domibus plugin API .....                       | 16        |

|   |           |
|---|-----------|
| 6.2.5. Domibus MSH (Corner 2/3) .....   | 16        |
| 6.2.6. Administrative GUI .....   | 16        |
| <b>7. DEPLOYMENT VIEW .....</b>   | <b>17</b> |
| <b>8. IMPLEMENTATION VIEW .....</b>   | <b>18</b> |
| 8.1. Overview .....   | 18        |
| <b>9. DATA VIEW .....</b>   | <b>20</b> |
| 9.1. Data Model .....   | 20        |
| 9.1.1. Data Auditing .....  | 23        |
| 9.2. State Machines .....   | 23        |
| 9.2.1. Outgoing Message State Machine .....                                     | 23        |
| 9.2.2. Incoming Message State Machine .....                                     | 23        |
| <b>10. SIZE AND PERFORMANCE .....</b>   | <b>25</b> |
| 10.1. Size .....  | 25        |
| 10.2. Performance .....   | 25        |
| <b>11. QUALITY .....</b>  | <b>26</b> |
| 11.1. Extensibility .....   | 26        |
| 11.2. Reliability .....   | 26        |
| 11.3. Portability .....   | 26        |
| <b>12. LOGGING .....</b>  | <b>27</b> |
| 12.1. Implementation .....  | 27        |
| 12.2. Domibus log codes .....   | 28        |
| <b>13. CACHING .....</b>  | <b>35</b> |
| <b>14. MULTITENANCY .....</b>   | <b>36</b> |
| 14.1. General .....   | 36        |
| 14.1. Identifying the domain (tenant) .....                                     | 36        |
| 14.1.1. Selecting the database schema .....                                     | 37        |
| 14.2. User association to a domain .....  | 37        |
| 14.3. UI .....  | 37        |
| 14.3.1. Managing multiple domains from the Domibus Administration Console ..... | 37        |
| 14.3.2. Security .....  | 38        |
| 14.4. Plugins .....   | 38        |
| 14.4.1. Security .....  | 38        |
| 14.4.2. Plugin API .....  | 39        |
| 14.4.3. WS Plugin .....   | 39        |
| 14.4.4. JMS Plugin .....  | 39        |
| 14.4.5. FS Plugin .....   | 40        |
| 14.5. Domibus Properties .....  | 40        |
| 14.6. Logging .....   | 42        |

|  |           |
|--|-----------|
| 14.7. Message Payloads .....                                       | 42        |
| 14.8. Quartz.....  | 43        |
| <b>15. UI REPLICATION MECHANISM .....</b>                          | <b>44</b> |
| 15.1. TB_MESSAGE_UI table and V_MESSAGE_UI_DIFF view .....         | 44        |
| 15.1.1. TB_MESSAGE_UI .....  | 44        |
| 15.1.2. V_MESSAGE_UI_DIFF .....                                    | 45        |
| 15.1.3. Native tables.....   | 46        |
| 15.2. UIReplication queue, JMS message producer and consumer ..... | 46        |
| 15.3. UIReplication Quartz Job .....                               | 47        |
| 15.4. UIReplication REST methods .....                             | 47        |
| 15.5. Migration script.....  | 47        |
| 15.6. Enabling/disabling the UIReplication mechanism.....          | 48        |
| <b>16. CONTACT INFORMATION .....</b>                               | <b>49</b> |

# 1. INTRODUCTION

## 1.1. Purpose

This document provides a comprehensive architectural overview of the system, using a number of different architectural views to depict individual aspects of the system. It is intended to capture and convey the significant architectural decisions that have been made on the system.

## 1.2. Scope

The architecture described in this document concerns the middleware Domibus created by the e-CODEX project and adopted by the CEF as sample platform for e-delivery. It is compliant with the eDelivery profile [REF2] of the OASIS ebMS3/AS4 standard. This document is not intended to explain the ebMS3/AS4 standards, the four-corner model or any other concepts described in the provided references.

## 1.3. References

| #      | Document                                | Contents outline   |
|--------|---|--|
| [REF1] | <a href="#">eDelivery AS4 Profile</a>   | The eDelivery AS4 Profile is a profile of the <a href="#">ebMS3</a> and <a href="#">AS4</a> OASIS Standards. It has provisions for use in four-corner topologies, but it can also be used in point-to-point exchanges. |
| [REF2] | <a href="#">OASIS AS4 Profile</a>       | AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23 January 2013.  |
| [REF3] | <a href="#">ebMS3 Core</a>              | OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features. OASIS Standard. 1 October 2007.   |
| [REF4] | <a href="#">Domibus plugin cookbook</a> | Technical manual on Domibus plugin development.  |
| [REF5] | <a href="#">Apache CXF</a>              | Apache CXF is an open source services framework. These services can speak a variety of protocols such as SOAP, XML/HTTP, RESTful HTTP, or CORBA and work over a variety of transports such as HTTP, JMS or JBI.        |

---

|                |   |  |
|----------------|---|--|
| <b>[REF6]</b>  | <a href="#">Apache WSS4J</a>            | The Apache WSS4J™ project provides a Java implementation of the primary security standards for Web Services, namely the OASIS Web Services Security (WS-Security) specifications from the <a href="#">OASIS Web Services Security TC</a>   |
| <b>[REF7]</b>  | <a href="#">WS-Policy Specification</a> | The Web Services Framework provides a general-purpose model and corresponding syntax to describe the policies of entities in a Web services-based system.  |
| <b>[REF8]</b>  | <a href="#">Spring Security</a>         | Spring Security is a framework that focuses on providing both authentication and authorization to Java applications. It can easily be extended to meet custom requirements.  |
| <b>[REF9]</b>  | Bcrypt                                  | <i>Provos, Niels; Mazières, David; Talan Jason Sutton 2012 (1999). "<a href="#">A Future-Adaptable Password Scheme</a>". <i>Proceedings of 1999 USENIX Annual Technical Conference</i>: 81–92.</i>   |
| <b>[REF10]</b> | <a href="#">JMS</a>                     | The Java Message Service (JMS) API is a Java Message Oriented Middleware API for sending messages between two or more clients.   |
| <b>[REF11]</b> | <a href="#">e-CODEX</a>                 | The e-CODEX project improves the cross-border access of citizens and businesses to legal means in Europe and furthermore creates the interoperability between legal authorities within the EU.   |
| <b>[REF12]</b> | <a href="#">Java Servlet 3.0</a>        | A Java servlet is a Java program that extends the capabilities of a server. Although servlets can respond to any types of requests, they most commonly implement applications hosted on Web servers. Such Web servlets are the Java counterpart to other dynamic Web content technologies such as PHP and ASP.NET. |
| <b>[REF13]</b> | <a href="#">Xtext</a>                   | Xtext is a framework for development of programming languages and domain-specific languages.   |
| <b>[REF14]</b> | <a href="#">SOAP</a>                    | Simple Object Access Protocol  |

---

[REF15] [HTTP Chunking](#)

A mechanism by which data is broken up into a number of chunks when sent over an HTTP connection.

---

---

## 1.4. Document Content Overview

After summarizing the architectural representation, goals and constraints, this document describes the system using several architectural views (Use Case, logical, process, deployment, implementation and data) and then concludes with size, performance and quality considerations.



## 2. ARCHITECTURAL REPRESENTATION

The next two sections of the document describe the architectural goals and constraints.

Architecturally relevant Use Cases are described by a Use Case diagram and a short explanation of their impact on the architecture. The following views will also be provided:

- A logical view provides a high-level view of the platform presenting the structure of the system through its components and their interactions.
- An implementation view describes the software layers and the main software components. A component diagram is used in this view.
- A deployment view provides a description of the hardware components and how they are linked together. This view gives a technical description of protocols and hardware nodes used.
- A data view provides information about the data persistency. A class diagram will be used to model the main system data.

UML diagrams are systematically used to represent the different views of the system.

### 3. ARCHITECTURAL GOALS AND CONSTRAINTS

The following non-functional requirements that affect the architectural solution have been identified:

| Non-functional requirement | Description  |
|----------------------------|--|
| Adaptability               | The application shall be easy to be integrated into existing business workflows using different communication protocols and data formats |
| Portability                | The application shall be able to be deployed on a wide variety of software/hardware systems  |
| Interoperability           | The system shall be interoperable with both commercial and free alternative implementations of the eDelivery profile.                    |

## 4. SECURITY

### 4.1. Introduction

The Domibus middleware provides built-in security in accordance to the implemented [REF2] specification and industry best practices. It can also be easily integrated into existing security domains.

### 4.2. Corner 1 - Corner 2 Communication

As no assumptions can be made about the security architecture of corner 1/4 (back office), the integration into the existing architecture has to be provided by the Domibus plugins. While the default plugins do not include any security constraints they can be easily extended to accommodate most of the security requirements.

### 4.3. Corner 2 – Corner 3 Communication

The communication between corner 2 and corner 3 is able to fulfil all the security requirements specified in the eDelivery AS4 profile. The configuration is handled via WS-Policy files and PMode configuration. All webservice security is enforced by the Apache CXF framework [REF5].

#### 4.3.1. Certificate Configuration

The location and credentials of private and public certificates used by CXF are configured in the **domibus.properties** property configuration file.

#### 4.3.2. Client Certificate

The client certificate for use with client authentication (two-way SSL) is configured in the “clientauthentication.xml” spring configuration file. Incoming TLS secured connections terminate at the proxy server (e.g. Apache httpd) and must be configured according to the employed proxy server’s documentation.

### 4.4. Corner 3 – Corner 4 Communication

The security between corner 3 and corner 4 is handled via the same mechanisms used in the communication corner 1 – corner 2.

## 4.5. Administrative Sites

Access to the Domibus administration page is secured with username/password. The credentials are managed by a Spring authentication manager and multiple authentication providers can be plugged into it. By default, the credentials are stored in the database and they are managed by an authentication provider that uses a Bcrypt strong hashing function for encoding them. Integration into an existing authentication scheme (i.e. LDAP) can be performed via Spring configuration.

### SECURITY DISCLAIMER

On top of the security that Domibus provides, the user shall take additional security measures according to best practices and regulations. This includes, but is not limited to, using firewalls, IP whitelists and file system/database encryption. DIGIT shall not be held responsible for any security breach that might occur due to User not respecting this recommendation.

## 5. USE-CASE VIEW

This section provides a representation of the use cases relevant for the architecture.

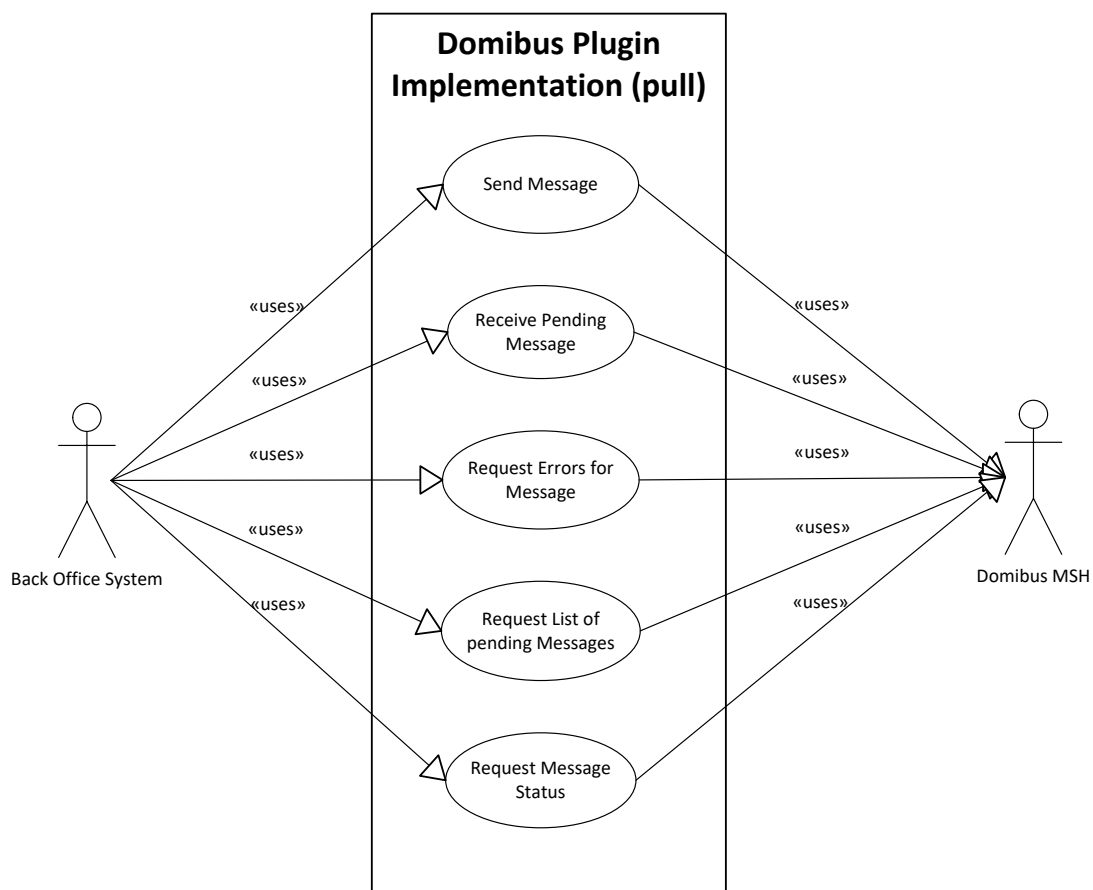
### 5.1. Selection Rationale

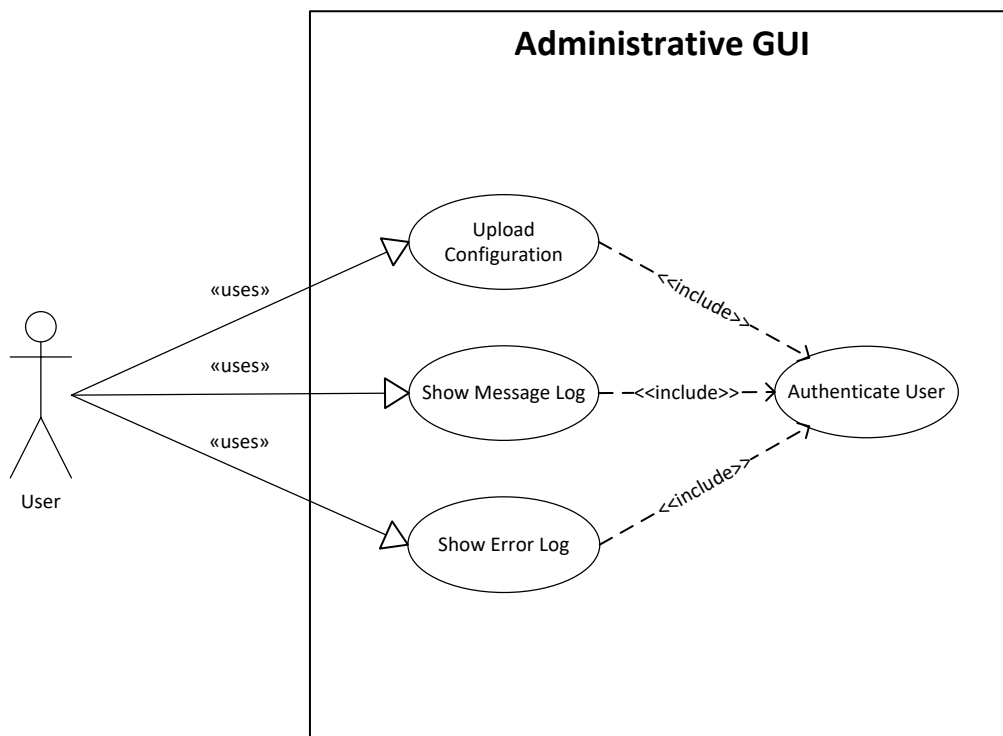
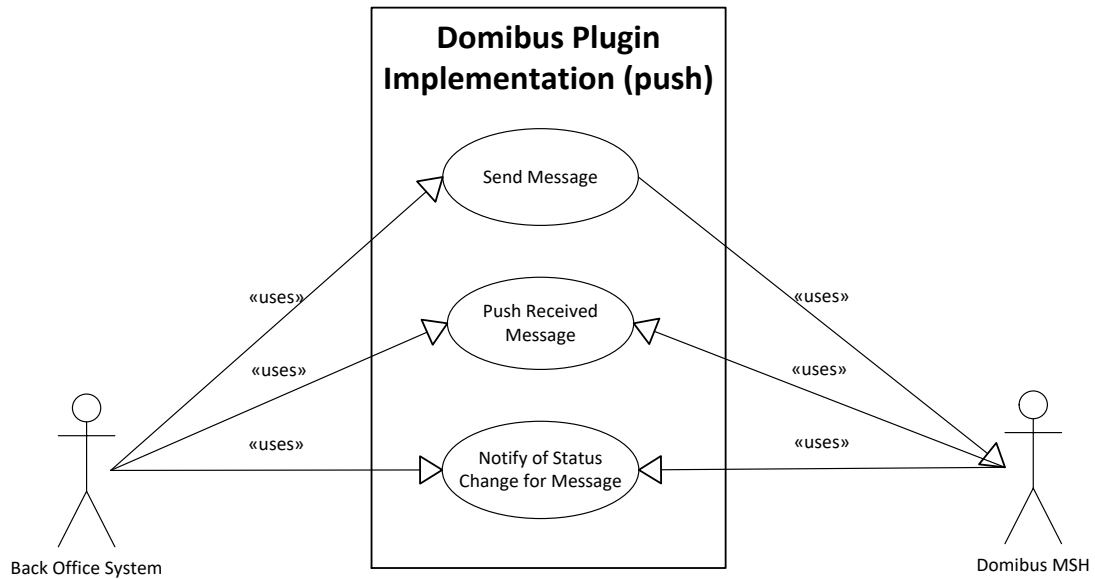
The use cases relevant for the architecture have been selected based on the following criteria:

- Use cases affecting the exchange between the back office system and the Domibus MSH.
- Use cases representing critical parts of the architecture, thereby addressing the technical risks of the project at an earlier stage.

The following use cases have been selected:

- Back office integrations using pull communication (i.e. WebService)
- Back office integrations using push communication (i.e. JMS)
- Usage of the administrative GUI





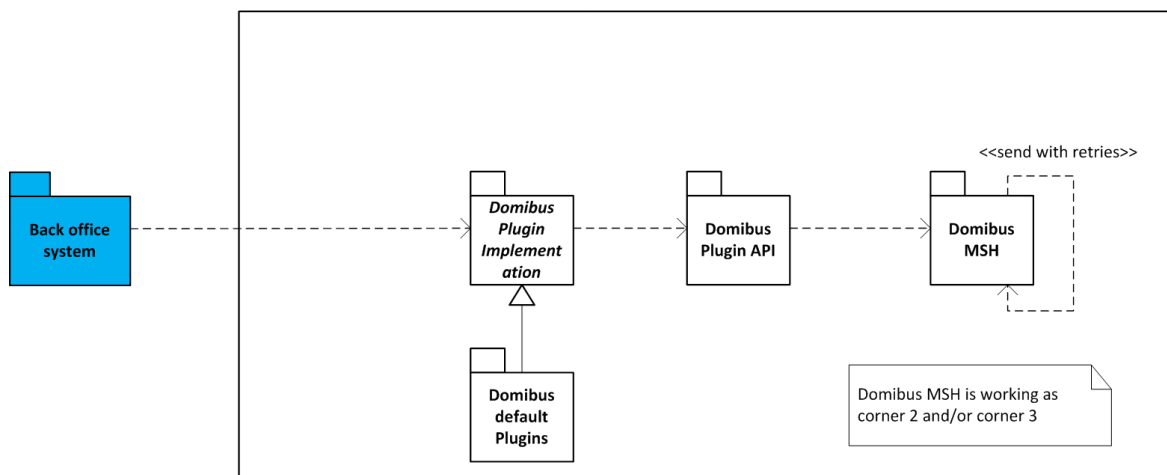
## 6. LOGICAL VIEW

### 6.1. Overview

This chapter describes the main application modules, how they interact and how they implement the specification and profile.

### 6.2. Architecturally Significant Design Packages

The following diagram provides a high-level view of the main packages composing the system. The Database persistence and file system persistence are logical packages representing the physical data storages used by the platform. The others represent different application layers and give an overview of the organisation of the platform's code.



#### 6.2.1. Back office system (Corner 1/4)

The whole purpose of Domibus is to connect different back office systems via structured, secure message exchange. While, regarding a single message exchange, corner 1 and 4 are usually different applications running in different environments, within a single deployment the role of corner 1 and corner 4 (for different message exchanges) is usually occupied by the same application. Therefore, from a logical point of view, corner 1 and 4 are the same package.

#### 6.2.2. Domibus plugin implementation

This module is responsible for the communication between the back office system and Domibus and for the mapping from the back office internal data format to Domibus internal data format. The communication and the mapping of the data can be done in both directions. Integration into existing security architecture can also be implemented here.

As there can be made few assumptions about the back office system, this module is commonly implemented by the Domibus user. Details on this process can be found inside the Domibus Plugin Cookbook.

### **6.2.3. Domibus default plugins**

Domibus provides three default plugins, which serve for testing purposes and as examples for custom implementations. They were initially developed to accommodate the needs of the e-CODEX project and thus will not be suitable for every use case.

### **6.2.4. Domibus plugin API**

This package contains all necessary interfaces and classes required to implement a Domibus plugin

### **6.2.5. Domibus MSH (Corner 2/3)**

The Domibus MSH (Message Service Handler) is the main module, representing corner 2 and/or 3 in a 4-corner message exchange. All the implementation relevant to the eDelivery profile is done inside this package. It is deployable on any Container supporting the Java Servlet Specification v 3.0.

To support the required AS4 retry mechanisms a spring configured cronjob regularly checks for messages that need to be resent. The cronjob is configured using Spring and it uses the property: "domibus.msh.retry.cron" defined in the configuration file domibus.properties. This does not configure the retry interval for messages (which is done via PModes).

### **6.2.6. Administrative GUI**

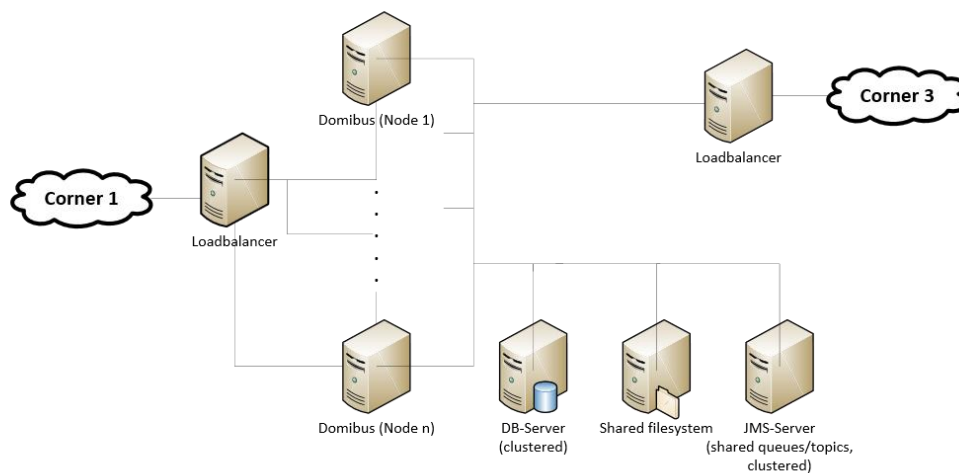
This package contains of a Spring MVC web application providing basic monitoring and configuration options.



## 7. DEPLOYMENT VIEW

The following is a description of the hardware nodes running the execution environment for the system.

The following diagram provides a view of hardware components involved in this project. Note that a clustered environment is shown. If a single server deployment is sufficient (i.e. for testing purposes), a load balancer and multiple hardware nodes are not required.



It is important to note that not all physical nodes are represented on this diagram. Indeed load balancers, database servers and JMS servers could be duplicated for scalability, performance and availability reasons. Furthermore, security mechanisms like firewalls are not shown.

These are the identified hardware nodes.

- Load balancers are responsible for distributing requests among multiple Domibus nodes. A random round robbing/no sticky session setup is recommended.
- Java servlet containers with deployed Domibus instances are responsible for message processing
- A database server (MySQL or Oracle ) is responsible for storing messages and PMode configuration data
- The shared file system contains shared Domibus configuration data, file based PMode data (Keystores) and, depending on configuration, binary data of message attachments.

## 8. IMPLEMENTATION VIEW

### 8.1. Overview

The following diagram describes the software layers of the system and their components.

The AS4 MSH Service is the web service which accepts the AS4 requests and it is the one that is called by the external systems. External MSH services are accessed through the **AS4 Message Dispatch Service**, which is a web service client capable of sending AS4 requests. The Back office systems can access the platform through their respective plugin implementations. The **Web Layer** is accessed typically by a web browser. The MSH SOAP handling is implemented using the Apache CXF framework.

The **Integration Layer** uses the Spring framework and is responsible for the integration of custom plugins and all communication processes and data format translations between back office systems and Domibus.

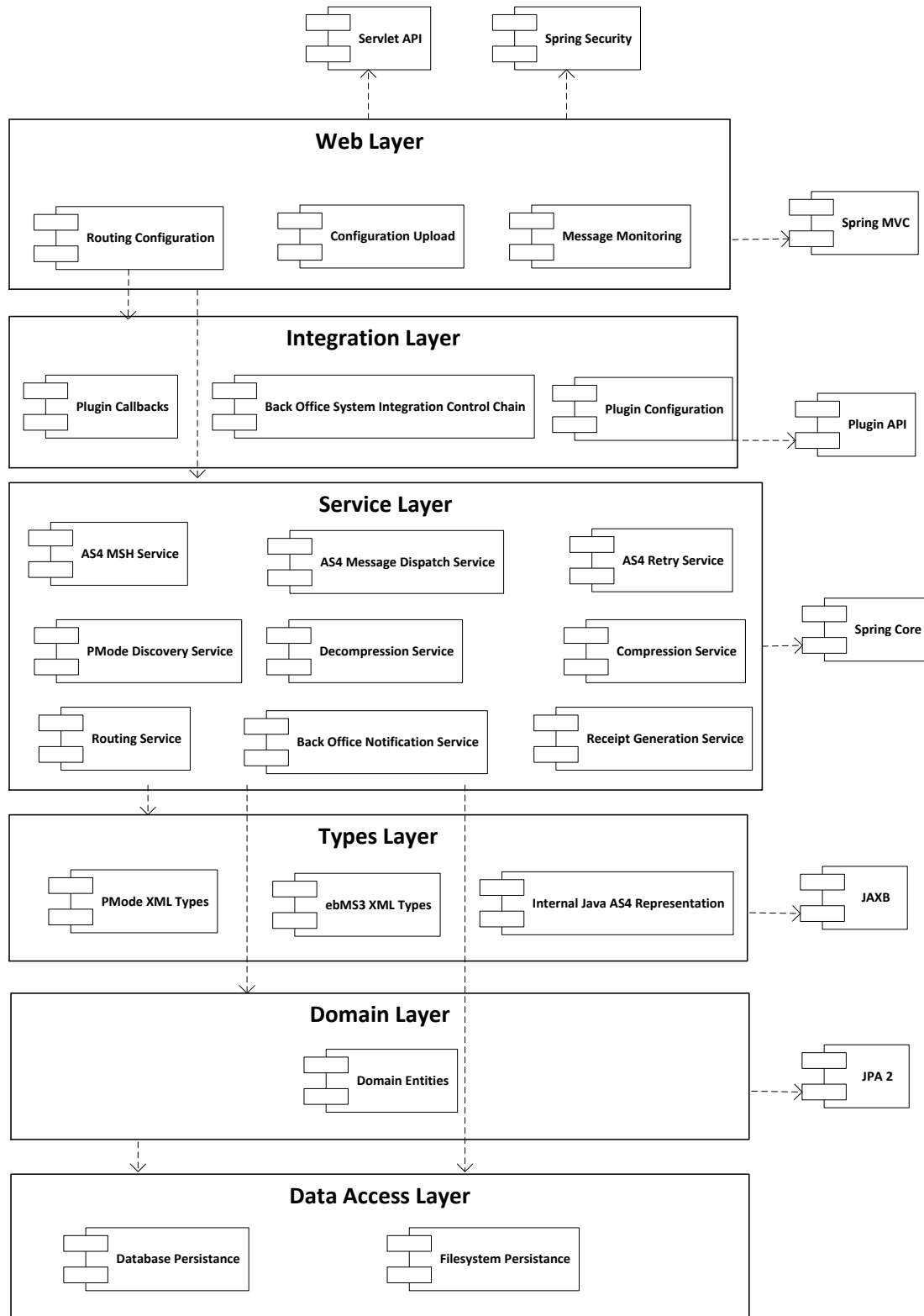
The **Services Layer** offers access to the domain objects of the platform as well as to the platform data layer. These services are Plain Old Java Objects relying on the Spring framework for dependency injection and for transaction management.

The **Types Layer** contains all the java objects generated from the XSDs used by the platform. These are JAXB generated objects.

The **Domain Layer** holds all the platform entities. The persistence of these entities is implemented using the Java Persistence API version 2.0.

Finally, the **Data Persistence** relies on the database and the file system to persist the data. The file system is used to store configuration data and the database to persist the incoming and outgoing messages.

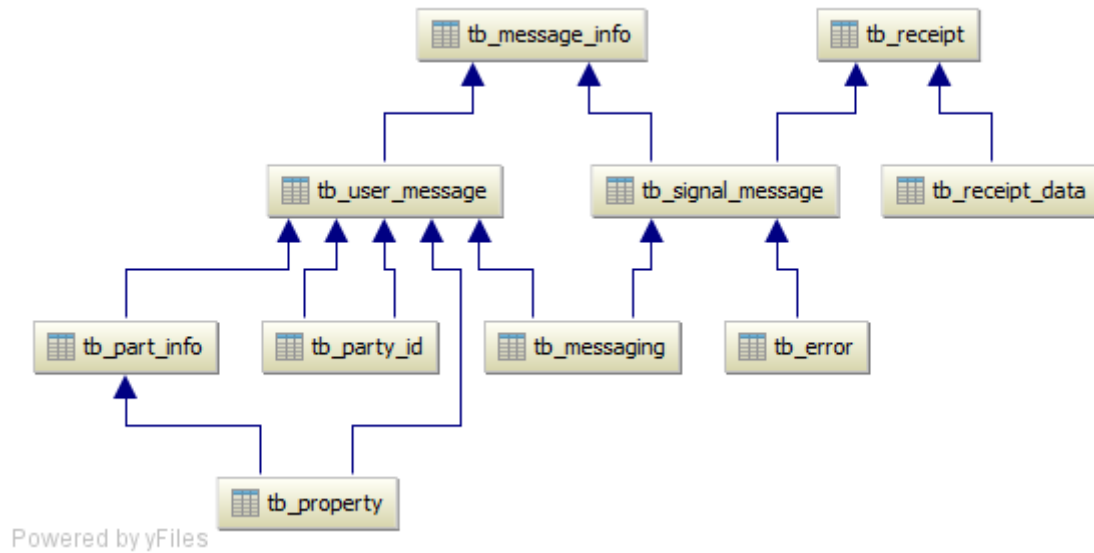
All these layers run on a Java Servlet Container.



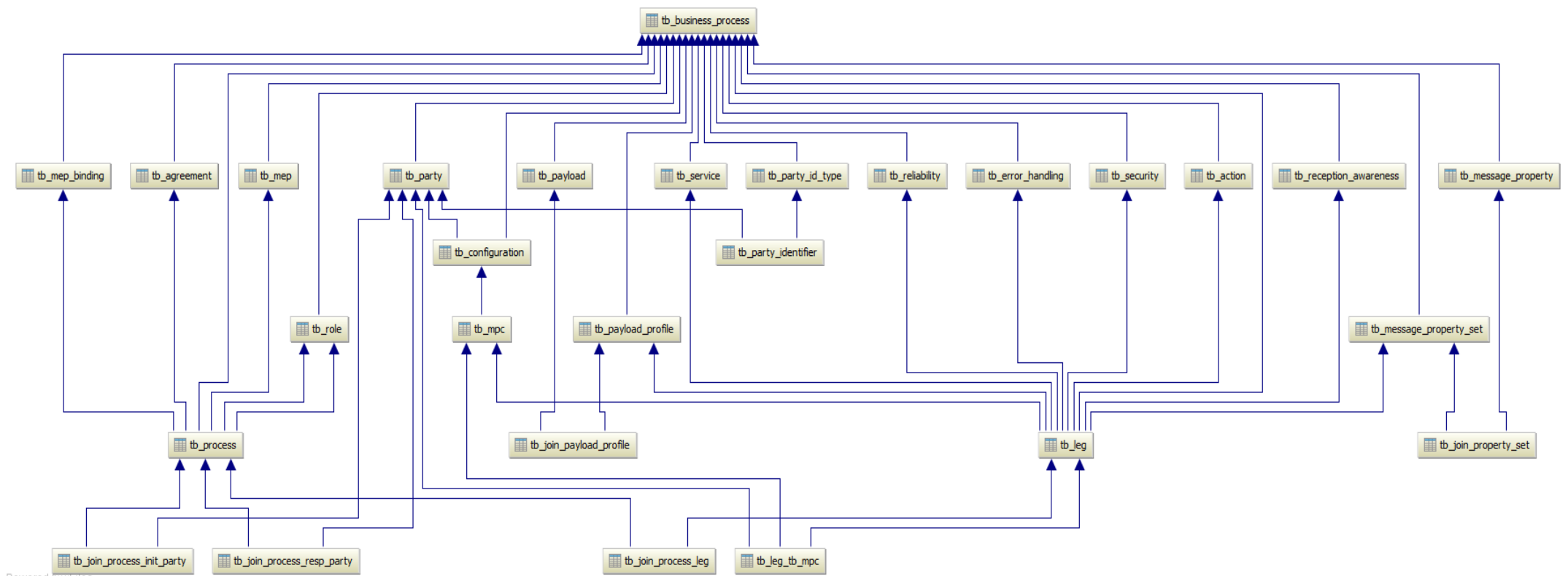
## 9. DATA VIEW

### 9.1. Data Model

The following diagrams show a high-level abstraction of the data entities, which must be implemented by the system:

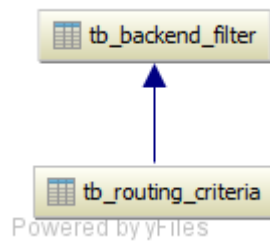


The above tables represent a 1:1 mapping of the ebMS3 XSD to database tables.



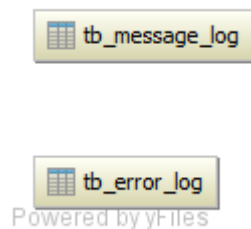
Powered by yFiles

The above tables represent a 1:1 mapping of the PMode configuration XSD to database tables.



Routing criteria contains the data that are needed to perform the routing of the messages to a specific plugin implementation.

Backend filters are collections of routing criteria associated with a specific backend representation.



The TB\_MESSAGE\_LOG table contains information about the User Messages and the Signal Messages (both sent and received ones). The stored values are the following:

MESSAGE\_ID, MESSAGE\_STATUS, MESSAGE\_TYPE, MPC, MSH\_ROLE, NEXT\_ATTEMPT, NOTIFICATION\_STATUS, RECEIVED, SEND\_ATTEMPTS, SEND\_ATTEMPTS\_MAX, BACKEND, ENDPOINT, DELETED

The TB\_ERROR\_LOG table contains information of the errors occurred during message transmission. The stored values are the following:

ERROR\_CODE, ERROR\_DETAIL, ERROR\_SIGNAL\_MESSAGE\_ID, MESSAGE\_IN\_ERROR\_ID, MSH\_ROLE, NOTIFIED, TIME\_STAMP

### 9.1.1. Data Auditing

The database tables contain information which provide audit information about their entries including the name of the user who created or last updated a particular entry or about the creation time or the last update time of a particular entry. The stored values are the following:

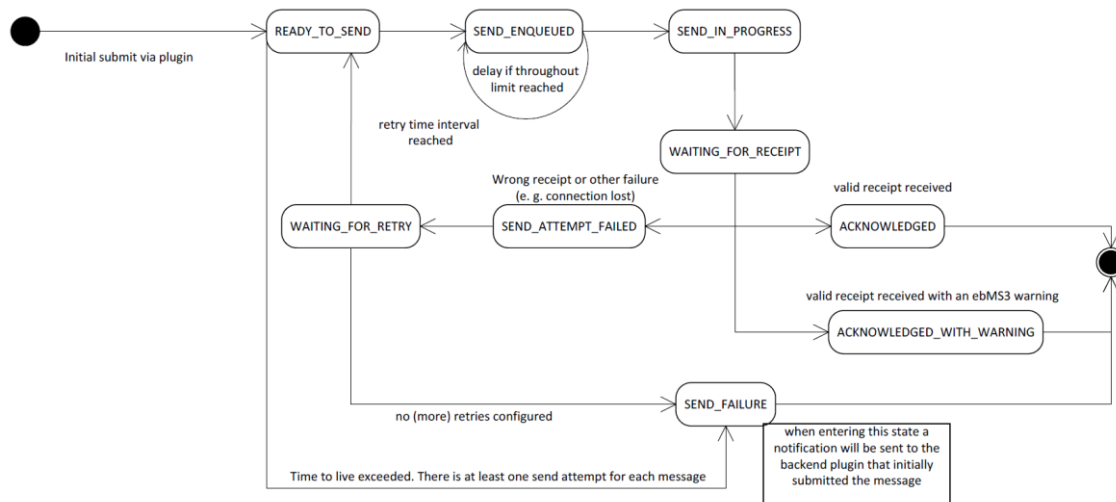
CREATED\_BY, MODIFIED\_BY, CREATION\_TIME, MODIFICATION\_TIME

These values are not visible to the Domibus user and can be only inspected at the database level. Data created or updated by the Domibus users will use their user names for the CREATED\_BY and MODIFIED\_BY columns. Data created using plugin users will use their plugin user names for the CREATED\_BY and MODIFIED\_BY columns. The rest of the entries (e.g. created during the invocation of an asynchronous JMS listener) will use the user name used to connect to the database for MySQL or the Oracle user schema for the CREATED\_BY and MODIFIED\_BY columns. There is one exception involving reference data (i.e. data that has to exist before the application can be used) on MySQL where we use the value 'DOMIBUS' for the CREATED\_BY and MODIFIED\_BY columns.

## 9.2. State Machines

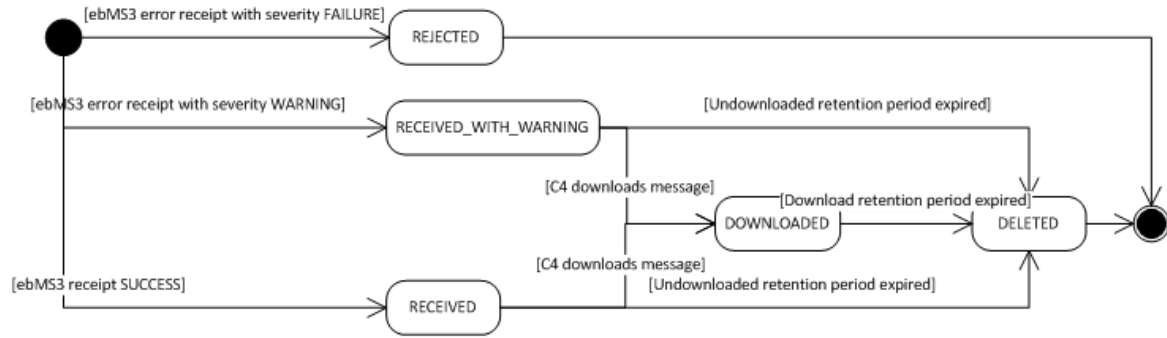
### 9.2.1. Outgoing Message State Machine

The outgoing messages have the following state machine:



### 9.2.2. Incoming Message State Machine

The incoming messages have the following state machine:





## 10. SIZE AND PERFORMANCE

### 10.1. Size

Size restrictions applied on the data that is exchanged by the back office systems, but not on the application or its components themselves, have an impact on the architecture and on the configuration of the system.

To support the exchange of large binary files, the plugin API supports payload submission by reference, meaning that Domibus is able to download a payload from a given URI. Additionally payloads can be stored on the file system instead of the database to avoid the processing of huge blobs.

As the eDelivery AS4 profile provides no provisions for ebMS large file handling (split/join) the transfer of data is limited by bandwidth and memory constraints.

Extra restrictions can be implemented via the business process PModes. These restrictions concern the maximum size of a payload and the maximum number of payloads in a message.

### 10.2. Performance

An important architectural decision that benefits the performance of Domibus includes the decoupling of the solution into corner 1/4 representing the back office systems and corner 2/3 representing the Domibus Access Point.

The back office systems (corner1/4) interact with the Domibus MSH (corner 2/3) via the interfaces (web services, JMS, REST, etc.) exposed by the plugins deployed on the Domibus MSH side.

Domibus MSH is using internally JMS queues to perform the processing of the messages coming from the back office systems via the plugins or from other access points.

All this architectural decisions lead to an improved throughput and load distribution of the messages.

## 11. QUALITY

The architecture of Domibus contributes to improve extensibility, reliability and portability.

### 11.1. Extensibility

Domibus is designed in a layered fashion and consists of multiple interconnected modules. This modular design facilitates the upgrades by replacing existing modules and extensions by adding additional modules.

### 11.2. Reliability

The reliability of Domibus is enhanced through the decoupling of each architectural layer by JMS queues. A store and forward mechanism and automatic retry policy ensures that parts of the system can continue functioning without losing data when an issue occurs in a specific component.

### 11.3. Portability

Currently the application can be deployed on Tomcat, WebLogic and WildFly and can connect to Oracle and MySQL databases.

With minor changes, it might be deployed on any Java Servlet 3.0-compliant server and it might connect to any RDBMS (Relational Database Management System).

Besides being extensible, Domibus is carefully designed in such a way that it is independent of the specific external system that communicates with. The use of a generic plugin API leaves the different layers unaffected when an additional external systems need to be supported by Domibus.

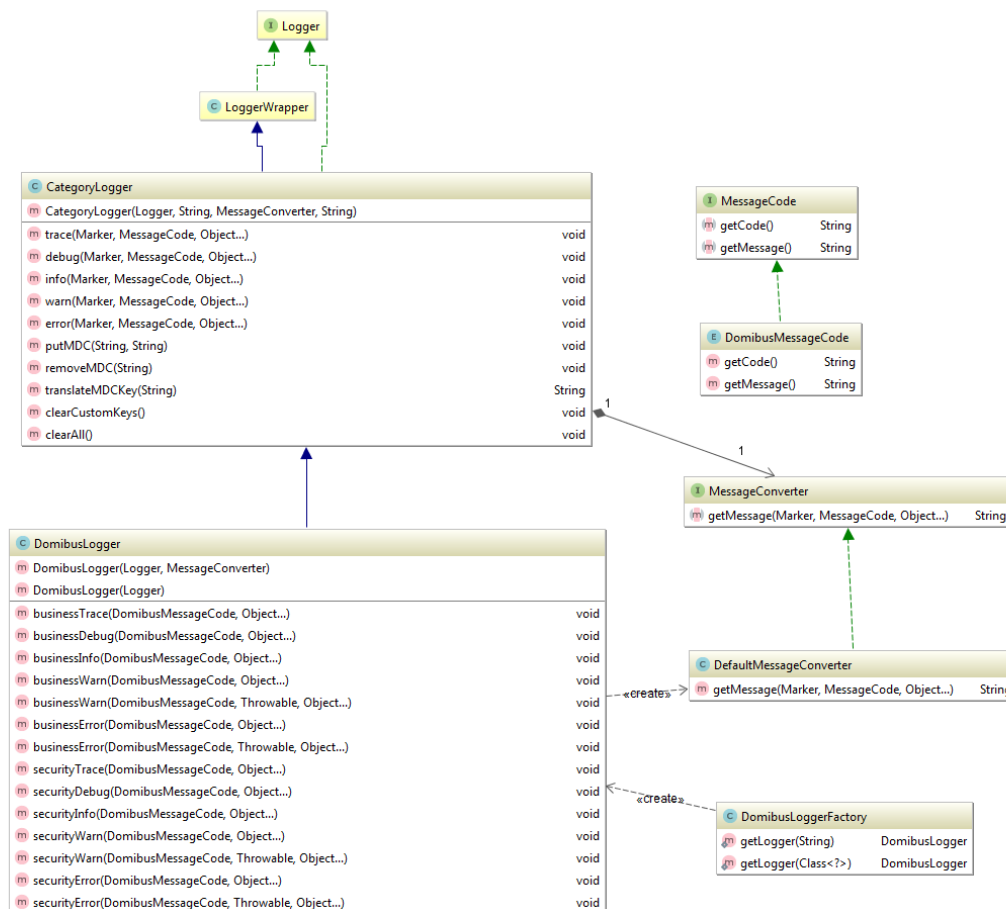
The usage of JPA to access the database makes it easy for implementers to change the relational database used to store the platform data.

## 12. LOGGING

### 12.1. Implementation

The logging framework used by Domibus is SLF4J API together with Logback as the SLF4j implementation.

The *domibus-logging* module provides the custom SLF4J logger *DomibusLogger*. This logger must be used for all the logs within the Domibus application.



There are three types of logs: security logs, business logs and miscellaneous logs. Each log category has its own marker defined in the *DomibusLogger* class. By default, each category will be logged in a separate file:

- **domibus-security.log** : This log file contains all the security related information. For example, you can find information about the clients who connect to the application.
- **domibus-business.log**: This log file contains all the business related information. For example, when a message is sent or received, etc.
- **domibus.log** : This log file contains both the security and business logs plus miscellaneous logs like debug information, logs from one of the framework used by the application, etc.

The security and business logs require a code that is defined in the *DomibusMessageCode* class.

The logs pattern is defined in the *logback.xml* file. The default pattern is:

```
%d{ISO8601} [%X{d_user}] [%X{d_messageId}] %5p %c{1}:%L - %m%n
```

- *d\_user*: The authenticated user.
- *d\_messageId*: The message id currently being sent/received.

The values for the *d\_user* and *d\_messageId* properties can be set by calling the method *DomibusLogger.putMDC(String key, String value)*. The prefix *d\_* is added automatically by the *DomibusLogger* in order to easily identify the Domibus specific MDC properties.

Eg:

```
LOGGER.putMDC(DomibusLogger.MDC_USER, authenticationResult.getName());
```

The MDC values need to be always cleaned after the thread execution. Otherwise, the thread might be returned back to the thread pool with previously set MDC values and on the next thread execution, the old MDC values will be used.

In order to easily clear the MDC values after a method execution a custom annotation, *MDCKey*, has been created in order to mark a method that is setting values in the MDC. An AOP aspect is detecting the methods annotated with the *MDCKey* annotation and after the execution of the method it is clearing the MDC values.

Eg:

```
@MDCKey(DomibusLogger.MDC_MESSAGE_ID)
public String submit(final Submission messageData, final String backendName)
```

## 12.2. Domibus log codes

| Category | Event code | Description  |
|----------|------------|--|
| SECURITY | SEC-001    | Unsecure login is allowed, no authentication will be performed |
| SECURITY | SEC-002    | Basic authentication is used                                   |
| SECURITY | SEC-003    | X509Certificate authentication is used                         |
| SECURITY | SEC-004    | Blue coat authentication is used                               |
| SECURITY | SEC-005    | The host [{}] attempted to access [{}]                         |

|                 |         |   |
|-----------------|---------|---|
| <b>SECURITY</b> | SEC-006 | The host [{}] has been granted access to [{}] with roles [{}]   |
| <b>SECURITY</b> | SEC-007 | The host [{}] has been refused access to [{}]   |
| <b>SECURITY</b> | SEC-008 | Certificate is not valid at the current date [{}]. Certificate valid from [{}] to [{}]                      |
| <b>SECURITY</b> | SEC-009 | Certificate is not yet valid at the current date [{}]. Certificate valid from [{}] to [{}]                  |
| <b>SECURITY</b> | SEC-010 | No security policy (intended for testing alone) is used. Security certificate validations will be bypassed! |
| <b>SECURITY</b> | SEC-011 | User [{}] is trying to access a message having final recipient: [{}]  |
| <b>SECURITY</b> | SEC-012 | X509Certificate invalid or not found  |
| <b>SECURITY</b> | SEC-013 | The user [{}] is unknown  |
| <b>SECURITY</b> | SEC-014 | The user [{}] is not active   |
| <b>SECURITY</b> | SEC-015 | The user [{}] is suspended  |
| <b>SECURITY</b> | SEC-016 | The user [{}] is trying to login with bad credentials   |
| <b>SECURITY</b> | SEC-017 | The user [{}] is locked after trying to login for [{}] wrong attempts.                                      |
| <b>SECURITY</b> | SEC-018 | The certificate with alias [{}] will be revoked on [{}]   |
| <b>SECURITY</b> | SEC-019 | The certificate with alias [{}] is revoked since [{}]   |
| <b>SECURITY</b> | SEC-020 | The password for user [{}] will expire on [{}]  |
| <b>SECURITY</b> | SEC-021 | The password for user [{}] expired on [{}]  |
| <b>BUSINESS</b> | BUS-001 | Message successfully received   |

|                 |         |   |
|-----------------|---------|---|
| <b>BUSINESS</b> | BUS-002 | Failed to receive message   |
| <b>BUSINESS</b> | BUS-003 | Failed to validate message  |
| <b>BUSINESS</b> | BUS-004 | Failed to notify backend for incoming message   |
| <b>BUSINESS</b> | BUS-005 | Invalid charset [{}] used   |
| <b>BUSINESS</b> | BUS-006 | Invalid NonRepudiationInformation: no security header found                                     |
| <b>BUSINESS</b> | BUS-007 | Invalid NonRepudiationInformation: multiple security headers found                              |
| <b>BUSINESS</b> | BUS-008 | Invalid NonRepudiationInformation: eb:Messaging not signed                                      |
| <b>BUSINESS</b> | BUS-009 | Invalid NonRepudiationInformation: non repudiation information and request message do not match |
| <b>BUSINESS</b> | BUS-010 | There is no content inside the receipt element received by the responding gateway               |
| <b>BUSINESS</b> | BUS-011 | Reliability check failed, check your configuration  |
| <b>BUSINESS</b> | BUS-012 | Reliability check was successful  |
| <b>BUSINESS</b> | BUS-013 | Compression failure: no mime type found for payload with cid [{}]                               |
| <b>BUSINESS</b> | BUS-014 | Error compressing payload with cid [{}]   |
| <b>BUSINESS</b> | BUS-015 | Payload with cid [{}] has been compressed   |
| <b>BUSINESS</b> | BUS-016 | Decompression failure: no mime type found for payload with cid [{}]                             |
| <b>BUSINESS</b> | BUS-017 | Payload with cid [{}] will be decompressed  |
| <b>BUSINESS</b> | BUS-018 | Decompression is not performed: leg compressPayloads  |

|                 |         |   |
|-----------------|---------|---|
|                 |         | parameter is false  |
| <b>BUSINESS</b> | BUS-019 | Decompression is not performed: partInfo with cid [{}] is in body   |
| <b>BUSINESS</b> | BUS-020 | Message action [{}] found for value [{}]  |
| <b>BUSINESS</b> | BUS-021 | Message action not found for value [{}]   |
| <b>BUSINESS</b> | BUS-022 | Message agreement [{}] found for value [{}]   |
| <b>BUSINESS</b> | BUS-023 | Message agreement not found for value [{}]  |
| <b>BUSINESS</b> | BUS-024 | Party id [{}] found for value [{}]  |
| <b>BUSINESS</b> | BUS-025 | Party id not found for value [{}]   |
| <b>BUSINESS</b> | BUS-026 | Party [{}] is not a valid URI [CORE] 5.2.2.3  |
| <b>BUSINESS</b> | BUS-027 | Message service [{}] found for value [{}]   |
| <b>BUSINESS</b> | BUS-028 | Message service not found for value [{}]  |
| <b>BUSINESS</b> | BUS-029 | Message service [{}] is not a valid URI [CORE] 5.2.2.8  |
| <b>BUSINESS</b> | BUS-030 | Leg name found [{}] for agreement [{}], senderParty [{}], receiverParty [{}], service [{}] and action [{}]  |
| <b>BUSINESS</b> | BUS-031 | Matching Process or Leg not found for agreement [{}], senderParty [{}], receiverParty [{}], service [{}] and action [{}].<br><br>Process mismatch details:[{}].<br><br>Leg mismatch details:[{}]. |
| <b>BUSINESS</b> | BUS-032 | Preparing to send message   |
| <b>BUSINESS</b> | BUS-033 | Message sent successfully   |

|                 |         |  |
|-----------------|---------|--|
| <b>BUSINESS</b> | BUS-034 | Message send failure   |
| <b>BUSINESS</b> | BUS-035 | No Attachment found for cid [{}]   |
| <b>BUSINESS</b> | BUS-036 | More than one Partinfo referencing the soap body found   |
| <b>BUSINESS</b> | BUS-037 | Payload profile validation skipped: payload profile is not defined for leg [{}]                    |
| <b>BUSINESS</b> | BUS-038 | Payload profiling for this exchange does not include a payload with CID [{}]                       |
| <b>BUSINESS</b> | BUS-039 | Payload profiling for this exchange requires all message parts to declare a MimeType property [{}] |
| <b>BUSINESS</b> | BUS-040 | Payload profiling error, missing payload [{}]  |
| <b>BUSINESS</b> | BUS-041 | Payload profile [{}] validated   |
| <b>BUSINESS</b> | BUS-042 | Property profile validation skipped: property profile is not defined for leg [{}]                  |
| <b>BUSINESS</b> | BUS-043 | Property profiling for this exchange does not include a property named [{}]                        |
| <b>BUSINESS</b> | BUS-044 | Property profile [{}] validated  |
| <b>BUSINESS</b> | BUS-045 | Message persisted  |
| <b>BUSINESS</b> | BUS-046 | Message receipt generated with nonRepudiation value [{}]   |
| <b>BUSINESS</b> | BUS-047 | Message receipt generation failure   |
| <b>BUSINESS</b> | BUS-048 | Message status updated to [{}]   |
| <b>BUSINESS</b> | BUS-049 | All payloads data for user message [{}] have been cleared  |
| <b>BUSINESS</b> | BUS-050 | Security policy [{}] was not found for outgoing message  |



|                 |         |  |
|-----------------|---------|--|
| <b>BUSINESS</b> | BUS-051 | Security policy [{}] is used for outgoing message                                |
| <b>BUSINESS</b> | BUS-052 | Security algorithm [{}] is used for outgoing message                             |
| <b>BUSINESS</b> | BUS-053 | Security algorithm [{}] is used for incoming message                             |
| <b>BUSINESS</b> | BUS-054 | Security encryption username [{}] is used for outgoing message                   |
| <b>BUSINESS</b> | BUS-055 | Security policy [{}] for incoming message was not found                          |
| <b>BUSINESS</b> | BUS-056 | Security policy [{}] for incoming message is used                                |
| <b>BUSINESS</b> | BUS-057 | No Role with value [{}] has been found   |
| <b>BUSINESS</b> | BUS-058 | Party with name [{}] has not been found  |
| <b>BUSINESS</b> | BUS-059 | Message with id [{}] has not been found  |
| <b>BUSINESS</b> | BUS-060 | Message with id [{}] has been consumed from the queue [{}]                       |
| <b>BUSINESS</b> | BUS-061 | Received payload with cid [{}] for message [{}] of size [{}] (in bytes)          |
| <b>BUSINESS</b> | BUS-062 | Saved payload with cid [{}] for message [{}] of size [{}] (in bytes) for sending |
| <b>BUSINESS</b> | BUS-063 | Notifying about message status change from [{}] to [{}]                          |
| <b>BUSINESS</b> | BUS-064 | Message submitted  |
| <b>BUSINESS</b> | BUS-065 | Message submission failed  |
| <b>BUSINESS</b> | BUS-066 | Message retrieved  |
| <b>BUSINESS</b> | BUS-067 | Message retrieval failed   |
| <b>BUSINESS</b> | BUS-068 | Test message successfully received from [{}] to [{}]                             |

|                 |         |   |
|-----------------|---------|---|
| <b>BUSINESS</b> | BUS-069 | Failed to receive test message from [{}] to [{}]  |
| <b>BUSINESS</b> | BUS-070 | Preparing to send test message from [{}] to [{}]  |
| <b>BUSINESS</b> | BUS-071 | Test message sent successfully from [{}] to [{}]  |
| <b>BUSINESS</b> | BUS-072 | Test message sending from [{}] to [{}] failed   |
| <b>BUSINESS</b> | BUS-073 | Message property [{}] exceeds [{}] characters limit   |
| <b>BUSINESS</b> | BUS-074 | Receiver Party id [{}] found for value [{}]   |
| <b>BUSINESS</b> | BUS-075 | Receiver Party id not found for value [{}]  |
| <b>BUSINESS</b> | BUS-076 | Duplicate Message Property found for property name [{}]                                     |
| <b>BUSINESS</b> | BUS-077 | Payload size is greater than maximum size [{}] defined in payload profile [{}]              |
| <b>BUSINESS</b> | BUS-078 | Mandatory Message Header metadata [{}] is not provided                                      |
| <b>BUSINESS</b> | BUS-079 | Value of [{}] is too long (over 255 characters). Value provided: [{}]                       |
| <b>BUSINESS</b> | BUS-080 | Value of [{}] does not conform to the required MessageIdPattern: [{}]. Value provided: [{}] |
| <b>BUSINESS</b> | BUS-081 | Message with id [{}] already exists. Message identifiers must be unique                     |

## 13. CACHING

In order to enhance the performance domibus uses caching in specific areas of the application:

- caching of security policies
- caching of backend filter configuration
- caching of pmodes, when using the “CachingPModeProvider”

This is the default configuration of cache that defines the following properties:

```
maxBytesLocalHeap = 5m  
timeToLiveSeconds = 3600  
overflowToDisk= false
```

## 14. MULTITENANCY

### 14.1. General

There were multiple options to choose from to support Multitenancy:

1. Selected option: **One Schema per tenant**: tenant's data is saved in the same database for all tenants but in different schemas. When a new tenant needs to be added a new related DB schema is created in the same database instance. It is easier to add new tenants comparing with the **DB per tenant** approach, as the same connection pool can be reused. Switching between tenants is performed centrally by selecting the DB schema related to the tenant. A huge advantage of this approach is that the application code impact is limited compared to the **Discriminator field** approach described below.
2. **One DB per tenant**: each tenant has its own separate database. This is the highest level of isolation, however it is complex and cumbersome to maintain. Whenever a new tenant has to be added a new database instance needs to be created, a new database connection pool also needs to be created in Domibus which points to the tenant database, etc...
3. **Discriminator field**: All tenants' data is saved on common tables, and each table holds a discriminator field to distinguish data from each tenant. This approach has quite some disadvantages: no physical isolation of data between tenants (a bug in the application might leak between tenants), performance decrease as the data for all the tenants are saved into the same tables (resulting in bigger tables and more complex/heavier queries), and significant changes to the application code to take into account that discriminator field.

The solution that has been chosen to implement Multitenancy in Domibus is "One **Schema per tenant**" due its many advantages. Hibernate 5.0, already used in Domibus, comes by default with support for "One **Schema per tenant**" strategy, more info about Multitenancy in Hibernate [https://docs.jboss.org/hibernate/orm/5.0/userguide/html\\_single/chapters/multitenancy/MultiTenancy.html](https://docs.jboss.org/hibernate/orm/5.0/userguide/html_single/chapters/multitenancy/MultiTenancy.html) .

In the following document the term *tenant* is (the technical) synonym with the (more business-oriented) term *domain*.

### 14.1. Identifying the domain (tenant)

For every outgoing/incoming message, the related unique domain needs to be identified in order to use the configuration related to the appropriate domain (DB schema, PMode, keystore, truststore, Domibus properties, etc.).

**For outgoing messages**, sent by C2 to C3, the association to a specific domain is performed based on the Spring Security info available in the current thread after the authentication has been done by the plugins.

**For incoming messages**, received by C3 from C2, the association to a domain is based on an HTTP parameter ("domain") appended by C2 to the MSH endpoint of C3. In case the domain name sent by C2 is not defined in C3, an EBMS3 exception will be sent to C2.

**Example:**

Let us suppose that C3 exposes the MSH endpoint with URL:

<http://localhost:8080/domibus/service/msh>. Then C2 belonging to the domain **DIGIT** will call the MSH C3 endpoint using <http://localhost:8080/domibus/service/msh?domain=DIGIT>.

Please note that adding the HTTP parameter in the MSH endpoint is in-line with eDelivery AS4 specification.

#### **14.1.1. Selecting the database schema**

In Multitenancy mode, the database schema has to be configured per domain in the Domibus domain properties. More information on how to configure it please refer to the **Domibus Administration Console**.

### **14.2. User association to a domain**

When a user authenticates in the Admin Console, the domain is not yet identified and Domibus must find out which DB schema to select. In order to achieve this, a **general DB schema** is used. In this general DB schema, a table tells which user that has access to the Admin Console (defined in the **tb\_user** table) and to the domain he belongs to. This association is automatically updated by Domibus when users are added or removed. Therefore, a constraint has been added in Domibus: a username needs to be unique amongst the existing domains. The same mechanism and constraints applies to the **tb\_user** table and has been implemented for the table supporting plugins security: **tb\_authentication\_entry**.

### **14.3. UI**

#### **14.3.1. Managing multiple domains from the Domibus Administration Console**

All the screens from **Domibus Administration Console** have been adapted in order to support Multitenancy. This paragraph briefly summarizes these changes throughout the application.

The **Login page** does not require filling in the domain. Once the user is authenticated, Domibus automatically identifies its associated domain based on the association of the users to their domain contained in the general schema. For more information how this mechanism works please check **14.1 Identifying the domain (tenant)** section.

There is a new **super** admin user for the Administration Console that has access to all domains' data but only one domain at a time. This solution has been chosen in order to simplify the user interface. In addition, the **super** admin user is responsible to manage **admin** users for every domain and is the only one authorized to do so.

### 14.3.2. Security

The UI is communicating with the Domibus backend via REST resources.

The UI REST resources are protected so that users belonging to domain **A** are forbidden to modify the configuration belonging to any other domain. This is implemented with an interceptor acting on the all the UI REST resources that automatically identify the DB schema associated to the logged in user (please check the **14.1.1 Selecting the database schema** section for more details). Using this strategy, a user belonging to domain **A** is not able to access the data of any other domain.

## 14.4. Plugins

The introduction of Multitenancy has an impact on how the plugins manage the incoming/outgoing messages.

**For outgoing messages**, C1 to C2, the plugins need to authenticate first so that Domibus can identify the domain of the user and treat the message accordingly.

Domibus identifies the associated domain of the user based on the Spring Security information from the current thread (for instance the logged in user id) and the users configuration in table **tb\_authentication\_entry**. As a result, it is mandatory for C1 to authenticate itself so that Domibus is able to determine the domain related to the authenticated user. It is possible for the same C1 to send messages to different domains C1 needs to authenticate with different user credentials

**For incoming messages**, e.g. from C3 to C4, the plugins have to segregate the messages based on the domain name received from Domibus and deliver to C4 only the messages associated to the C4's domain.

The changes implemented in the Default Plugin for Multitenancy are described in the following sections.

### 14.4.1. Security

The plugins security configuration is stored in database table **tb\_authentication\_entry**. As every domain has its own separate schema, the table **tb\_authentication\_entry** will contain entries specific to each domain.

| ID_PK | CERTIFICATE_ID                              | USERNAME | PASSWD                                     | AUTH_ROLES | ORIGINAL_USER                                      | BACKEND |
|-------|---|----------|--|------------|--|---------|
| 1     | NULL  | admin    | \$2a\$10\$HApapHvDSiTEwjneMCvXuqUKVyyeX... | ROLE_ADMIN | NULL   | NULL    |
| 2     | NULL  | user     | \$2a\$10\$HApapHvDSiTEwjneMCvXuqUKVyyeX... | ROLE_USER  | urn:oasis:names:tc:ebcore:partyid-type:unregist... | NULL    |
| 3     | CN=blue_gw,O=eDelivery,C=BE:103700358308... | NULL     | NULL                                       | ROLE_ADMIN | NULL   | NULL    |

#### Example of the data in tb\_authentication\_entry

As mentioned in section **14.1 Identifying the domain (tenant)** the **username** should be unique amongst all domains. Moreover, there is a table **tb\_user\_domain** in the general DB schema that maps all usernames defined in the **tb\_authentication\_entry** to one associated domain.

When multiple domains are configured in Domibus, the plugins security activates automatically overriding the value configured using the following property.

```
#To activate security set this to false  
domibus.auth.unsecureLoginAllowed=false
```

If Domibus is running only with one domain, the plugins security activation is optional.

#### **14.4.2. Plugin API**

As every domain has its own dedicate DB schema, there are little changes required in the **Plugin API**. The only change that is required is to include in the class **eu.domibus.plugin.Submission** a new field named **domain**. This way the plugins can select the domain for a specific message. This is specifically useful for the incoming messages, C3 to C4, when the plugins need to segregate messages and expose to C4 only messages that are intended to C4 domain.

#### **14.4.3. WS Plugin**

Security is already implemented in the WS Plugin using the **CustomAuthenticationInterceptor** and the **eu.domibus.ext.services.AuthenticationService**, which retrieves information from the DB table **tb\_authentication\_entry**. For the WS Plugin security, activation is mandatory in order to use Domibus with multiple domains.

The implementation of the WS Plugin has been changed to take into account the domain according with the general requirements stated in the **14.4 Plugins** section.

#### **14.4.4. JMS Plugin**

The JMS Plugin is implemented using 5 queues:

- One queue for outgoing messages, C1 to C2: **domibus.backend.jms.inQueue**
- One queue for incoming messages, C3 to C4: **domibus.backend.jms.outQueue**
- Three queues for reporting message statuses and errors:  
**domibus.backend.jms.replyQueue**, **domibus.backend.jms.errorNotifyConsumer**,  
**domibus.backend.jms.errorNotifyProducer**

C1 and C4 interact with the JMS Plugin by sending/receiving messages from queues mentioned above so the JMS Plugin does not really have control on the messages once they are put in a JMS queue.

In order to segregate the data between domains, the JMS Plugin needs to connect to queues dedicated to each domain. Therefore, every domain will have its own set of 4 queues mentioned above with the exception of the **domibus.backend.jms.inQueue**. The queue **domibus.backend.jms.inQueue** is common to all the domains but when sending message to Domibus, C1 needs to authenticate with specific domain credentials. This is needed to allow Domibus to associate the submitted message with a specific domain. The association of the JMS queues and the domain are be done in the **jms-plugin.properties** file.

In order to make the migration easier the existing queue names used by the JMS plugin and associated to the **default** domain will not be modified.

The following convention to prefix the JMS queues with the domain name must be used to associate the JMS queues to a specific domain in the **jms-plugin.properties** file:

***domain\_name.domibus.backend.jms.inQueue***

where ***domain\_name*** is the name of the domain.

**For outgoing messages**, C1 to C2, C1 sends JMS messages containing the credentials of a specific domain to the **IN** queue **domibus.backend.jms.inQueue**. The JMS Plugin reads the JMS message, performs the authentication using the credentials sent by C1 and determines the domain based on Spring Security information from the current thread.

**For incoming messages**, C3 to C4, the JMS Plugin receives the domain name from Domibus API and then sends the incoming message to the JMS **OUT** queue associated to the domain where C4 is listening to.

#### **14.4.5. FS Plugin**

The FS Plugin has been designed in such a way that it is already domain aware. Briefly, the domain concept is implemented in the FS Plugin as follows:

- A file system location is defined per domain, which is protected with username/password. The username/password credentials are defined per domain in the FS Plugin property file
- In order to send messages, a user  $\alpha$  belonging to domain A will copy the payloads to be "sent" directory in the file system location configured for domain A (the user  $\alpha$  must have access to the protected file location). A similar process is happening when user A wants to retrieve messages.

**For outgoing messages** (C1 to C2), the FS Plugin authenticates itself using credentials (username/password) configured per FS Plugin domain. These new credentials are configured in the FS Plugin properties file. Once the user is authenticated, user information is extracted from the Spring Security data, associated to the current thread and passed to the Domibus Core.

**For incoming messages** (C3 to C4), the FS Plugin receives the domain name from Domibus so that the incoming messages are into the directory associated to the respective domain.

The domains configured in Domibus and the domains configured in the FS Plugin properties must match. An error will be raised if the domain is not configured as needed in the FS Plugin properties.

### **14.5. Domibus Properties**

The Domibus properties defined in the **domibus.properties** file are used for the **single** domain, when Domibus manages one single domain.

When Domibus is configured with multiple domains, several properties will have to be customized per domain. More information on which properties can be overridden per domain are available in the **Domibus Administration Guide**.

There are 3 types of properties in multitenancy mode:



1. Global/infrastructure - properties that have a meaning for the whole application and, as such, a single value
2. Domain - properties that can/should be customized for each domain. In case a value is not defined for a domain, it falls back to the one defined in global properties file (or an error is thrown in case the fallback is not allowed by the property metadata)
3. Super – properties applicable to super-users. Same behaviour as domain properties.

To distinguish between these types of properties, one needs to define a property **metadata** in the appropriate **metadata manager** (each module has its own property metadata manager). If a property does not have a metadata defined then it is treated as global.

In order to define a property, the following conventions are used:

| Property Type                   | File where it is defined          | Property name                                       |
|---------------------------------|-----------------------------------|---|
| Global/Infrastructure           | <b>domibus.properties</b>         | domibus.config.location                             |
| Domain property, domain1        | <b>domain1-domibus.properties</b> | <b>domain1</b> .domibus.security.keystore.location  |
| Domain property, default domain | <b>default-domibus.properties</b> | <b>default</b> .domibus.security.keystore.location  |
| Super property                  | <b>super-domibus.properties</b>   | <b>super</b> .domibus.console.login.maximum.attempt |

All common properties are defined in **core metadata manager**. The properties that are specific to a server (Tomcat, WildFly, WebLogic and WebLogic-ecas) are defined in a **specific metadata manager** like TomcatMetadataManager. All these properties are managed by the Domibus Property Provider.

These are considered as **internal properties**, as opposed to properties defined in **external modules** and **plugins** (DSS module, JmsPlugin). Each external module has also a **property manager** that gets and sets its own properties.

External modules can manage their properties by using their own property bag (as do default WS and FS plugins) or by delegating to the Domibus Property Provider bag (as do default JMS plugin and DSS module).

All property metadata, both internal and external, are managed centrally by the Domibus Property Provider.

The property metadata is used by the Domibus Property Provider to determine how and from where to get and set its value.

Domibus Property Provider is the single-entry point for getting and setting property values in MSH.

An external module can use its own property manager to do the same or it can call the Domibus Property Provider Delegate to do the same (as it manages all properties and knows how to route the call to the appropriate module manager).

## 14.6. Logging

In order to associate each log statement to a specific domain the **Logback** format pattern contains the domain name.

**Eg:** `<pattern>%d{ISO8601} [%X{d_user}] [%X{d_domain}] [%X{d_messageId}] %5p %c{1}:%L - %m%n</pattern>`

The domain name is added in the MDC context so that every log statement contains the domain name.

The domain name is added in the MDC context as soon as a thread is started:

- For a web service, a CXF interceptor is adding the domain to MDC as close as possible to the START phase. The MDC context value is cleared with a CXF interceptor added at before the END phase.
- For a JMS message listener, the domain name is extracted from the JMS message that is being consumed and added programmatically to MDC.

The separation of logs per domain is achieved using the existing **Logback** marker mechanism and a **Logback** configuration file distributed in each server configuration archive. As a result, separate log files are created containing only the logs for one domain. For instance for a domain named **DOMAIN1** the following log files are saved under the **logs/DOMAIN1** directory: **DOMAIN1-domibus.log**, **DOMAIN1-business.log**, **DOMAIN1-security.log** provided that the **DOMAIN1-logback.xml** is configured.

This configuration is managed in the Domibus **logback.xml** file and it is independent of the Domibus application.

For more detail on how to configure the Domibus logging can be found in the **Domibus Administration Guide**.

## 14.7. Message Payloads

Domibus supports two strategies for saving the messages payloads: in the database or in a local directory on the file disk. Each domain can customize the strategy for saving the payloads via the **domibus.properties** file.

In case a domain chooses to save the payloads in the database, the payloads segregation is ensured as only the users registered in that domain have access to the domain specific schema.

In case a domain chooses to save the payloads in a local filesystem directory configured per domain, the payloads segregation needs to be ensured via OS access rights. It is recommended that each domain configures its own dedicated filesystem directory.

## 14.8. Quartz

In the current version of Domibus, each domain can customize the Quartz jobs (like the retry job expression defined with the property **domibus.msh.retry.cron**). The Quartz jobs are saved in the database schemas of each domain. A **Quartz Scheduler** can only be configured to work with one DB schema at a time. In order to support Multitenancy, a **Quartz Scheduler** instance is created for each domain with specific properties for that domain. The creation of a Quartz Scheduler per domain is performed at runtime during the Domibus starts up.

## 15. UI REPLICATION MECHANISM

There have been situations when due to a large volume of data in the database message tables (from 100k to even 5M messages) the search in the Domibus GUI messages page takes longer than few seconds – up to 30 seconds.

The UI Replication mechanism consists in using a dedicated flat table (optimized with indexes for search) which is asynchronously populated when native message tables are populated. If the mechanism is enabled the search screen will use this table which should perform faster on large amount of data.

Below will follow description for main components.

### 15.1. TB\_MESSAGE\_UI table and V\_MESSAGE\_UI\_DIFF view

#### 15.1.1. TB\_MESSAGE\_UI

TB\_MESSAGE\_UI table is the main table which is asynchronously populated when UI replication is enabled. It has the following structure:

| Column name         | Data type (Oracle) |
|---------------------|--------------------|
| ID_PK               | NUMBER(38,0)       |
| MESSAGE_ID          | VARCHAR2(255 BYTE) |
| MESSAGE_STATUS      | VARCHAR2(255 BYTE) |
| NOTIFICATION_STATUS | VARCHAR2(255 BYTE) |
| MSH_ROLE            | VARCHAR2(255 BYTE) |
| MESSAGE_TYPE        | VARCHAR2(255 BYTE) |
| DELETED             | TIMESTAMP(6)       |
| RECEIVED            | TIMESTAMP(6)       |
| SEND_ATTEMPTS       | NUMBER(38,0)       |
| SEND_ATTEMPTS_MAX   | NUMBER(38,0)       |
| NEXT_ATTEMPT        | TIMESTAMP(6)       |
| CONVERSATION_ID     | VARCHAR2(255 BYTE) |
| FROM_ID             | VARCHAR2(255 BYTE) |
| TO_ID               | VARCHAR2(255 BYTE) |
| FROM_SCHEME         | VARCHAR2(255 BYTE) |
| TO_SCHEME           | VARCHAR2(255 BYTE) |
| REF_TO_MESSAGE_ID   | VARCHAR2(255       |

|                 |                       |
|-----------------|-----------------------|
|                 | BYTE)                 |
| FAILED          | TIMESTAMP(6)          |
| RESTORED        | TIMESTAMP(6)          |
| MESSAGE_SUBTYPE | VARCHAR2(255<br>BYTE) |
| LAST_MODIFIED   | TIMESTAMP(6)          |
| LAST_MODIFIED2  | TIMESTAMP(6)          |

Where ID\_PK is the generated sequence, LAST\_MODIFIED and LAST\_MODIFIED2 are columns dedicated for the mechanism of replication. All the other columns (from MESSAGE\_ID to MESSAGE\_SUBTYPE) are used for search on message page and populated with data from native tables.

### **15.1.2. V MESSAGE UI DIFF**

V\_MESSAGE\_UI\_DIFF is a control view. His purpose is to show in real time how many records from native tables are not in sync with TB\_MESSAGE\_UI – as this number is always 0 everything is in sync. Also this view is used for UIReplicationJob to update the TB\_MESSAGE\_U records not in sync.

| Column name         | Data type (Oracle) |
|---------------------|--------------------|
| MESSAGE_ID          | VARCHAR2(255)      |
| MESSAGE_STATUS      | VARCHAR2(255)      |
| NOTIFICATION_STATUS | VARCHAR2(255)      |
| MSH_ROLE            | VARCHAR2(255)      |
| MESSAGE_TYPE        | VARCHAR2(255)      |
| DELETED             | TIMESTAMP(6)       |
| RECEIVED            | TIMESTAMP(6)       |
| SEND_ATTEMPTS       | NUMBER             |
| SEND_ATTEMPTS_MAX   | NUMBER             |
| NEXT_ATTEMPT        | TIMESTAMP(6)       |
| CONVERSATION_ID     | VARCHAR2(255)      |
| FROM_ID             | VARCHAR2(255)      |
| TO_ID               | VARCHAR2(255)      |
| FROM_SCHEME         | VARCHAR2(255)      |
| TO_SCHEME           | VARCHAR2(255)      |
| REF_TO_MESSAGE_ID   | VARCHAR2(255)      |
| FAILED              | TIMESTAMP(6)       |
| RESTORED            | TIMESTAMP(6)       |
| MESSAGE_SUBTYPE     | VARCHAR2(255)      |

### **15.1.3. Native tables**

These tables are the source for populating TB\_MESSAGE\_UI and for the V\_MESSAGE\_UI\_DIFF view:

TB\_MESSAGE\_LOG

TB\_MESSAGE\_INFO

TB\_USER\_MESSAGE

TB\_PROPERTY

TB\_PARTY\_ID

TB\_MESSAGING

TB\_SIGNAL\_MESSAGE

## **15.2. UIReplication queue, JMS message producer and consumer**

There is a UIReplication JMS queue which is defined as internal queue

```
#Domibus internal queue used for UI replication  
domibus.jms.queue.ui.replication=domibus.internal.ui.replication.queue
```

The name of the queue could be overwritten as is defined in domibus-default.properties file

There is a producer defined for this JMS queue which will produce messages in the following situations:

- creation of a User or Signal message
- update of status, notification status and other fields of a User or Signal message

For this we create several types of JMS messages:

```
USER_MESSAGE_RECEIVED,  
USER_MESSAGE_SUBMITTED,  
MESSAGE_STATUS_CHANGE,  
MESSAGE_NOTIFICATION_STATUS_CHANGE,  
MESSAGE_CHANGE,  
  
SIGNAL_MESSAGE_SUBMITTED,  
SIGNAL_MESSAGE_RECEIVED
```

The consumer on the other hand is multi-thread (in order to speed up the replication process) and is able to insert or update a row into TB\_MESSAGE\_UI based on the type of JMS messages above. Also a type of Optimistic Lock mechanism based on LAST\_MODIFIED (status) and LAST\_MODIFIED2 (notification status) is in place which assures that only latest relevant information is updated or inserted.

The level of the multi-threading of the consumer is defined by this property from domibus-default.properties files:

```
#concurrency (no of threads) for dispatching messages of ui replication queue
domibus.ui.replication.queue.concurrency=3-10
```

### 15.3. UIReplication Quartz Job

The purpose of the job is to check regularly (once per day) any unsynchronized data between native tables and TB\_MESSAGE\_UI.

The frequency to run is defined in the following domibus-default.properties key:

```
#Cron job that will check unsynchronized data between native tables and
TB UI MESSAGE UI
domibus.ui.replication.sync.cron=0 0 2 * * ?
```

And it could be overridden in the domibus.properties if the user wants a different moment of time.

If there are more rows to be synchronized than the following property:

```
#max number of records that will be processed by cron job
domibus.ui.replication.sync.cron.max.rows=10000
```

Then the job will stop and issue a warning to use the REST method.

### 15.4. UIReplication REST methods

The purpose of the REST service is to offer a manual synchronization between the native tables and TB\_MESSAGE\_UI.

There are two methods:

GET /rest/ui replication/count – it will just count the differences

GET /rest/ui replication/sync?limit=x – this will sync the first x unsynchronized rows where x has a default value of 10.000

### 15.5. Migration script

A Migration script is intended to be run for both Oracle and MySQL database and is provided within distribution packages.

It performs an INSERT into TB\_MESSAGE\_UI and it should be run with the table having no records:

```
-- *****
-- This script should be run if UIReplication feature is enabled
-- ( before setting domibus.ui.replication.enabled=true).
--
--
```

```
-- *****
INSERT /*+ append*/ INTO tb_message_ui (
  id_pk,
  message_id,
  message_status,
  notification_status,
  msh_role,
  message_type,
  deleted,
  received,
  send_attempts,
  send_attempts_max,
  next_attempt,
  conversation_id,
  from_id,
  to_id,
  from_scheme,
  to_scheme,
  ref_to_message_id,
  failed,
  restored,
  message_subtype
)
SELECT
...
```

## 15.6. Enabling/disabling the UIReplication mechanism

There is a property defined into domibus-default.properties:

```
#enabled or disabled the UI Replication mechanism
domibus.ui.replication.enabled=false
```

The value set to false will disable:

- JMS consumer and producer
- UIReplication Job to run
- UIReplication REST methods – just to show a message and not to execute the sync

More information about configuring UIReplication mechanism could be found in the Admin Guide for Domibus.



## 16. CONTACT INFORMATION

eDelivery Support Team

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

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