Architecture Overview

Feasibility Study for the establishment of an Electronic Data Interchange for Waste Shipments

Date: 01/09/2014
Doc. Version: Final
This Report has been prepared by TRASYS S.A., member of the STRATIQO Consortium, for DG Environment of the European Commission under Specific Contract N° 009633-070307/2013/654373/ETU/A2 implementing Framework Contract DI/06772-00.

Authors: Dijana Spasojevic, Angelos Moschovinos, Constantinos Simatos, Margaritis Makatis
Contributors: Ioannis Oikonomou, Stylianos Gkorilas

The views express herein are those of the consultant alone and do not necessarily represent the official views of the European Commission.

The project team does not accept any liability for any direct or indirect damage resulting from the use of this report or its content.

Contact for this study: Dijana Spasojevic, Tel: +32 2 893 17 46; Fax: + 32 893 14 00;
Email: dijana.spasojevic@trasysgroup.com
TABLE OF CONTENTS

1 INTRODUCTION ........................................................................................................5
  1.1 Purpose .................................................................................................................. 5
  1.2 Scope ..................................................................................................................... 5
  1.3 Intended Audience ............................................................................................... 5
  1.4 Overview of the document .................................................................................... 5

2 INFORMATION SYSTEM DESCRIPTION ................................................................. 6
  2.1 Information System Position Statement ............................................................... 6
  2.2 Information System Perspective ......................................................................... 6
  2.3 Assumptions and Dependencies ......................................................................... 6
  2.4 Information System Requirements and Quality Ranges ..................................... 7
    2.4.1 Availability ..................................................................................................... 7
    2.4.2 Usability ......................................................................................................... 7
    2.4.3 Maintainability ............................................................................................... 7
    2.4.4 Applicable Standards ...................................................................................... 8
    2.4.5 System Requirements ..................................................................................... 8
    2.4.6 Performance Requirements ......................................................................... 8

3 COMPLIANCE ............................................................................................................. 8
  3.1 Security Compliance ............................................................................................ 8
    3.1.1 Security Statement .......................................................................................... 8
    3.1.2 Philosophy ...................................................................................................... 8
    3.1.3 Scope ............................................................................................................... 9
    3.1.4 Assumptions ................................................................................................... 9
    3.1.5 Alternative Security Designs ......................................................................... 9
    3.1.6 Mapping of Features to Requirements ......................................................... 9
  3.2 Document Management Compliance .................................................................. 9
  3.3 Data Protection Compliance .............................................................................. 9
  3.4 OLAF Compliance ............................................................................................. 9
  3.5 Constraints (Optional) ....................................................................................... 9

4 ARCHITECTURE OVERVIEW .................................................................................... 10
  4.1 Architectural Goals .............................................................................................. 10
  4.2 Architecture Decisions ....................................................................................... 11
    4.2.1 Architecturally Significant Requirements .................................................. 11
    4.2.2 Architectural Constraints ............................................................................. 11
    4.2.3 General Findings and Recommendations .................................................... 11
  4.2.3.1 Architectural Decision AD-001 – Overall architecture and topology .......... 12
  4.2.3.1.1 CENTRALIZED SYSTEM ................................................................. 12
  4.2.3.1.2 DECENTRALIZED SYSTEM ............................................................ 13
  4.2.3.1.3 HYBRID SYSTEM .............................................................................. 14
    4.2.3.1.3.1 Hybrid system – simplified central component call Central EU router 15
    4.2.3.1.3.2 Hybrid system – elaborate central components called central EU application 17
  4.2.3.1.4 SUMMARY .............................................................................................. 19
  4.2.3.2 Architectural Decision AD-002 – Digital signatures .................................... 20
  4.2.3.3 Architectural Decision AD-003 – Message format ........................................ 22
4.2.3.4 Architectural Decision AD-004 – Message exchange ....................................................... 24
4.2.3.5 Architectural Decision AD-005 – System to system communication channel ............... 25
4.2.3.6 Architectural Decision AD-006 – User to system communication channel ................. 26
4.2.3.7 Architectural Decision AD-007 – User authentication and authorization .................... 27
  4.3 Architecture Overview Diagram ....................................................................................... 29
  4.4 Key Concepts .................................................................................................................... 30
    4.4.1 Central EU application ............................................................................................... 30
    4.4.2 Shared MS application ............................................................................................... 31
5 RE-USABLE ARCHITECTURAL ASSETS ................................................................................. 32
APPENDIX 1: REFERENCES AND RELATED DOCUMENTS .................................................. 35
APPENDIX 2: HYBRID ARCHITECTURE ILLUSTRATIVE SCENARIO ................................. 36
1 INTRODUCTION

1.1 Purpose


Article 26 of the Regulation provides information on the submission of documents and information relating to how shipments of waste should be processed. The current process is mainly paper-based and requires considerable amount of resources. Most of the work involved in the process is also repeated by each of the involved participants and this makes the process unnecessarily slow and cumbersome.

A number of MS either have started or have developed an IT solution. However, existence of different IT systems among groups of Member States (MS) also creates an issue regarding the incompatibility and inconsistency between these solutions.

Additionally, a significant number of MS doesn’t have any solution in place for implementation of the WSR. The process is paper-based and creates significant administrative burden for both, the industry and the authorities.

This project creates an opportunity for the industry and Member States Competent Authorities (MSCA) to define an Electronic Data Interchange (EDI) format for data exchange between Member States and Industry and for data exchange between different Member States. Additionally, it creates an opportunity to have one common application for WSR for MS authorities not having any IT system for WSR in place.

1.2 Scope

The project scope is built around Article 26 of the Regulation and the possibility to exchange the information electronically. In terms of business processes, it covers the following:

- Notification process, from the moment of submission of the notification document and related documentation by the industry to the point of issuing consent by the MS competent authorities.
- Movement process in line with Article 16 of the regulation, including submission of the required documents by the industry and issuing of the consent by the MS competent authorities.
- Annex VII procedure with submission of the required documents by the industry.

Additionally, the project covers the exchange of documents between the industry and authorities, and the reporting obligations of the MS competent authorities.

This document complements the Project Charter and describes the possible architectural scenarios for a common IT system to be used by the Industry and MSCA. It also gives comparative analyses of two protocols\(^1\), EUDIN and e-TFS.

1.3 Intended Audience

Intended audience includes all relevant entities of the WSR together with private software companies.

1.4 Overview of the document

Document is organised in 5 sections:

First section, Introduction, describes the purpose, scope and intended audience of the document.
Second section, Information system descriptions, presents the statement, information system perspective, together with assumptions and dependencies.
Third section, Compliance, explains the security aspects of the information system.
Fourth section, Architectural overview, depicts different scenarios for a future information system with analysis of the specific topics, such as, digital signature, messages, communication channels, etc.
Fifth section, Re-usable architecture assets, indicates which ones would be used in the project.

---

\(^1\) In the context of this study, a protocol specifies interactions between the communicating entities.
2 INFORMATION SYSTEM DESCRIPTION

2.1 Information System Position Statement

<table>
<thead>
<tr>
<th>For</th>
<th>DG Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>who</td>
<td>needs to define a common Electronic Data Interchange (EDI) format to allow data exchange between the MSCA and industry, different MSCA and the Commission and MSCA</td>
</tr>
<tr>
<td>the Electronic Transboundary Waste Shipments System (e-TWSS)</td>
<td>Is an information system</td>
</tr>
<tr>
<td>that</td>
<td>will replace paper-based processes of the WSR and create a common EU-wide IT system for all relevant entities</td>
</tr>
<tr>
<td>unlike</td>
<td>existence of MS-specific IT systems that support some of the WSR processes exclusively for the shipments of waste within their respective national boundaries</td>
</tr>
<tr>
<td>our Information System</td>
<td>will allow existing MSCA IT systems to connect and exchange data directly and create a common application for MS not having any system in place. It will also facilitate MSCA reporting to the Commission.</td>
</tr>
</tbody>
</table>

2.2 Information System Perspective

The information system discussed as part of this study is expected to present a solution for Member States to apply the Waste Shipments Regulation (WSR). The alternative approaches to design such a system are discussed in section 4.2.3, however regardless of the one selected, the foreseen system is expected to be used by multiple parties in multiple participating Member States. Moreover, considering that Member States already have information systems in place to cover their national needs, it is expected that the discussed system will need to integrate with them allowing both national and transboundary waste movement processes to be supported. To support this integration, a communication protocol comprising of a message exchange format and communication channel setup will need to be established, the exact form of which will be defined by the topology of the eventual solution. This protocol and the interfaces defined to support this are elaborated in the subsections of section 4.2.3.

In order to fulfil its goals, the foreseen system will make use to the fullest possible extent existing work and solutions. One such reuse point concerns the initiatives launched up to now by groups of Member States providing different approaches to handle transboundary waste movements. These initiatives, discussed in 4.2.3.3, are currently implemented to varying degrees of maturity and offer proposals not only for the communication protocol to put in place but also on the philosophy of the solution as a whole. On the other hand, regardless of the approach selected, existing Commission assets will be investigated for reuse as much as possible, in order to separate concerns and employ tried and tested solutions. This will typically be the case for the system’s non-functional needs such as the authentication of users, as is further described in sections 4.2.3.7 and 5.

2.3 Assumptions and Dependencies

The functionality and processes that the foreseen system needs to support are based on the waste movement regulation and the user needs collected as part of this study. It is important to state the main points of these as assumptions to be true, since the supported processes have an impact on decisions relating to the system’s architecture and its communication protocol with national systems:

- The system needs to support the Notification, Movement and Annex VII processes for transboundary waste movement.
- The system is required to provide reporting features on transboundary waste movements in the form of predefined templates and waste movement statistics.
In addition, considering that the solution will involve both Member States that have existing IT solutions in place and others that do not, we assume that the following are true:

- The proposed solution needs to respect the investment made by certain Member States in existing national solutions and allow them to continue using them if needed. Moreover, any required changes to national systems should be as limited as possible and if possible transparent to their end users.
- The proposed solution needs to allow Member States, currently lacking a national IT solution for waste movement, to participate in the common system for transboundary movements. The investment from such Member States, apart from the organisation of the workshops and planning meetings, should be kept to a minimum.

Achieving the proposed system’s goals is possible through multiple candidate architectures that differ mainly in terms of topology, the existence of central EU applications and the possibility to adapt existing national IT systems. The possible alternatives are discussed in section 4.2.3.1 with the eventual choice largely dictating the subsequent decisions that need to be taken. Before formulating and considering these alternatives we need to make certain assumptions as to what is possible, specifically:

- Concerning the national IT systems for waste management that are in place, we assume that it is possible to have them modified, to a limited extent, in order to accommodate the needs of the pan-European solution. Any such modifications will be the responsibility of the respective Member States following the definition of the common EDI Protocol. In other words, apart from defining the EDI Protocol, the Commission will not need to implement itself changes to existing national systems.
- Considering that certain architecture alternatives may require the operation of Central EU application, we assume that the Commission is willing to centrally host and operate any such required applications (e.g. by DIGIT). If the Commission is not willing to do so, the available choices would be severely limited, resulting in a fully decentralized architecture relying only on national systems.

Additional information and assumptions on the system’s goals, main requirements and constraints are discussed in sections 4.1, 4.2.1 and 4.2.2.

2.4 Information System Requirements and Quality Ranges

The information in the current section provides currently guidelines based on the system’s expected requirements. Specific information such as availability percentages that will need to be considered cannot be determined at the present but will be elaborated as the vision of the solution matures.

2.4.1 Availability

The availability requirements for the envisaged system would be based on the topology of the system as well as the possibility to use alternative means to complete the system’s goals. Concerning the topology of the system, as discussed in section 4.2.3.1, the proposed approach is a hybrid solution containing both decentralized and centralized aspects. With this topology two centrally hosted applications are foreseen, a central EU application and a shared MS application, that require high availability considering their key role in the entire solution. Further elaboration on the specific availability percentages will be made once the solution matures.

2.4.2 Usability

In terms of usability, the system is foreseen to be used by a large user base across Member States, although not the general public. It should be easy to use and should include on-line help facilities (e.g. an online user manual). Concerning compatibility with web browsers, significant effort will be made to support a wide range of browsers and versions although it could be agreed explicitly with the system’s end users to exclude certain problematic cases. Examples of such exclusions could be outdated browser versions (e.g. Internet Explorer prior to version 8) and restrictions on the use of JavaScript. The possibility of these constraints will be elaborated and validated as the solution matures.

2.4.3 Maintainability

The system will be built in order to promote maximum maintainability, especially considering that it will need to interface with multiple external systems that are outside its control. To facilitate the maintainability goal, a rich configuration module will be foreseen through which all properties of the system that could be subject to change will be exposed as configuration elements. Moreover, this
configuration will be persisted in the system’s relational database thus allowing storing and looking up configuration values without requiring stopping and redeploying applications.

2.4.4 Applicable Standards

The envisaged system will be designed in order to comply with any standards required to support transboundary waste movements involving EU Member States. Relevant international standards, such as UN/EDIFACAT\(^2\) shall be taken into consideration. In terms of other European Commission specific standards relating to IT systems and IT project governance, it is too early to determine specific requirements. It can however be stated that compliance will be assured for any standards that are deemed necessary by the Commission once the solution matures.

2.4.5 System Requirements

The foreseen system will be built in compliance with the technology stack and platforms used by the Commission. Specifically the foreseen applications will be built on the Java Enterprise Edition (JEE) 6 platform, running on clustered Oracle WebLogic servers and using an Oracle 11g DB for persistence. Specific product versions to be used will be determined based on the support offered by DIGIT at the time of system elaboration. It is important to note at this stage that no special requirements or assumptions in terms of specific topologies or OS versions will be made. This will allow the envisaged applications to be deployed and operate on DIGIT’s infrastructure without problems.

2.4.6 Performance Requirements

It is currently premature to determine specific performance characteristics of the envisaged system. What can be safely assumed however that a large number of exchanged messages will need to be supported and that the foreseen centralized EU applications must not present a performance bottleneck to the entire solution. Expected volumes of processed messages, volume of concurrent users, as well as acceptable transaction processing times will be elaborated as the solution matures.

3 COMPLIANCE

3.1 Security Compliance

3.1.1 Security Statement

This section will be defined once the vision on the solution matures.

| Our Information System has a Confidentiality level | TBD |
| Our Information System has an Integrity level | TBD |
| Our Information System has an Availability level | TBD |
| Our Information System has a Security classification | TBD |

3.1.2 Philosophy

To elaborate the security philosophy behind the proposed solution one needs to consider the following:

- The envisaged topology
- The foreseen information exchange between systems and from end users to systems.
- The sensitivity of the data communicated and recorded in the system.

In terms of topology the system will comprise of a central EU application, a shared Member State application and remotely connected national Member State applications. The participation of remote

\(^2\) [http://www.unece.org/trade/untdid/welcome.html](http://www.unece.org/trade/untdid/welcome.html)
systems requires the exchange of messages with however the important point that all information is routed through a central EU application. The presence of this central EU application adds a degree of trust to the solution that effectively limits the need of using digital signatures in exchanged messages. What is important is that the communication channels between Member State applications and the central EU application is secured. This is foreseen to be achieved through the use of SSL for channel encryption and specifically through 2-way SSL to allow both participants to authenticate to each other through the presented server and client certificates. Finally, concerning the solution’s topology, the implementation of two distinct applications is foreseen, the central EU application and a shared Member State application, in order to separate concerns and restrict access to the more critical central node. More information on the proposed system’s topology is presented in 4.2.3.1.

In terms of user access, discussed in detail in 4.2.3.6 and 4.2.3.7, it is important to robustly establish the identity of end users and authorize their actions, while at the same time prevent access to exchanged data by malicious parties. This is achieved by authenticating users through ECAS with an SMS challenge as a 2nd authentication factor. The communication channel between authenticated users and the EU applications is foreseen to be encrypted using (1-way) SSL. In general, concerning the prevention of malicious access, the Industry standard best practices will be applied such as measures to address the OWASP top 10 vulnerabilities.

Specific security needs would also need to be determined based on the sensitivity of the data exchanged and recorded. Although the level of sensitivity can be deemed lower when comparing to e.g. banking systems, one can foresee malicious parties desiring to access communicated messages to facilitate fraudulent activities. The user authentication and authorization measures as well as the foreseen channel encryption serve to avoid such threats, however specific additional requirements can be foreseen if this is deemed appropriate by the Commission and involved Member State stakeholders.

3.1.3 Scope

To be defined.

3.1.4 Assumptions

To be defined.

3.1.5 Alternative Security Designs

To be defined.

3.1.6 Mapping of Features to Requirements

To be defined.

3.2 Document Management Compliance

In order to support transboundary waste movement processes the exchange of documents is indeed foreseen. It is however premature to define whether these documents will be exchanged through the system and whether they will be stored. If recording of documents becomes a requirement then the information on document management compliance will be elaborated and the reuse of existing Commission services such as HERMES will be investigated and most likely integrated into the solution.

3.3 Data Protection Compliance

User management for the envisaged system is foreseen to take place through ECAS. However, a certain amount of user information will need to be replicated or introduced into the system in order to facilitate its processes (e.g. the user’s email) and to allow user authorization (e.g. the link between usernames and roles). Once the solution is further elaborated and the requirements on user data replicated or introduced into the system mature, the information on data protection compliance will be further elaborated.

3.4 OLAF Compliance

Not applicable at this stage.

3.5 Constraints (Optional)

Not applicable at this stage.
4 ARCHITECTURE OVERVIEW

4.1 Architectural Goals

In order to state the goals of the proposed system’s architecture, one first needs to understand the high-level needs it is expected to fulfill and the context in which it will exist. In terms of needs, the Waste Shipments Regulation (WSR) has to be respected while at the same time the Industry, Competent Authority and Commission user needs, determined as part of this study, need to be catered for to the fullest extent possible. In addition, it is important to consider that the discussed system will exist in a landscape where certain Member States already have IT systems in place, used to implement their national regulatory needs, whereas others lack an existing solution or the resources to implement one. From these points one can derive the first clear goals of the system:

- Implement the WSR and fulfil user needs to the fullest extent possible.
- Provide a solution for Member States lacking an existing solution.
- Allow interoperability with existing Member State systems.

The next set of goals can be determined from the fact that the core of the system’s operations are Notification and Movement processes that require the communication of messages and documents between multiple parties. As such, specific goals relating to the communication aspects of the system need to be stated:

- Communication between participants needs to be secure, ensuring that no information can be obtained by unintended parties. In addition, recipients need to be able to trust that messages indeed originate from the claiming party.
- Communication needs to be reliable ensuring that a sending party has confirmation that his messages are received, especially in cases where multiple recipients are involved.
- Unexpected communication issues need to be handled gracefully without a negative impact on the system (e.g. repeated messages or technical failures in the delivery process).

The next set of goals can be derived through the inspection of non-functional goals common to most enterprise architectures, and their specific application to the current context:

- **Performance**: The system is expected to handle large numbers of messages in the form of Notification and Movement requests that would exceed observed volumes in existing national solutions. The system will need to ensure that it does not present a bottleneck and that its communication and reporting needs complete in a timely manner.
- **Scalability**: The system needs to be able to respond to fluctuations in communication volume and scale for peaks. An example would be that, considering the purpose of Movement requests, peaks could be witnessed in seasons with favourable weather and transport conditions.
- **Reliability**: The system must ensure that data integrity is not compromised and that processing and message delivery is transactional, even when load increases.
- **Availability**: Even though the current paper-based approach could be used if the system is rendered unavailable, the system should be designed to promote its availability. This would mean the introduction of redundancy and the presence of a disaster recovery system.
- **Extensibility**: Considering that the WSR could evolve over the time and that additional Member State needs may materialize, it is imperative that the proposed system allows easy extension to accommodate new requirements.
- **Manageability**: Considering that the proposed system will effectively orchestrate communication between numerous Industry and Authority parties, it is imperative that it offers facilities for health and quality monitoring and allows easy configuration, such as in the case of including additional participants.
- **Security**: Extending the earlier stated goal of secure communications, the system needs to ensure that all users are authenticated and authorized (including end-users and integrating IT systems) and that the best practices on prevention of malicious access are incorporated into its design.
4.2 Architecture Decisions

4.2.1 Architecturally Significant Requirements

The requirements that drive the system’s architecture originate from the WSR that defines the core processes that need to be supported, and the Industry and Competent Authority (CA) needs as collected through the current study. In addition, the approach followed by existing solutions or proposals needs to be considered in order to identify elements that would be important for the envisaged system.

Taking into account these sources, the following key requirements can be formulated:

- Support of the Notification, Movement and Annex VII processes. These require the exchange of messages between Notifiers, Consignees and appropriate CAs and the possibility to track their status.
- Messages pertinent to the supported processes (e.g. Notification request) and user input that supports them (e.g. a CA’s consent or its withdrawal) need to be created and communicated securely, reliably and with specific acknowledgements.
- Verification of messages entails first a technical validation (e.g. ensuring that specific formats are respected) and then the appropriate business action per-case (e.g. a CA’s provision of consent). Acknowledgement of messages should be automatic following technical acceptance.
- A common format for all transboundary message exchange needs to be used between all participants. To the extent possible this format and its principles should be based on existing Member State initiatives and solutions.
- The system is required to provide reporting features on transboundary waste movements, in the form of defined templates and to allow extraction of statistics (e.g. amount of notifications per year)\(^3\).
- Users of the system need to be authenticated and authorized using a common standard approach. This entails both authentication of external IT systems integrating with the proposed system as well as the authentication of end-users.

4.2.2 Architectural Constraints

The main constraint for the system’s architecture comes from the fact that both Member States with and without an existing IT solution need to be supported. In addition Member States without an existing solution often lack the resources required to put such a system in place. On the other hand existing Member State solutions typically implement national regulations that need to be respected. As such the following main constraints need to be considered:

- The investment required by Member States that lack a current IT solution and that are not planning to put one in place must be kept at a minimum. Ideally, such Member States should be provided with a solution for transboundary waste movement that works “out of the box”.
- The system should not impose significant changes on existing Member States’ IT solutions and should not hinder these in the implementation of their national waste movement regulations.
- The system should offer realistic means to fulfil centralized reporting needs on transboundary waste movements taking into account performance and minimizing the impact on Member States’ systems.

4.2.3 General Findings and Recommendations

The decisions taken to define the proposed system’s architecture are governed by the presented goals, aim to satisfy the described needs, and take into account the listed constraints. In order to provide sufficient background information, each significant decision will be presented in a distinct subsection, in which the full analysis of the decision process will first be provided and then summarized in a table listing the main points.

---

\(^3\) The extent to which such reporting features would allow Member States to completely fulfil their reporting obligations requires evaluation. A point to consider is the additional information that would be required (e.g. considering Annex IX) that is not provided from the movement and notification processes themselves.
4.2.3.1 Architectural Decision AD-001 – Overall architecture and topology

To define the overall architecture of the proposed system, four different alternatives were considered. These alternatives are based on the basic premise that, at its core, the overall solution is essentially a communication platform between multiple different parties (Industries and CAs). The alternatives considered are:

- A fully centralized system.
- A fully decentralized system.
- A hybrid solution between full centralization and decentralization. This approach is further broken down in two possible options:
  - A solution where the central part of the topology is the simplest possible.
  - A solution where the central part of the topology is enriched to its fullest extent.

Each alternative is subsequently presented along with a summary SWOT (Strength, Weaknesses, Opportunities and Threats) analysis per case.

4.2.3.1.1 Centralized system

In a fully centralized system there exists a single EU application for all EU transboundary waste movements. All relevant stakeholder entities (e.g. Notifiers, Consignees, Competent Authorities, Commission Agents) are registered in this system and need to access it directly in order to perform each task.

The significant benefit of this approach is the possibility to centrally manage and control all processes. In fact the waste movement processes would be ideally suited for implementation through a workflow engine where a single process is split into multiple distinct steps and user assigned tasks. This supports long running operations and allows their fine grained monitoring and management. Combined with a queuing system to act as the backbone through which distinct steps are processed, this approach also effectively scales at peak times and provides a robust fault tolerance mechanism through message redeliveries.

Additionally, the fact that all parties directly operate on the same system effectively obsoletes any need of remote message exchange since messages are created, assigned, acted upon and completed internally. By avoiding remote message exchange the concerns of authenticating remote IT systems, defining and securing the communication channel with them, and establishing a communication protocol based on acknowledgements and redeliveries are automatically avoided. Legal documents for the notification and movement procedure are electronically registered and dispatched between the involved stakeholders. The system will automatically produce and print upon user’s request all relevant document entities specified by legislation (e.g. Movement Document, Notification Document etc.).

This approach also offers the possibility of including a monitoring module to provide the relevant stakeholders (e.g. DG ENV and Competent Authorities) with the relevant metrics for transboundary waste notifications and movements. With a centralized system the information to produce these reports can be retrieved locally, a fact that would significantly enhance the reporting options, which could be fully customizable, and their performance.
A centralized system is able to support the Member States that do not have the resources to put in place their own IT system. On the other hand however, this poses a major issue for the Member States that currently operate, or are planning to operate, an IT solution to cover their national waste management needs (e.g. Germany). Since direct use of the centralized system will be needed, the stakeholders of such Member States would effectively need to use two systems in parallel, one for domestic and one for transboundary purposes, without guarantees that this would even be possible. If this were not the case, a centralized approach would figure as the most attractive solution. As the situation stands however, the approach needs to be currently disqualified.

<table>
<thead>
<tr>
<th>SWOT – Centralized system</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
</tr>
<tr>
<td>- Single, harmonized implementation</td>
</tr>
<tr>
<td>- Maintenance of a single application</td>
</tr>
<tr>
<td>- Workflow support for elaborate processes</td>
</tr>
<tr>
<td>- Enhanced monitoring and reporting capabilities</td>
</tr>
<tr>
<td>- All participants can directly communicate</td>
</tr>
<tr>
<td>- Simplified communication security and protocol</td>
</tr>
</tbody>
</table>

**Opportunities**

- Deadline of the project met with the delivery of a single application

**Threats**

- Cooperation of multiple Member States to produce a single application
- Application would need to offer at least all the functionality available in existing Member State solutions

4.2.3.1.2 Decentralized system

Using a decentralized approach there is no central EU application. The solution comprises of individual national applications that communicate between each other with the use of a commonly accepted interface. This interface is implemented as an agreed set of SOAP web services that use an agreed XML format to communicate the messages foreseen by the transboundary waste movement processes. The only component playing a central role is a reference service exposing the code lists and other enumerated values (e.g. identification of Waste producers, Notifiers, Treatment facilities etc. or lists of wastes) that individual national systems would need to periodically refresh.

The main benefit of this approach is that existing national systems can continue operating albeit with an adapter module that would ensure that outbound transboundary messages are formatted according to the agreed standard and incoming ones are converted to the internally consumed format. In addition,
already existing work on the definition of common communication protocols (e.g. EUDIN; e-TFS) can serve as the starting point in defining the protocol to put in place.

The lack of a central EU application, with the exception of the non-critical reference lookup service, also means the lack of a single point of failure and the lack of a single bottleneck. If a national system is brought offline this has no effect on the communication between other systems. In order to facilitate adoption, it would be advisable that the Commission implements an open source National Reference Application (NRA) that fully supports the defined communication interface. This NRA could be used as-is by Member States without an existing solution or could serve as the starting point for a Member State that wants to extend what is provided for its own needs. Note however, that even with the provisioning of a NRA implementation, Member States would still need to ensure resources for the hosting and operation of the system which could be problematic.

A requirement that would be challenging, if not impossible, to fulfil with a decentralized architecture would be the monitoring and reporting at an EU level (e.g. by Commission Agents). First of all, in order to do this, an additional non-national node (Reporting module) would need to be put in operation, which would need to retrieve all required data from the remote national systems through additional messages, specifically designed for this purpose. Apart from the increased effort in defining such messages and implementing their support, the reporting possibilities would be limited and very difficult to evolve. Moreover, performance would be a significant concern since most reports would require combining information from multiple remote data sources. Finally, without a central node keeping track of the exchanged messages, inconsistencies between different national systems could appear that would be difficult to resolve.

Another concern of this approach would also be securing communications and establishing trust that received messages are authentic and that remote national systems are authenticated. In order to secure the communication channel and provide system authentication, all web service message exchange takes place over channels encrypted with 2-way SSL, i.e. using server and client digital certificates. SSL prevents malicious parties intercepting and replaying messages, whereas the use of server and client certificates allows both communicating systems to securely establish the identity of each other. Even with 2-way SSL however, personal digital signatures on the message content (e.g. a Notification request) would be highly desirable to ensure message integrity and non-repudiation, considering that the source of the messages is not a single commonly trusted central node.

The monitoring and reporting challenges, increased security measures, and the need for individual Member States to develop and operate their own system leads to this alternative being disqualified.

<table>
<thead>
<tr>
<th>SWOT – Decentralized system</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
</tr>
<tr>
<td>- Member States with existing systems can continue using them with small adaptations</td>
</tr>
<tr>
<td>- Existing work of cooperative systems (e.g. EUDIN) can be reused as the protocol basis</td>
</tr>
<tr>
<td>- No single point of failure or congestion</td>
</tr>
<tr>
<td>- No centralized monitoring and reporting at the EU-level</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Opportunities</strong></th>
<th><strong>Threats</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Full implementation of the project can be phased by including early Member States with an existing system, whereas other can join when ready</td>
<td>- Possibility of not reaching an agreement on the protocol among the MS.</td>
</tr>
<tr>
<td>- Definition of the implementing act on a common protocol for an EDI by the Commission.</td>
<td>- Big challenge in synchronizing the independent implementation by all Member States implying significant effort for the central authority (DG ENV).</td>
</tr>
</tbody>
</table>

4.2.3.1.3 Hybrid system

The hybrid approach attempts to bridge the gap between the centralized and decentralized approaches by keeping the best aspects of both without their main problems. The topology put forth by this approach foresees individual national Member State systems that, in contrast to the fully decentralized approach, do not communicate directly with each other but rather relay all communication through a central EU node. The overall topology resembles that of a star.
This topology offers multiple options for further elaboration:

- The **central EU node** can be implemented as a simple router, without significant additional functionality, or can be elaborated to support features such as centralized reporting, automated rule-based validation of routed messages, and management of ongoing message exchanges.

- The **national MS endpoints** can either be implemented as systems specific to a single MS or grouped in systems commonly used by multiple MS. At the level of the central EU node what would be needed is the configuration of the endpoint that corresponds to each MS, regardless of whether or not these endpoints are physically distinct. For an endpoint that is indeed a single and distinct MS system, this could either be an existing MS IT solution adapted to the needs of the common communication protocol, or an MS-hosted instance of a National Reference Application (NRA), developed and provided by the Commission, that was previously discussed. On the other hand, IT systems that represent multiple MS could either be an independent initiative of a group of MS, or an application built by the Commission to support MS without separate IT solutions.

The different approaches that these options allow are the subject of the subsequent sub sections. In its high level form however, the hybrid, star-based topology discussed offers certain key benefits that are common to all cases:

- **Security**: the communication channels are limited since we now have one channel per MS rather than channels connecting each MS system to all others. The limited number of channels makes use of 2-way SSL realistic and significantly simplifies certificate management.

- **Location abstraction**: the central EU node effectively acts as an Enterprise Service Bus\(^4\), abstracting the physical location of each MS system from the others. An address change for one MS system endpoint would require a single configuration update in the central EU node, rather than an update of all other MS systems.

- **Evolution possibilities**: as discussed previously, this topology allows multiple options for evolution which can also be rolled out in an iterative manner. An example is the central EU node that can be extended from performing simple routing tasks to also exposing rich use cases for reporting by Commission and MSCA officials.

4.2.3.1.3.1 Hybrid system – simplified central component call Central EU router

This approach is a version of the hybrid topology where the central EU node is a simple routing service whereas no provision is made by the Commission for the national IT system of each Member State. Following this approach, each Member State is required to provide and operate their own IT system, and connect it to the central EU node for routing purposes. Considering its simplified purpose, the central EU node is referred to here as the central EU router.

\(^4\) An **enterprise service bus** (ESB) is a **software architecture** model used for designing and implementing communication between mutually interacting software applications
The benefits of this approach are the ones listed in the previous section that generally apply when comparing the hybrid to the fully centralized or decentralized topologies. The central EU router could well be envisioned as a system without a web user interface since all of its tasks are automated. It is however more realistic to consider that a very basic interface is foreseen for Commission administrators in order to verify the health of the system and adapt its configuration (e.g. when an MS endpoint address changes). Implementation of the routing logic is mandatory in the initial version of the system, whereas additional extensions can be foreseen and added to its set of functionalities after it is initially operational. A first apparent extension would be the automated validation of received messages against a basic rule set to ensure that they make sense (e.g. block an approval message for a process that has already been rejected by the same party).

Concerning the national IT systems, each Member State would be responsible for providing and operating their own system. An EDI protocol based on the exchange of XML messages through SOAP-based web services is required, for which Member States with existing IT solutions would be expected to update their applications to handle the conversion of messages to and from the common format. Considering that one of the envisaged architecture’s goals is to provide a solution to Member States without an existing IT system, it is expected, although not mandatory, that the Commission implements and shares a National Reference Application (NRA) as first discussed in 4.2.3.1.2. Such Member States would thus be able to reuse as-is the NRA without the need to invest in analysis and development effort of their own solution, without excluding the option to extend and customize it to suit their own national needs. It needs to be taken into account however, that even with a reuse of the NRA, a Member State would be expected to host, operate and maintain this application themselves at their own effort and cost.

This simplified version of the hybrid approach fails to meet the goal of providing centralized reporting features for the Commission and the MSCAs, and also expects Member States without an existing IT solution to make significant investments, even if a NRA is foreseen. For these purposes this approach is disqualified in preference of a hybrid approach where these concerns are addressed, discussed in the next section.

<table>
<thead>
<tr>
<th>SWOT – Hybrid system (simplified central component called central EU router)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
</tr>
<tr>
<td>- Support for Member States with existing systems</td>
</tr>
<tr>
<td>- Enhanced security and configurability compared to a fully decentralized approach</td>
</tr>
<tr>
<td>- Ability to reuse existing work to define communication protocol (e.g. EUDIN)</td>
</tr>
<tr>
<td>- Limited costs for Commission for the development of the central components</td>
</tr>
</tbody>
</table>

Date: 01/09/2014
### Opportunities
- The central EU router can be incrementally extended to support additional needs
- Full implementation of the project can be phased by including early Member States with an existing system, whereas other can join when ready
- Member States wanting to implement their own systems can use the envisaged NRA as a starting point

### Threats
- Cooperation of multiple Member States to define the central EU router and the EDI protocol.
- Coordination of the Member States without an existing solution to setup their national system (based on a NRA or not)

#### 4.2.3.1.3.2 Hybrid system – elaborate central components called central EU application

This approach is an elaboration of the hybrid topology that foresees an elaborated central EU application as well as a Commission provided solution for Member States with no solution of their own. The elements of this architecture are as follows:

- **A central EU application.** The purpose of this is to act as a hub for all national systems, perform the appropriate message routing, and maintain centrally the information required to satisfy monitoring and reporting requirements.

- **National MS systems.** Each Member State can connect its own national system to the central EU application. This case is oriented for Member States that have an existing IT solution in place or for those that want to implement their own (e.g. to cover specific national needs). Existing national systems would need to be updated with an adapter module to transform transboundary messages to and from their national format.

- **Shared MS application.** This is a single application that can be accessed by all parties of Member States that either do not have an existing solution or do not want to invest in one. This application could be developed, operated and hosted by the Commission (driven by DG ENV and hosted at DIGIT) thus removing such requirements from Member States. Note that additional multinational systems could be implemented as well by groups of Member States (e.g. the Nordic-TFS participants) as long as they comply with the communication protocol and can internally route messages.

A first benefit of this approach is the fact that it supports both Member States with existing systems that want or need to continue their operation, as well as Member States that are unable to invest in their own application. In the central EU application all Member States are configured as distinct endpoints even though multiple endpoints may be implemented by a single multinational system. This is an important note since it gives flexibility to the overall solution to evolve either to a fully centralized or a more decentralized landscape. Member States with an existing system may choose to discontinue its use and...
join the multinational domain whereas others already participating in this may opt to leave once their own national system (which they have customized to suit potential additional needs) is ready.

As in the case of the decentralized approach, an EDI Protocol is required. This is foreseen to be a common XML format that describes all messages necessary to support the transboundary waste movement processes. These XML messages will be exchanged using SOAP-based web services. An important difference in this case is that the communication channels are significantly fewer since each existing national system will connect only to the central EU node. The channels are again encrypted using 2-way SSL, where the presence of server and client certificates serve to establish each system’s identity. Moreover, the fact that each national system only receives messages from the central and trusted EU node can be used to enhance trust in their authenticity and origin.

Concerning the Commission-hosted shared MS application, this is foreseen to be deployed as a separate application even though it could simply be a part of the central EU node. The reason for this is primarily security since its end-users will be all Industry and CA users of the represented Member States. On the other hand, access to the central EU application will most likely be possible only to Commission Agents and, possibly, Member State CAs. We can still however take advantage of the colocation of both applications in order to optimize the communication of messages by using technologies more efficient than SOAP (e.g. JMS messaging).

This architecture also allows the system to fulfil its needs with respect to centralized reporting on transboundary waste movements. This is achieved through the central EU node that records all messages exchanged between Member States. In order to achieve this, all multinational systems (the one implemented by the Commission and any possible additional ones) need to always route transboundary messages through the central EU node even for cases that could be satisfied internally. In contrast, communication that originates and ends within the same Member State is not routed to the central node.

**Figure 4-1:** Communication from external MS application to MS in shared application

**Figure 4-2:** Communication between MS in shared application
The described hybrid solution is selected as the proposed architecture considering that it combines the good elements of the centralized and decentralized alternatives without their significant weaknesses. In addition, in contrast to the more simplified hybrid approach described in 4.2.3.1.3.1, this approach caters for Member States with no solution and covers the required reporting needs. It could be argued that an attractive choice would be to use the simplified hybrid approach with subsequent iterative extensions, however it is the position of this study that the only way to address the full set of goals and constraints is to adopt the currently described elaborated, hybrid approach. Appendix 2 includes an illustrative scenario that discusses the hybrid system’s message communication in more details.

### SWOT – Hybrid system (elaborate central components called central EU application)

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
</table>
| - Support for Member States with and without existing systems  
- Flexibility to evolve into a more decentralized or centralized system  
- Enhanced monitoring and reporting capabilities  
- Ability to reuse existing work to define communication protocol (e.g. EUDIN) | - Single point of failure  
- Increased cost for the development of the more elaborate central EU components. |

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
</table>
| - Member States can drop their existing systems  
- Member States wanting to implement their own systems can participate from the beginning and only switch when fully ready  
- Member States not having an IT system in place will benefit from the Commission-developed Shared MS application. | - Cooperation of multiple Member States to produce a single application. |

### 4.2.3.1.4 Summary

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Overall architecture</th>
<th>Topic</th>
<th>Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>Hybrid architecture involving a central EU node for routing and reporting with connected national and shared MS applications.</td>
<td>ID</td>
<td>AD-001</td>
</tr>
<tr>
<td>Issue or Problem Statement</td>
<td>Define the overall architecture of the solution in terms of which systems are foreseen and how they communicate in order to best address the stated goals and requirements, while taking into account the constraints.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>The main principle that defines this decision is the need to support the foreseen transboundary waste movement processes and provide reporting, while at the same time support both Member States that have existing systems in place and those that do not.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Motivation
Defining the overall architecture is important as a first step since this identifies the subsequent decisions that need to be taken.

Alternatives
The alternatives considered are:
- A fully centralized approach (single central EU system).
- A fully decentralized approach (no central system – individual national systems).
- A hybrid approach (central EU application – connected national MS applications) further elaborated as:
  - Simplified (central EU router)
  - Elaborate (feature rich central EU application and shared MS application)

Decision
The elaborate hybrid approach using a central EU application connected with the existing national systems and a multinational system for all Member States without an IT solution in place.

Justification
The selected approach best covers the stated goals and requirements and is the only one that supports both Member States that have existing systems in place and those that do not. This approach offers also the best flexibility for future evolution.

Implications
Existing Member State systems will need to include an adapter module to interface with the central EU node.

Derived requirements
The approach decided upon mandates the definition of a communication protocol (message format, message exchange sequence and web service interface) and securing the channel between remote systems.

Related Decisions
AD-002, AD-003, AD-004, AD-005, AD-006, AD-007

4.2.3.2 Architectural Decision AD-002 – Digital signatures

The transboundary waste movement processes involve creating and sending messages to multiple appropriate recipients that typically need to be acted upon. The use of digital signatures is an interesting point due to the benefits that they would bring to this message exchange:

- **Authentication**: Personal digital signatures provide proof of the identity of the signer. This would be very important if industry actors could directly communicate between each other in order to enabler trust on the participants’ identity.

- **Non repudiation**: Providing a personal signature of an appropriate level also acts as proof that the message was indeed created by the sender. A sender that has personally signed a message is thus unable to subsequently deny having performed this action.

- **Message integrity**: A signature on a message allows subsequent checks to ensure that the current contents of the message correspond exactly to the contents that were initially signed. This would be a necessity if we are unable to fully trust the communication channel or the intermediate applications that handle messages.

One important point to consider is the holder of the certificate that is used to generate the signature. If this is an e.g. intermediate system, the guarantees that you have start only from the system itself, which you need to trust, but can’t be extended to the actual user that performed the original action. The only way to establish authentication and non-repudiation for a personal user’s action is to have the signature created by himself on his local machine (i.e. not on his behalf from a remote system), using his own private personal certificate.

In principal, when having the choice between requiring personal digital signatures for the system’s messages and no signatures at all, it is typically always preferable to opt for digital signatures. The challenge is to consider if signatures are truly required in the current context, considering the significant administrative overhead and cost in:

- Creating certificates. Personal certificates need to be created following verification, in person, of the user’s identity.
- Delivering certificates. Created certificates need to be delivered securely and in person to end-users to ensure that it is them who receive them (you can’t e.g. send a certificate by email).
- Managing the certificates’ lifecycle. This involves issuing new certificates (upon e.g. expiry) and revoking certificates that can no longer be trusted.
• Verifying certificates. This involves establishing trust of the certificate chain while taking into account expiration dates and revocation lists.

These points are the reason why national electronic ID (e-ID) schemes are interesting, since the steps to create, deliver and manage certificates are carried out by the appropriate local authorities. As stated in the design choices made for EUDIN, the handling of e-ID schemes for transboundary purposes is indeed not mature enough to rely upon. Moreover, it needs to be considered that most Member States lack such a scheme to begin with. The alternative in this case would be to issue certificates specifically for this purpose (e.g. by a Commission Certification Authority) which however entails the previously mentioned complexities.

Another important point to consider concerning the use of personal digital signatures comes from the fact that this needs to take place from the actual end user. Doing this would pose significant problems for Member States with existing waste movement solutions since either two solutions would need to be used in parallel (one for transboundary movements and the existing national one), or the existing system would need adaptation to use the appropriate certificates and the common message format. In other words, it is not possible to apply this transparently to end users since reformatting a message at a national layer through an adapter module before routing to the central EU node would change the message contents and invalidate any signature. Signed content is required to originate from the end users themselves, after having inspected the content to be signed, which upon signature, can’t be altered in any way.

The architecture of the proposed system introduces a central EU node and requires that messages are always routed through national CA nodes. In other words there is no direct communication between Industries (a Notifier and a Consignee) but all communication passes through multiple verification steps at trusted nodes. This fact allows us to no longer mandate the use of signatures for authentication and non-repudiation. On the other hand, message integrity is provided by securing and encrypting the communication channel between the national and central nodes. It is proposed however that signatures are introduced as an optional element in order to:

• Allow for a phased adoption of national e-ID schemes as they are implemented and their transboundary handling matures.
• Allow individual Member States to require signatures from their national participants that, through appropriate configuration, could be verified by the central EU node. For cases where signatures are present these would then be stored to serve the purpose of non-repudiation.

Note that these optional signatures should be of a level appropriate to enable offline and long term validation (i.e. XAdES-X-L, XAdES-A). Having said this, we still need to consider two important points concerning even the optional use of digital signatures, in order to evaluate their usefulness:

• It is often the case that trusted third party representatives are used to carry out a legal entity’s regulatory obligations. The envisaged solution would most likely need to cater for such third parties and foresee or integrate a means of automatically verifying such a third party's relationship to the legal entity.
• When signing, an end user must be presented with the exact content to be signed in order for the signature to be meaningful. This presents a challenge when dealing with structured data (XML), as in the case of the envisaged system, to ensure that the displayed content is meaningful to a non-technical user.

Such concerns would need to be addressed from a functional perspective in order to determine how signatures, even optional, should be incorporated into the solution in a way that is meaningful to the end users and that is in line with how the Industry’s legal entities operate.

A final point relating to digital signatures concerns the actual movement documents that transporters are required to present to local authorities. Considering that these documents represent a significant part of the paper-based approach this system aims to replace, it would be interesting to provide a solution that could allow the same verification digitally. A potential solution would be to enable the downloading of documents from the central EU node in an acceptable format (e.g. PDF) that would be signed appropriately (e.g. using PAdES) by the trusted central EU node. Presenting these documents electronically would allow local authorities to verify that the documents are genuine and produced by the EU node, which has ensured the correct participation and consent of involved parties.
### Architectural Decision

**Security**

**Topic**

**Digital signatures**

<table>
<thead>
<tr>
<th>Architectural Decision</th>
<th>Personal digital signatures are included as optional elements that can be enforced by individual Member States. The decision can be revisited once national e-ID schemes and their transboundary use matures.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue or Problem Statement</td>
<td>Evaluate the use of digital signatures as part of the communication protocol taking into account the feasibility of proposed alternatives and the degree to which they are required considering the current system and its architecture.</td>
</tr>
<tr>
<td>Assumptions</td>
<td>National e-ID schemes and their use for transboundary purposes are currently not mature. In addition, the proposed system architecture involves routing through national CAs and the central EU node. Finally, existing national systems would be significantly impacted by the use of signatures on a new common format.</td>
</tr>
<tr>
<td>Motivation</td>
<td>Using digital signatures provides solutions for authentication, non-repudiation and message integrity but involves a significant administrative cost that needs to be taken into account.</td>
</tr>
<tr>
<td>Alternatives</td>
<td>The alternatives are essentially to use digital signatures (either through national e-IDs or via certificates specific to the current system) or to not require them, assuming that their purpose is otherwise served.</td>
</tr>
<tr>
<td>Decision</td>
<td>Digital signatures are at this stage only included as optional elements in the communication protocol.</td>
</tr>
<tr>
<td>Justification</td>
<td>The choice was made considering the lack of a common transboundary approach based on national e-ID schemes, and considering that requiring signatures would significantly impact existing national solutions. The properties of the proposed architecture provide assurances that the benefits of personal signatures are, to a degree, otherwise achieved.</td>
</tr>
<tr>
<td>Implications</td>
<td>The communication channel between national and the central nodes needs to be secured and encrypted. In addition, to enhance trust, routing must only be possible by involving trusted nodes.</td>
</tr>
<tr>
<td>Derived requirements</td>
<td>To include optional signatures in the communication protocol and ensure that the communication channel is appropriately secured.</td>
</tr>
<tr>
<td>Related Decisions</td>
<td>AD-001, AD-003, AD-005</td>
</tr>
</tbody>
</table>

### 4.2.3.3 Architectural Decision AD-003 – Message format

The proposed system architecture entails communication between the central EU node and the currently existing national systems. These systems will need to be updated at the top national level with an adapter module that will transform incoming transboundary messages from the common format to the internal national one and vice versa. Note that the discussed multinational application to cover Member States with no existing solution will also comply with the common format and the related message exchange although the communication itself will be adapted to enhance performance (i.e. messages will be exchanged using efficient messaging rather than SOAP web service calls).

A requirement that needs to be taken into account is to benefit as much as possible from existing investments by Member States in the definition of a protocol and format for transboundary waste movement. There are two “standards” defined by Member States for interfacing between different applications that implement the Waste Shipment regulation in EU. These are:

- **EUDIN**: Initiative by Austria, Belgium, Luxembourg, Switzerland, Nordic TFS
- **e-TFS**: Initiative by Germany and the Netherlands.

The following table offers a point comparison between these two.
| Support for transboundary waste movement processes | Notification and Movement related messages are covered. | Notification and Movement related messages are covered. |
| Communication between participants | No direct electronic data interchange between businesses and competent authorities other than the businesses’ local competent authorities. | e-TFS is more flexible on this matter and supports direct data interchange of involved business parties. |
| Use of digital signatures | Currently no use of digital signatures. The rationale is that the globally and EU-wide available standards and technologies for digital signatures are not sufficiently mature to be used in cross-border public administration related data interchange. | The exchange of digital signatures for notification and movement documents is required. Additionally, a layered approach is used in order to ensure auditability of the order of signatures. This means that a message should contain the full set of the digitally signed documents up to the specific point by all relevant stakeholders. |
| Use of a central node | The existence of a central node playing the role of a message broker is mandated. | Communication can happen directly and without the participation of a central message broker. |
| Message format | XML message format agreed by all participant Member States. | Based on the BMU protocol but at the same time makes use of the EUDINv2.1 message specifications. |
| Implementation status | Central EUDIN component implemented and currently in use by certain EUDIN – participant Member States. | Used as an interface in the context of a pilot project between Lower-Saxony and the Netherlands. |

A critical point to consider from the above comparison is the enforcement of digital signatures, required due to the decentralized topology in e-TFS that would not be possible for most Member States. In addition, it would need to be further investigated whether the e-TFS format defines additional elements that cannot be applied to all EU Member States.

---

5 Belgium comments that in the latest version of EUDIN certain adaptations have been made with regard to the exchange of messages between all involved entities.

6 Based on comments by Switzerland, the communication in e-TFS adds complexity since Industries need to connect to each competent authority system involved. Additionally, handling the number of Industry and competent authority interfaces is considered a possibly unfeasible task. Finally, it is stated that Member States would need to anyway invest in centralized frontends to support small companies unable to invest in separate system implementations.

7 Based on comments provided by Germany, one of the complications of having such a central node is establishing a shared set of business rules to validate message contents.

8 Based on comments provided by Austria on current EUDIN use and tests that have already taken place to cover simple and complex scenarios.
With these points in mind, EUDIN appears as a more suitable candidate considering that it is designed as a pan-European format and does not impose difficult to achieve requirements to its participants (i.e. use of signatures\(^9\)). The proposal as such is to use the EUDIN format with the following assumptions:

- It is extended where and if needed in order to fully support the foreseen regulatory processes as well as any other transboundary waste movement aspects not currently covered.
- It is modified where needed to ensure that Industries can also be direct senders and recipients of messages. To avoid confusion on this point, the envisaged solution’s hybrid architecture (see decision AD-001) does not only foresee message exchange between competent authorities. The important point is that the physical participants in the message exchange are centralized nodes (the central EU application, shared MS application and, where applicable separate applications at the MS level) and not applications at the Industry level, whereas the logical recipients can be competent authorities or Industry actors connecting to these centralized applications.
- It is refined where needed to allow optional digital signatures as per decision AD-002. Note that signatures may already be supported if their inclusion in SOAP message headers is sufficient.
- It is examined in detail in order to ensure that any unnecessary elements are removed. An example would be the username/password information included which for system to system communication is not required.

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Communication protocol</th>
<th>Topic</th>
<th>Message format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>The EUDIN message format is used as a starting point assuming that it is elaborated to cover all required processes.</td>
<td>ID</td>
<td>AD-003</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>To define the message format to be used in the communication between the national and central EU nodes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>Assumptions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The EUDIN format can be extended where needed, digital signatures are optional and the system’s architecture requires the message format only for communication between the central EU node and the national nodes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Motivation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defining the message format is important since this, along with the related web service interfaces, forms the contract to be respected between participating systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alternatives</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alternatives are either to define a new format, or consider existing ones to use as-is or extend where appropriate. Existing formats to consider are EUDIN and e-TFS.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Decision</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use the EUDIN message format, assuming that it will need to be extended to support the notification process, allow optional signatures, and be modified where needed to remove unnecessary elements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EUDIN is more appropriate for use in the proposed architecture and is closer to a common standard than e-TFS.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implications</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The need to involve Member States in the further extension and full adoption of EUDIN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Derived requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Further examine and extend the EUDIN format as needed by the regulation requirements and its use in the proposed system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Related Decisions</td>
<td></td>
<td>AD-001, AD-002</td>
</tr>
</tbody>
</table>

**4.2.3.4 Architectural Decision AD-004 – Message exchange**

The precise messages exchanged for each transboundary waste movement process are out of the scope of the current study. What is important to clarify however is:

- The type of endpoints that participate in the communication, i.e. how is the communication interface implemented.

---

\(^9\) Based on comments provided by Germany, electronic signatures remain indispensable for secure authentication considering that the WSR currently holds responsible for irregularities the person signing.
- The principles guiding the message exchange (e.g. synchronous vs asynchronous, acknowledgements etc.).

The systems participating in the message exchange are independent and no assumptions can be made on their implementation. The only point that can be assumed is that each system fully supports the commonly defined interface that consists of operations and the messages’ structure. The most fitting implementation for this scenario is SOAP web services where a common WSDL defines the expected endpoint operations and a referenced XSD describes the messages’ structure. SOAP messages also support well digital signatures that, as discussed, will be optionally included.

Concerning the message exchange, we need to consider that sent messages require acknowledgements and that in various scenarios multiple messages need to be sent as part of a single operation (e.g. a Notifier request sent to multiple CAs). Synchronous operations are impractical considering possible timeouts and the fact that most messages require manual treatment. Assuming the use of asynchronous calls, an efficient approach that avoids continuous polling or custom callbacks is to require that all messages are eventually responded to with an acknowledgement message. Such acknowledgements may either be generated automatically following a failure of technical checks or as the result of a user action (e.g. a CA user providing consent for a request).

Similar to the EUDIN specifications, each message will need to have a unique identifier and will potentially reference other message identifiers. Receiving multiple identical messages must not cause adverse side-effects, whereas operations to manually or automatically request that a message is resent need to be foreseen. All messages exchanged between Member States will be routed through the central EU node, where they will be recorded. Since the central EU node maintains a log of all exchanged messages it can automatically detect expected responses that are not received and can resend their original requests.

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Communication protocol</th>
<th>Topic</th>
<th>Message exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>Asynchronous SOAP web service calls with distinct acknowledgment messages.</td>
<td>ID</td>
<td>AD-004</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>Define the implementation of the interface and the message exchange principles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>The approach for message exchange must not make any assumptions on the implementation of participating systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation</td>
<td>The approach to exchange messages will allow external systems to connect and the overall solution to automatically resolve problems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternatives</td>
<td>Use SOAP web services or an alternative integration technology (e.g. RMI, CORBA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>SOAP web services are selected used with asynchronous calls and message acknowledgements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td>Web services allow systems with varying implementations to communicate and support digital signatures. Asynchronous calls with explicit acknowledgements per message avoids polling and custom callbacks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>The Commission needs to coordinate with the Member States to agree on the supported operations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derived requirements</td>
<td>The implementation of the central EU node should log all exchanged messages and should provide means of automatically resolving problems (e.g. message resend after a specific time).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.2.3.5 Architectural Decision AD-005 – System to system communication channel

The proposed architecture requires the exchange of messages between the central EU node and the remote, existing national systems. This decision relates to defining the specifics of these communication channels. An approach needs to be selected that will ensure:

- The participants in the communication are able to establish the identity of each other.
- Unintended participants are not allowed to monitor exchanged messages, intercept them and modify them before replaying them to their intended recipient.
To address the second need SSL is foreseen as a means of encrypting the communication channel. More specifically, considering that remote system authentication is required, the channel will be encrypted using 2-way SSL, i.e. using client and server certificates. This requires that each remote system will have:

- A server certificate to be presented when receiving incoming web service calls.
- A client certificate to be presented when outgoing web service calls are made.

An alternative or additional option to consider is the establishment of a VPN connection between remote points. Using a VPN is however not considered necessary because:

- The encryption offered is already covered by the 2-way SSL channel.
- Simulating a private network brings no added value to the system.
- In terms of authentication VPNs provide site-to-site authentication but not application-to-application authentication that is offered by the web service calls using 2-way SSL. Application-to-application authentication is more specific than site-to-site and, as such a VPN would not enhance security.
- Establishing a VPN requires additional effort in configuring and maintaining infrastructure that is not justified by the current needs.

### Subject Area

<table>
<thead>
<tr>
<th>Architectural Decision</th>
<th>Security</th>
<th>Topic</th>
<th>System to system communication channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web service calls over channels encrypted using 2-way SSL.</td>
<td>ID</td>
<td>AD-005</td>
<td></td>
</tr>
</tbody>
</table>

### Issue or Problem Statement

The need to provide authentication between each remote national and the central EU node and to prevent unintended parties to intercept and modify messages.

### Assumptions

The distinct communication channels are limited to the number of remote national systems that need to connect to the central EU node.

### Motivation

Apart from enhancing communications’ security, this decision is important to determine if additional measures are required (e.g. digital signatures).

### Alternatives

Use of 1-way or 2-way SSL and/or use of VPNs.

### Decision

2-way SSL channels will be used for the web service calls used to exchange messages between the remote national systems and the central EU node.

### Justification

2-way SSL channels is the Industry standard approach of encrypting communications where additionally authentication of both parties is required. The derived need for client and server certificates is acceptable considering the small number of remote participants.

### Implications

The Commission as well as Member States with existing systems will need to each obtain server and client certificates. Maintenance of these certificates for each participant will incur a degree of administrative overhead.

### Derived requirements

Client and server certificates are required for each participating remote system.

### Related Decisions

- 4.2.3.6 Architectural Decision AD-006 – User to system communication channel

Apart from system-to-system communication for the exchange of messages, the system needs to foresee as well end-users that will directly access the central EU node and the multinational application for Member States with no distinct solution. The communication channel connecting end-users with the Commission systems will need to similarly provide guarantees of confidentiality.

Using SSL to encrypt the communication channel is the Industry standard means of preventing malicious parties of monitoring and modifying transmitted information. In this case however 2-way SSL using client and server certificates is not preferable considering that each end-user would need to have a trusted personal digital certificate. 1-way SSL using only server certificates avoids this issue as long as it is combined with a robust means of authenticating end-user identity. Note that 1-way SSL is foreseen both
for accessing the central EU node (e.g. for Commission or Member State CAs) as well as the multinational application.

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Security</th>
<th>Topic</th>
<th>User to system communication channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>1-way SSL using a server certificate.</td>
<td>ID AD-006</td>
<td></td>
</tr>
<tr>
<td>Issue or Problem Statement</td>
<td>The need to prevent unintended parties of monitoring or modifying information transmitted between end users and the Commission systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>A robust user authentication scheme is in place to remove the need for 2-way SSL.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation</td>
<td>Securing the communication channel between end-users and the Commission systems is a critical link in the overall system security.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternatives</td>
<td>Use of 1-way or 2-way SSL.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>1-way SSL used (server certificates only) combined with a separate user authentication scheme.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td>2-way SSL is disqualified as an option considering the need of providing all end users with trusted personal certificates. 1-way SSL is the Industry standard approach and is easily implemented.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>A server certificate will need to be obtained for the central EU node and the multinational application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derived requirements</td>
<td>Ensure that a robust user authentication scheme is in place.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Decisions</td>
<td>AD-007</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.2.3.7 Architectural Decision AD-007 – User authentication and authorization

The proposed system requires a robust scheme for authenticating end-users that is common for all participating Member States. Having such a scheme in place is critical considering that:

- The encrypted communication channel (see AD-006) makes no assumptions or guarantees about an end-user’s identity.
- The lack of personal digital signatures (see AD-002) places a greater need to trust the central EU node and the multinational application. Messages and documents produced by these systems need to be considered authentic and should indicate that all appropriate processes have been upheld (e.g. communication of a Movement request to all appropriate parties).

User accounts will need to be created for all Commission Agents expected to access the system, Member State CAs, and Industry users of the multinational application for Member States without an existing system. Since this system is hosted by the Commission an ideal candidate for its authentication purposes is ECAS that offers a trusted service to contain user credentials and provide 2\textsuperscript{nd} factor authentication using SMS challenges. In addition ECAS offers standard features such as the regeneration of passwords that would be expected by such a service.

In terms of authenticating end users the following measures are proposed:

- Usernames and passwords recorded in ECAS. ECAS addresses issues such as appropriate password strength, account blocking, password history and offers related services such as password regeneration.
- A required 2\textsuperscript{nd} factor using SMS challenges. For a system where establishing user identity is critical for its overall trust a 2\textsuperscript{nd} factor is considered mandatory. An SMS challenge offers the simplest approach avoiding the need to e.g. send secure token generators to end-users.

It is proposed that SMS challenges are also used for important actions in the system such as the creation of Notification or Movement requests.

In terms of authorization, the proposed system will offer a scheme based on roles and permissions, where permissions capture low level actions grouped together into meaningful roles that are eventually assigned to end-users. Through a user’s roles each individual action will be authorized on the server-side to ensure that the appropriate permissions to carry it out are present.
Apart from this static permission checking, server-side data specific authorization will also take place in order to provide segregation between different Member States and to ensure that only authorized data is accessed (e.g. an Industry user can only access his own Industry’s requests).

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Security</th>
<th>Topic</th>
<th>User authentication and authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>Authentication of users using ECAS, with 2nd factor SMS challenges. Authorization implemented server-side to ensure data segregation.</td>
<td>ID</td>
<td>AD-007</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issue or Problem Statement</th>
<th>The measures required to authenticate and authorize users of the central EU node and the multinational application.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assumptions</td>
<td>The security and trust requirements mandate the use of two authentication factors.</td>
</tr>
<tr>
<td>Motivation</td>
<td>Ensuring users are thoroughly authenticated and authorized in the central EU node and multinational application increases the trust in the overall solution.</td>
</tr>
<tr>
<td>Alternatives</td>
<td>New implementation of authentication process or use of ECAS service.</td>
</tr>
<tr>
<td>Decision</td>
<td>ECAS is selected to enable username/password authentication and SMS challenges as a 2nd factor. Authorization will be performed server-side to ensure data-segregation.</td>
</tr>
<tr>
<td>Justification</td>
<td>ECAS offers a trusted Commission service that fully covers the authentication needs of the current system. The effort and risk of implementing a custom approach is thus avoided.</td>
</tr>
<tr>
<td>Implications</td>
<td>All foreseen users will need to register with ECAS either personally or ECAS’s bulk import process.</td>
</tr>
<tr>
<td>Derived requirements</td>
<td>If bulk user registration is foreseen, Member States will need to coordinate with the Commission to collect user information and provide back the generated credentials.</td>
</tr>
<tr>
<td>Related Decisions</td>
<td>-</td>
</tr>
</tbody>
</table>
4.3 Architecture Overview Diagram
4.4 Key Concepts

The component diagram in the preceding section presents the two applications that form the core of the proposed architecture:

- **The central EU application**, responsible for routing messages between Member State applications, and exposing functionalities to Commission and possibly Member State actors to monitor and report on transboundary waste movements.

- **The shared MS application**, used to provide a solution to all Member States that do not operate a distinct national system for waste movement.

Before describing the components of each system it is important to note the following points concerning the applications’ topology:

- Both applications are load balanced clusters, allowing high availability and increased performance from the distribution of load. Moreover designing the applications for a clustered deployment allows them to be horizontally scaled to respond to traffic peaks by adding additional nodes where appropriate.

- The applications, and especially the central EU node, are expected to each have a mirror disaster recovery site in order to allow operations to continue even in cases of extreme problems. The combination of clustering and disaster recovery sites effectively covers the solution’s “single point of failure” weakness.

- Although being distinct, both applications are expected to be deployed on a common, trusted domain (e.g. by DIGIT). This assumption allows us to avoid use of SOAP web services for their communication in favour of more efficient messaging (e.g. JMS).

- Defining two applications does not mean doubling the effort since many system components are similar at least with respect to low level services. Common elements are foreseen to be reused with the appropriate packaging to ensure distinct deployments.

4.4.1 Central EU application

The central EU application defines a **SOAP service façade** that will implement the common interface defined for communication between remote systems. Calling this web service layer does not require application-level authentication actions since it is only accessible over 2-way SSL. Authentication of the calling system is thus achieved through its presented client certificate. To ensure immediate responses to calls, incoming web service calls don’t get synchronously treated but rather result in a work item (an object resulting from the deserialization of the received XML message) placed in an **Inbound message queue**. Queuing input is critical in order to allow the system to support peaks in input message rates. Eventually processing of the input messages is made by the **Business services** layer.

Sending messages to an MS application starts from the Business services layer that places the message object in its **Outbound message queue**. This queue serves the purpose of disassociating backend processing with the actual task of contacting a remote system. Messages placed in this queue are handled by a **Message broker** whose primary task is to determine whether the message should be delivered to the shared MS application or to an external national system. Messages directed to the shared MS application are posted directly on its respective Inbound message queue, whereas messages to be communicated to remote national systems via web services are passed to and processed by the **SOAP service client**. It is the task of the latter to serialize messages, select the correct remote service endpoint, and establish the 2-way SSL channel with the remote system.

The Business services layer will make use of a **Job scheduler**, a service that can provide asynchronous jobs to be scheduled for future execution. This component is foreseen to be used by the central EU node to repeat the sending of messages that have not been responded to, and to implement possible requirements on timeouts and delayed message sending. A **Process engine** is also foreseen to be used in order to better split backend processing in distinct steps, such as the case where a message needs to be first technically validated and then sent to multiple parties. Defining such long running tasks as processes allows better control, the repeat of individual failed steps, and allows enhanced monitoring. Finally a **Messaging service** is foreseen as the backbone upon which this process engine will run in order to allow individual process steps to execute transactional and to allow background work to be queued and processed without resource overload.
User access to the central EU application will be possible through a user interface built using lightweight front end technologies, calling over SSL a REST service façade. All calls to this façade will be authenticated by the Authentication service that will manage the redirection to ECAS for the discussed 2 factor authentication process. The Authorization service will also be used at this point in order to check that the calling user has the permissions to access the requested backend operation and also, by the Business services, in order to ensure the user is authorized to access the specific data in question.

Note that using lightweight front end technologies to implement the application’s user interface could be impossible according to Commission standards mandating the possibility to function without JavaScript. However, the application will not be accessible to the general public but to a specific user base that could explicitly agree on the usability requirements that need to be upheld, thus allowing the use of modern Web 2.0 technologies. This point will need to be elaborated once the solution matures and could result in replacing the lightweight front end and REST service layer with a more traditional server-side MVC approach.

4.4.2 Shared MS application

Industry and Authority users are foreseen to access the shared MS application through a user interface built with lightweight front end technologies that contacts the backend over SSL making calls to a REST service façade. Note that the same consideration concerning the use of a JavaScript-based user interface made in 4.4.1 applies here, with the possibility to move to a more traditional server-side MVC approach if the usability requirements dictate it. Similar to the central EU application, service calls are authenticated using 2 factors through the Authentication service, and authorized in terms of requested operation and specific requested data using the Authorization service. Operations are implemented by the Business services layer that, similar to the central EU application, makes use of a Process engine running on a Messaging service backbone for long-running tasks (e.g. sending a Movement request and having it approved from a local Competent Authority).

When transboundary communication is required, the Business services layer posts the message object on the Outbound message queue, thus separating business processing from the communication process. These messages are then picked up by the Message broker that posts the message to the central EU application’s Inbound message queue. Finally, for messages incoming from the central EU application, an Inbound message queue is foreseen to give an immediate response to the caller, allow scalability for peak handling, and separate message’s reception from its processing that takes place in the Business service layer.
### 5 Re-Usable Architectural Assets

In the table that follows, where assets are stated as not needed, this is based on current assumptions that are subject to evolution. This listing will this be re-evaluated as needed once the solution matures.

<table>
<thead>
<tr>
<th>Architectural Asset Category</th>
<th>Needed? (Yes/No)</th>
<th>Architectural Asset type</th>
<th>Architectural Asset name</th>
<th>Reference</th>
<th>Do you plan to use it in your project? If the answer is not, please, specify the reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Data Management</td>
<td>Service</td>
<td>COMREF</td>
<td>Reference data for the HR domain</td>
<td><a href="https://webgate.ec.europa.eu/CITnet/confluence/display/DIGITTELMA/COMREF">https://webgate.ec.europa.eu/CITnet/confluence/display/DIGITTELMA/COMREF</a></td>
<td>No, no need.</td>
</tr>
<tr>
<td>Auditing</td>
<td>Component</td>
<td>Audit Trail &amp; Logging</td>
<td>HAN Audit Trail Module</td>
<td></td>
<td>No, unless requested by the Commission.</td>
</tr>
<tr>
<td>Batch Management</td>
<td>Service</td>
<td>Universal Batch Scanning</td>
<td></td>
<td></td>
<td>No, no batch jobs are foreseen.</td>
</tr>
<tr>
<td>Business Intelligence</td>
<td>Component</td>
<td>Reporting</td>
<td>Light : Embedded BI</td>
<td></td>
<td>No, unless the Commission requires reporting outside the application’s scope.</td>
</tr>
<tr>
<td>Business Intelligence</td>
<td>Component</td>
<td>Reporting</td>
<td>Heavy: Business Objects</td>
<td></td>
<td>No, unless the Commission requires reporting outside the application’s scope.</td>
</tr>
<tr>
<td>Document Management</td>
<td>Component</td>
<td>No name yet(^\text{10})</td>
<td>Document generation (lightweight)</td>
<td></td>
<td>No, no need.</td>
</tr>
<tr>
<td>Document Management</td>
<td>Component</td>
<td>No name yet(^\text{10})</td>
<td>Document generation (heavy)</td>
<td></td>
<td>No, no need.</td>
</tr>
<tr>
<td>Document Management</td>
<td>Service</td>
<td>PDFCoDe</td>
<td>Document generation</td>
<td></td>
<td>No, will be handled within the application.</td>
</tr>
<tr>
<td>Document Management</td>
<td>DocsRoom (ENTR)</td>
<td></td>
<td></td>
<td></td>
<td>No, no need.</td>
</tr>
<tr>
<td>Error Handling</td>
<td>Component</td>
<td>Other components</td>
<td>Caching, transaction mgmt., exception handling ... For further investigation</td>
<td></td>
<td>No, will be handled within the application.</td>
</tr>
<tr>
<td>Graphical Interface</td>
<td>Component</td>
<td>JSCAF</td>
<td>UI Framework (JSCAF &amp; RefAppUI will converge)</td>
<td></td>
<td>No, no need.</td>
</tr>
</tbody>
</table>

\(^{10}\) The EC product management process still has to provide a recommendation.
<table>
<thead>
<tr>
<th>Graphical Interface</th>
<th>Component</th>
<th>RefAppUI</th>
<th>UI Framework (JSCAF &amp; RefAppUI will converge)</th>
<th>No, no need.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Exchange</td>
<td>Service</td>
<td>eTrustEx</td>
<td>Trusted Data Exchange</td>
<td><a href="https://webgate.ec.europa.eu/CITnet/confluence/display/CCDIGIT/Project+ETRUSTEX">https://webgate.ec.europa.eu/CITnet/confluence/display/CCDIGIT/Project+ETRUSTEX</a></td>
</tr>
<tr>
<td>Information Exchange</td>
<td>Service</td>
<td>e-Prior</td>
<td>Web services for the procurement domain</td>
<td>No, no need.</td>
</tr>
<tr>
<td>Information Exchange</td>
<td>Service</td>
<td>XML Gate (SANCO)</td>
<td>No, no need.</td>
<td></td>
</tr>
<tr>
<td>Information Management</td>
<td>Service</td>
<td>No name yet</td>
<td>Enterprise Service Repository &amp; Registry</td>
<td>No, no need.</td>
</tr>
<tr>
<td>Information Management</td>
<td>Service</td>
<td>Data Centre Services</td>
<td>Stress and Vulnerability tests</td>
<td>Yes, in order to performance test the foreseen applications.</td>
</tr>
<tr>
<td>Mail/Notification Service</td>
<td>Service</td>
<td>CNS - TNS</td>
<td>Notification Management <a href="https://webgate.ec.europa.eu/CITnet/confluence/display/CCESTAT/Project+CN">https://webgate.ec.europa.eu/CITnet/confluence/display/CCESTAT/Project+CN</a></td>
<td>No, no need.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Service</td>
<td>Data Centre Services</td>
<td>Monitoring</td>
<td>Yes, to monitor system health.</td>
</tr>
<tr>
<td>Persistence</td>
<td>Service</td>
<td>Ulysse Actor Management</td>
<td>Object life cycle &amp; State Transition Management</td>
<td>No, no need.</td>
</tr>
<tr>
<td>Rule Engine</td>
<td>Component</td>
<td>No name yet(1)</td>
<td>Rule Management</td>
<td>No, no need.</td>
</tr>
<tr>
<td>Security</td>
<td>Service</td>
<td>e-Signature</td>
<td>Action</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Component</td>
<td>Security Model</td>
<td>Requires however further investigation to see how exactly this will take place.</td>
<td></td>
</tr>
<tr>
<td>Workflow</td>
<td>Component</td>
<td>No name yet</td>
<td>No, no need.</td>
<td></td>
</tr>
<tr>
<td>Workflow</td>
<td>Service</td>
<td>No name yet</td>
<td>No, processes will be handled within the application.</td>
<td></td>
</tr>
<tr>
<td>Workflow</td>
<td>Service</td>
<td>IPCIS</td>
<td>No, no need.</td>
<td></td>
</tr>
</tbody>
</table>


## Appendix 1: References and Related Documents

<table>
<thead>
<tr>
<th>Doc ID</th>
<th>Reference/ Related Document</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>RD1</td>
<td>Project Charter</td>
<td></td>
</tr>
<tr>
<td>REF1</td>
<td>Information System Hosting Services – Guidelines</td>
<td></td>
</tr>
<tr>
<td>REF2</td>
<td>Decision 2002/47/CE, CECA, Euratom</td>
<td></td>
</tr>
<tr>
<td>REF3</td>
<td>Data Protection Regulation No 45/2001</td>
<td></td>
</tr>
<tr>
<td>REF4</td>
<td>OLAF Guidelines for IT Project Owners</td>
<td></td>
</tr>
<tr>
<td>REF5</td>
<td>Reference Architecture for information system development</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX 2: HYBRID ARCHITECTURE ILLUSTRATIVE SCENARIO

The current section aims to illustrate in further detail the message exchange steps that would take place considering the system’s hybrid architecture proposed and discussed in section 4.2.3.1. The scenario considered is a notification process whereby a Polish (PL) Industry wishes to make a notification for waste movement from Poland through the Czech Republic (CZ) and Germany (DE) with a final destination for waste disposal at the Netherlands (NL). The aforementioned Member States were selected in order to illustrate where different actors would connect and how messages would be exchanged considering Member States that have an existing, separate national waste management system and Member States with no such system. To illustrate the discussed scenario we consider:

- Poland (PL) as a dispatch Member State that has no separate waste management system.
- The Czech Republic (CZ) as a transit Member State with no separate waste management system.
- Germany (DE) as a transit Member State that has a separate national waste management system.
- The Netherlands (NL) as a destination Member State that also has a separate national waste management system.

To enhance clarity and avoid repetition, separate diagrams for certain steps have been excluded if they are effectively identical in concept to steps already illustrated. In all cases however details of all messages exchanged are discussed per case. Finally, consider that the illustrated scenario does not intend to be an exact application of the regulation or a depiction of a fully implemented business process. The goal is rather to clarify the role of participating systems and the rules that govern where each actor would connect and how messages are exchanged.

Overview

The following diagram provides an overview of the participating components.

The Central EU application is the hub to which individual separate systems connect to. Its primary purpose as discussed is to act as a message broker, hiding the routing details of individual systems that participate in inter Member State (MS) communication (i.e. not communication internal to a single MS). Its central role allows it to handle centralized technical tasks such as the automatic redelivery of unacknowledged messages but also provide functionality to European Commission (EC) agents and MS Competent Authorities (CAs) in order to follow up the progress of current processes and perform reporting. It is an application hosted centrally by the EC.

The Shared MS application is another application hosted centrally by the EC whose purpose is to provide virtual national applications for each MS that lacks a separate national system for waste management. Although being a single application, Industry and CA users connecting from each MS will only interact with it as if it were a dedicated application for their and only their MS. All messages exchanged that involve...
more than one MS are routed through the Central EU application. For the purpose of the current scenario, the PL and CZ applications are part of this shared application.

The NL and DE subsystems that figure on the diagram represent the distinct national waste management systems for NL and DE respectively. The details of these systems, whether they are a single national centralized application or a fully decentralized solution interconnecting all Industries and CAs, are of no importance to the overall system. What is important is that an adapter component (NL adapter and DE adapter on the diagram) is in place for each system that is responsible for filtering all communication inbound and outbound of the MS in question, converting between national and EU message formats and routing messages to internal national recipients.

Finally, the individual components participating in the overall solution, i.e. the Shared MS application and the NL and DE national waste subsystems (through their adapters) are connected to the Central EU application with a secure and encrypted communication channel (highlighted in red in the diagram).

Step 1: The PL Industry (notifier) initiates a notification process

In this step, the PL Industry user connects to the PL application in the Shared MS application and initiates a notification process sending a request message (“req”). The PL CA, connecting to the same virtual PL application, receives the request.

Once the PL CA user actually opens the received request message, an acknowledgment of receipt is sent directly to the PL Industry following the opposite direction. What is important to point out here is that the Central EU application is not contacted in this case since no communication need currently exists for other MS. Notifying the Central EU application could be foreseen, however it is currently not deemed appropriate since an information imbalance would be created between MS in the Shared application and MS with separate systems. This is due to the fact that such communication taking place e.g. within DE would never be recorded by the central EU application.

Step 2: The PL (dispatch MS) CA approves the request

In this step the PL CA has approved the Industry’s request and the request is ready to be approved by the destination CA of NL as well as the transit CAs of CZ and DE. The approval message (“OK (PL)”) of the PL CA is sent to the PL Industry (the notifier) and a request message (“req”) is sent to the CAs of CZ, NL and DE.
In this step, the Central EU application is contacted to route the approval request to all recipient CAs. This routing through the Central EU application occurs for all messages, including from PL to the CZ CA, even though PL and CZ both participate in the Shared MS application. Concerning the messages to the DE and NL CAs, these are received by their respective national subsystem adapters that take charge of correctly routing them internally. Note that once the CAs of CZ, DE and NL each receive the request, they send an acknowledgement message to all other parties through the Central EU application. Moreover, the acknowledgement of the NL CA sets the time in which the transit CAs need to react.

**Step 3: The NL (destination MS) CA approves the request**

Since the acknowledgement of the NL CA, the transit CAs of CZ and DE are expected to react to the communicated request. At any given point, actors from the EC or the involved Member States can connect to the Central EU application and inspect the overall status of the current notification process. This is a benefit of the hybrid approach versus a decentralized one since there is a single, consistent record of message exchange information.

In the illustrated step we assume that the transit MS of CZ and DE have individually approved the notification request. What is illustrated is the final approval by the destination NL CA, the information flow of which is identical to the aforementioned approvals of the other CAs. The approval message (“Ok (NL)” is sent by the NL CA after connecting to an internal application within the NL waste management subsystem. It is important to point out again that how this occurs is fully up to the national system. The point of interest for the EU-wide solution is when the NL adapter component sends the approval messages to the Central EU application. These messages get routed to the DE CA through the DE adapter, and to the CZ and PL CAs and PL Industry as part of the Shared MS application.
A first important point to make is the communication of the approval by the NL CA to the PL Industry, meaning that not all communication is restricted to CAs. The fact that the (virtual) PL application is the recipient of this message does not necessarily mean that it is meant for the PL CA. Finally, another point to make is that the system does not necessarily expect multiple approval messages from the NL CA (one for each of the other participants). The current proposal indeed foresees that the NL CA will send the approval message to the PL Industry with copies to each other participant CA, however the process could be refined in order to have the Central EU application receive a single message and decide itself, through centralized rules, which parties need to be informed.