European Commission

Feasibility study on interlinked databases, format and basic application to facilitate exchange of information between Poison Centres, according to Article 45 (4) of EC Regulation No 1272/2008 (CLP Regulation)

Final Report

Version 1.2
19/11/2015

Version linguistique	Numéro de catalogue	ISBN	DOI
EN	ET-02-15-133-EN-N	978-92-79-45823-1	10.2873/694243

Main contributors

Philippe Boveroux (Trasys)

Dijana Spasojevic (Trasys)

Eric Swalens (Trasys)

Company details

Trasys

Terhulpsesteenweg 6C
1560 Hoeilaart
Belgium

Telephone: +32/(0)2/893.12.11

Document revisions

1.0	First complete draft version	15/09/2015
1.1	Second version. Major review following comments	09/11/2015
1.2	Final version. Minor edits	19/11/2015

Report document details

Study title	Feasibility study on interlinked databases, format and basic application to facilitate exchange of information between Poison Centres, according to Article 45 (4) of EC Regulation No 1272/2008 (CLP Regulation)
Version linguistique	EN
Numéro de catalogue	ET-02-15-133-EN-N
ISBN	978-92-79-45823-1
DOI	10.2873/694243
Report No.	2015.2164

Executive summary document details

Version linguistique	EN
Numéro de catalogue	ET-02-15-134-EN-N
ISBN	978-92-79-45825-5
DOI	10.2873/282563

DISCLAIMER

Abstract

Harmonisation of the information about hazardous mixtures submitted by industry to Member State Appointed Bodies is an important objective stated in Article 45 (4) of the CLP Regulation (No 1272/2008) and it is expected to provide long-term benefits to all actors of the emergency health response submission scheme.

The definition of unambiguous data requirements and of a business model for the submission data is a first step towards harmonisation: this results in the design of a corresponding XML schema for the future electronic transfer of the data.

An application for encoding a submission and saving it as a format-compliant XML document as well as for viewing a submission is the second practical result of the study. This application has been developed for the benefit of Appointed Bodies and industry, but is particularly geared towards small and medium companies managing a small mixture portfolio.

The study of options for the secure electronic transfer of submissions shows that a semi-centralised system would maximise long-term benefits for all participants, facilitating submission by industry and reducing submission cost, and providing data of better quality to Poison Centres while retaining their autonomy regarding the overall local data management.

Résumé

L'harmonisation des informations relatives aux mélanges dangereux que l'industrie doit fournir aux organismes désignés par les États membres est un objectif important énoncé à l'article 45 (4) du Règlement CLP (n° 1272/2008). Il est attendu que cette harmonisation induise des avantages à long terme pour tous les acteurs du réseau de réponse sanitaire en situation d'urgence.

Une définition claire des données requises par le Règlement et du modèle de données correspondant est une première étape vers l'harmonisation. Cela s'est traduit par la conception d'un schéma XML adapté au transfert électronique des données.

Une application destinée à encoder et à afficher les données, ainsi qu'à les sauvegarder dans un document XML conforme au schéma est le deuxième résultat pratique de l'étude. Cette application a été développée au bénéfice des organismes désignés et de l'industrie, avec une attention particulière pour les petites et moyennes entreprises qui gèrent un petit portefeuille de mélanges.

L'étude des options pour le transfert électronique sécurisé des données montre qu'un système semi-centralisé permettrait de maximiser les avantages à long terme pour tous les participants. Il faciliterait et réduirait le coût de l'envoi des données par l'industrie et fournirait des données de meilleure qualité au centres antipoison tout en conservant leur autonomie en ce qui concerne la gestion locale des leurs données.

Executive summary

The information and views set out in this study are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

This report details the results of a project undertaken for the Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) of the European Commission by Trasys on a '*Feasibility study on interlinked databases, format and basic application to facilitate exchange of information between Poison Centres, according to Article 45 (4) of EC Regulation No 1272/2008 (CLP Regulation)*'.

Article 45 of the EU Regulation No. 1272/2008 on the classification, labelling and packaging of substances and mixtures (CLP) places a requirement on the EU Member States to appoint a body (or bodies) responsible for receiving information on hazardous mixtures. These Appointed Bodies often known as 'Poison Centres', provide a valuable service as part of national health care systems; relaying detailed information on health effects of chemicals within specific products during emergency incidents. Poison Centres play an instrumental role in the safe use of chemicals. In case of exposure to hazardous chemicals, they provide medical advice to general consumers and physicians.

While Article 45 of the CLP Regulation places a requirement to appoint bodies and gather information, it does not define the exact nature or the structure of the information to provide, nor does it specify the format for submitting the information to the Appointed Bodies, leaving these choices to Member States. This has resulted in Member States implementing different procedures, specific data requirements and their own notification formats and tools.

The existence of country-specific requirements and the diversity of submission systems place a significant burden on industry trading across the EU to manage different submissions for the same mixture. It also hinders the exchange of information between Poison Centres.

Recognising these problems, a working paper on the potential harmonisation and the standardisation of data requirements has been drafted by the Commission and discussed at the 14th CARACAL meeting in 2014. This paper supported the establishment of a harmonised format for the submission of information. Additionally, the Commission has launched a cost-benefit analysis to evaluate the cost of harmonising the information to be submitted to Poison Centres. Overall, the cost estimates suggest that there would be net savings of 550 M€ per year for industry across the EU, with the greatest savings made by those companies that trade in most EU Member States.

Building on previous results, this study aims at providing the European Commission with tools to support the electronic submission of information related to hazardous mixtures: (i) define an harmonised XML format for the submission of data to Appointed Bodies in Member States, (ii) develop a basic application to allow creating and viewing submissions, and (iii) analyse options for the secure data exchange between local databases of Member States having different submission systems.

As a prerequisite for these tasks, a study of the existing software used by the current national submission systems has been conducted. An online consultation, which included industry and Appointed Bodies, was opened for five weeks in February and March 2015, and received a good level of responses: 22 responses from Appointed Bodies out of 19 Member States and 160 responses from industry have been collected and processed. The responses were refined via 17 telephone interviews with stakeholders equally selected from Appointed Bodies and industry.

In addition to the identification of specific data requirements and a description of local submission systems, the survey results included a description of the main concerns of involved parties. Appointed Bodies emphasised the poor quality of the data submitted,

the lack of proper mixture identification and the lack of knowledge of industry concerning their obligations to notify. Industry representatives emphasised that their main challenges with the current submission scheme are linked to the differences between Member States (in format and procedure), the lack of versioning of the information and the lack of mixture identification.

The first main input for the definition of the harmonised format has been the Commission's Working Paper on harmonisation discussed at the 14th CARACAL meeting in April 2014 and refined at the 18th CARACAL meeting in June 2015. Another key source of information has been the compilation of Member State-specific data requirements that resulted from the consultation with Appointed Bodies. A first business model of the harmonised data has been developed and presented to stakeholders during a workshop in April 2015. The elaboration of the business model continued over a period of several months, integrating feedback from the workshop participants and the results from working meetings with the Commission services and Poison Centres. Eventually, a model was defined and translated into an XML schema specifying the harmonised format for the electronic submission of information about hazardous mixtures.

In parallel to the definition of the harmonised submission format, the functional specifications for an application to encode and view a submission were proposed, discussed with stakeholders and potential users in Member States and industry, and agreed upon. Essential features expected from the application are clarity and user-friendliness: the application must be easy to use for users in small and medium companies. The application is a "rich internet application" using modern user interface technology allowing direct input validation, clear error reporting and fluid navigation. The application has been developed by iterations and tested by end users from Member States and industry communities, delivering essential feedback incorporated whenever possible in a final version demonstrated during the 19th CARACAL meeting in November 2015.

The last task related to the proposed options for the secure exchange of information between Poison Centres using the harmonised format. This involved defining the security requirements for the data exchange, studying the relevant functional requirements, comparing tools and options, and coming up with a recommendation. The scope of this analysis has been extended from the exchange of information between Poison Centres to include the submission of information by industry to Poison Centres, thereby considering all transactions involving transfer of information on hazardous mixtures.

The study shows that the recommended solution that appears to be the most beneficial for all parties (Member State Appointed Bodies and industry), would consist of a semi-centralised system where (i) industry could submit once for all relevant countries data about the hazardous mixtures that they place on the market in the EU, and (ii) Poison Centres could subscribe to the data they need to fulfil their obligations and import them into their own local database.

Such an approach would benefit industry as it would eliminate the need for multiple submissions of the same data in Member State-specific formats and would allow better traceability of updates to their submissions. On the long term, it would also benefit Poison Centres that should see an improvement to the overall quality of the data submitted. Every exchange of information – submission by industry to the proposed semi-centralized system and export of data to the Poison Centres' local database – would be expected to be carried out in the defined harmonised format via secure data exchange protocols to guarantee data confidentiality.

Résumé opérationnel

Les opinions exprimées dans ce document représentent les points de vue des auteurs et ne reflètent pas nécessairement ceux de la Commission de l'Union européenne. La Commission ne garantit pas l'exactitude des données présentées dans ce rapport. Ni la Commission, ni les personnes agissant au nom de la Commission ne peuvent être tenus pour responsables de l'utilisation faite des informations présentées dans ce rapport.

Ce rapport détaille les conclusions d'un projet réalisé par Trasys pour la Direction générale Marché intérieur, industrie, entrepreneuriat et PME (DG GROW) de la Commission européenne sur une « *Etude de faisabilité sur les bases de données interconnectées, un format de données et une application simple pour faciliter l'échange d'informations entre les centres antipoison, en vertu de l'article 45 (4) du Règlement EC No.1272/2008 (Règlement CLP)* ».

L'article 45 du Règlement européen n° 1272/2008 relatif à la classification, à l'étiquetage et à l'emballage des substances et des mélanges (Règlement CLP) requiert que les États membres désignent un ou plusieurs organismes chargés de la réception d'informations sur les mélanges dangereux. Ces organismes, aussi connus sous le nom de centres antipoison, sont un composant important des systèmes nationaux de santé publique. En cas d'urgence sanitaire ils peuvent transmettre des informations détaillées sur la composition chimique de certains produits et leurs effets. Les centres antipoison jouent un rôle central dans la sécurité d'utilisation des substances et des mélanges. A la suite d'exposition à des produits chimiques dangereux les centres antipoison peuvent donner des conseils d'ordre médical pour assister le grand public et les professionnels de la santé.

Bien que l'article 45 requiert la désignation d'organismes chargés de la réception de la documentation, il ne définit pas la nature exacte ou la structure de l'information à fournir, ni le format dans lequel l'information doit être fournie aux organismes désignés, laissant ces choix aux États membres. Cela a abouti à la définition et à la mise en place par les États membres de procédures différentes, de structures et de formats de données hétérogènes et d'outils de notifications spécifiques à chaque Etat.

L'existence d'exigences spécifiques à chaque pays et la diversité des systèmes de notification représente une charge administrative considérable pour les entreprises qui commercent à travers l'Europe et doivent gérer différents envois pour un même mélange. En outre, cet état de fait limite l'échange d'informations entre les centres antipoison.

Reconnaissant ces problèmes, la Commission a préparé un document de travail sur les possibilités d'harmonisation et de normalisation des données requises par le Règlement. Ce document de travail a été discuté lors de la 14ième réunion CARACAL en 2014. Ce document de travail proposait l'établissement d'un format harmonisé pour l'information à communiquer. En outre, la Commission a lancé une analyse coûts-bénéfices, pour évaluer le coût de l'harmonisation des informations devant être transmises aux centres antipoison. Dans l'ensemble, les estimations suggèrent qu'une économie annuelle nette de 550 millions d'euros pourrait être engendrée pour l'industrie à travers l'Union européenne ; avec les plus grandes économies réalisées par les entreprises qui ont des échanges commerciaux dans la plupart des Etats membres.

La présente étude, qui se base sur ces résultats précédents, vise à fournir à la Commission européenne des outils pour faciliter le transfert électronique d'informations relatives aux mélanges dangereux : (i) définir un format XML harmonisé pour l'envoi des données aux organismes désignés par les Etats membres, (ii) développer une application simple qui permette de créer et de visualiser les données, et (iii) analyser les options pour l'échange sécurisé des données entre les bases de données locales des Etats membres ayant des systèmes de notification différents.

Comme condition préalable à la réalisation de ces tâches, une étude des logiciels utilisés par les systèmes de notification nationaux actuels a été menée. Une consultation en ligne, s'adressant à l'industrie et aux organismes désignés, a été ouverte pendant cinq semaines en février et mars 2015. Elle a reçu un bon niveau de participation avec 22 réponses d'organismes désignés dans 19 États membres et 160 réponses de l'industrie qui ont été collectées et traitées. Ces réponses ont été affinées par le biais d'entretiens téléphoniques avec 17 intervenants choisis de manière équilibrée parmi les organismes désignés et l'industrie.

En plus de la description des données requises et des systèmes de notification particuliers aux Etats membres, les résultats de l'enquête ont mis en évidence les principales préoccupations des parties concernées. Les organismes désignés ont souligné la mauvaise qualité des informations reçues, l'absence d'un mécanisme adéquat pour l'identification des mélanges et le manque de connaissance par l'industrie de ses obligations de notifier les données. Les représentants de l'industrie ont indiqué que leurs principales difficultés avec le système de notification en place sont liées aux différences entre les États membres (dans le format des données et les modalités de notification), l'absence d'un mécanisme d'historisation de l'information et l'absence d'identification des mélanges.

La première source d'information pour la définition d'un format harmonisé a été le document de travail de la Commission sur l'harmonisation discuté lors de la 14ième réunion CARACAL en avril 2014 et affiné lors de la 18ième réunion CARACAL de juin 2015. Une autre source d'information essentielle a découlé de la compilation des différentes données requises par les organismes désignés lors de la consultation.

Un premier modèle harmonisé des données a été élaboré et présenté aux parties prenantes lors d'une réunion de travail en avril 2015. Ce modèle de données a ensuite été complété pendant plusieurs mois en intégrant les commentaires des participants à l'atelier et les résultats de réunions de travail avec le services de la Commission et les centres antipoison. Finalement, un modèle a été défini et traduit dans un schéma XML qui spécifie le format harmonisé pour la transmission électronique de l'information requise sur les mélanges dangereux.

En parallèle à la définition du format de données harmonisé, les spécifications fonctionnelles d'une application destinée à encoder et afficher ces données ont été proposées et discutées avec les utilisateurs potentiels de l'application dans les États membres et l'industrie. Les principales caractéristiques attendues de l'application sont la clarté et la convivialité : l'application doit être facile à utiliser pour les utilisateurs dans les petites et moyennes entreprises. Il s'agit d'une « application internet riche » qui met en œuvre une interface utilisateur moderne, permet la validation directe des données entrées, fournit des messages d'erreur clairs et assure une navigation fluide. L'application a été développée par itérations et testée par les utilisateurs finaux des Etats membres et de l'industrie qui ont fourni des retours d'expérience qui ont été incorporés dans la version finale qui a pu être montrée au cours de la 19ième réunion CARACAL de novembre 2015.

La dernière tâche consistait en la présentations d'options pour l'échange sécurisé d'informations entre les centres antipoison en utilisant le format harmonisé. Cela a demandé de définir les exigences de sécurité pour l'échange de données, d'étudier les exigences fonctionnelles afférentes au métier, de comparer les outils et de proposer une recommandation. La portée de cette analyse n'a pas été limitée à l'échange entre centres antipoison et a été étendue à l'envoi d'informations par l'industrie aux centres antipoison, intégrant dès lors toutes les transactions impliquant le transfert d'informations sur les mélanges dangereux.

L'étude montre que la solution recommandée qui semble être la plus bénéfique pour toutes les parties (Organismes désignés par les États membres et l'industrie) serait constitué d'un système semi-centralisé dans lequel (i) l'industrie pourrait notifier une seule fois pour tous les pays concernés les informations requises sur les mélanges dangereux mis sur le marché dans l'Union, et (ii) les centres antipoison pourraient s'abonner aux données nécessaires à l'exécution de leurs missions et les importer dans leurs bases de données locales.

Une telle approche serait avantageuse pour l'industrie car elle permettrait d'éliminer la nécessité de notifier la même information dans des formats spécifiques aux États membres et assurerait une meilleure traçabilité des mises à jour de l'information. Sur le long terme, elle serait également bénéfique pour les centres antipoison qui devraient voir une amélioration de la qualité globale des données reçues. Tous les échanges d'informations – l'envoi des données par l'industrie au système semi-centralisé et le transfert de celles-ci par les centres antipoison vers leurs bases de données locales – devraient être effectués dans le format harmonisé et par l'intermédiaire de protocoles sécurisés d'échange de données.

Table of Contents

Tables

Figures

1 Introduction

1.1 Background

Consumers and workers come daily into contact with numerous chemicals, including sometimes hazardous substances and mixtures, be it in their private life or in their occupational environment. Although substances and mixtures placed on the market are expected to be safe when used according to their instructions, unintentional exposure to chemicals contained therein by ingestion, inhalation or through skin contact can occur for example through accidents or the inappropriate use of products.

Informing medical personnel (physicians, veterinarians, pharmacists) and/or the public about symptoms and treatment of acute intoxications is the main task of Poisons Information Centres. To fulfil this task adequately, information about the involved product(s) is crucial, especially information about the composition and the concentration of the ingredients.[1]

Article 45 (1) of Regulation (EC) No 1272/2008 on classification, labelling and packaging of substances and mixtures (hereinafter: the CLP Regulation[2]) states that the Member States (hereinafter MS) *"shall appoint a body or bodies responsible for receiving information relevant, in particular, for formulating preventative and curative measures, in particular in the event of emergency health response, from importers and downstream users placing mixtures on the market".*

However, the Regulation does not specify which authority should be appointed and whether this should be a Poison Centre or another institution. Also, the Regulation does not define a process for submission of information, allowing each Member State to develop its own specific requirements and a process for submission.

Article 45(4) of the CLP Regulation requires the Commission to carry out a review to assess the possibility of harmonising the information provided to poison centres for formulating preventive and curative measures in the event of emergency health responses. The work was carried out following the consultation with relevant stakeholders and with the support of the European Association of Poison Centres and Clinical Toxicology (EAPCCT) and the Review was published in early 2012.[3]

In the context of Article 45(4), the European Commission awarded a contract to TRASYS to carry out a study on interlinked databases, format and basic application to facilitate exchange of information.

1.2 Objectives of the study

The objectives of the study are to provide the Commission with:

i) An harmonised **data submission format** in XML following the XML Schema Definition (XSD) standard.

   The definition of an harmonised format is the prerequisite for the development of standard submission interfaces and the electronic exchange of data between

[1] DG Enterprise and Industry, Harmonisation of Information for Poison Centres, Stakeholder Workshop Report, Brussels, 24 November 2010 (http://ec.europa.eu/enterprise/sectors/chemicals/files/clp/workshop_report_en.pdf – Accessed on 15/10/2015).

[2] Regulation (EC) No 1272/2008 of the European Parliament and of the Council of 16 December 2008 on classification, labelling and packaging of substances and mixtures, amending and repealing Directives 67/548/EEC and 1999/45/EC, and amending Regulation (EC) No 1907/2006 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:353:0001:1355:en:PDF – Accessed on 15/10/2015).

[3] Harmonisation of Information for Poison Centres, Review according to Article 45(4) of Regulation (EC) No 1272/2008 on classification, labelling and packaging of substances and mixtures (http://ec.europa.eu/enterprise/sectors/chemicals/files/clp/review_art45_4_clp_final_en.pdf – Accessed on 15/10/2015).

industry and Competent Bodies as well as between Poison Centres. It is also an essential requirement for a possible harmonisation of the submissions process across the Competent Bodies.

ii) A **basic application** for input of data in the defined format.

This application will allow creating a submission in the harmonised format and saving it as a file. It will also permit viewing and updating a submission.

iii) The format and the application provide the building blocks to create submissions. Parts of a submission being confidential, submissions cannot be exchanged without securing the exchange. The third delivery of this study is thus an analysis of **options for secure data exchange** between MS Appointed Bodies.

1.3 Structure of the report

This Final Report is organised into the following sections:

- Section 1, the current section, provides the general context.
- Section 2 briefly describes the project approach. A detailed project description is provided in the project Inception Paper [INCEPTION][4].
- Section 3 details the results of the study on the applications presently used by national/regional Poison Centres, with a focus on submission mechanism and supporting IT systems.
- Section 4 presents the harmonised format and its representations in UML and XML.
- Section 5 introduces the basic application.
- Section 6 indicates the possible options for the secure exchange of data between Poison Centres.

1.4 References

Documents referred to in this report are listed below.

Table 1-1: External references

Reference	Description
[CLP]	Regulation (EC) No 1272/2008 of the European Parliament and of the Council of 16 December 2008 on classification, labelling and packaging of substances and mixtures, amending and repealing Directives 67/548/EEC and 1999/45, and amending Regulation (EC) No 1907/2006 O. J. L 353, 31.12.2008
[CA/48/2015]	18th Meeting of Competent Authorities for REACH and CLP (CARACAL), 23-24 June 2015

Table 1-2: Project references

Reference	Description
[INCEPTION]	Inception Paper, version 1.0, 27/02/2015 *Inception Paper v1.0.docx*
[INTERIM]	Interim Report, version 1.3, 19/06/2015

[4] A reference in bracket points to a document in the reference table in section 1.4.

Reference	Description
[BULK_NOTE]	Proposal for bulk submissions of information relating to emergency health response, version 1.3, 19/06/2015 *Poison Centre study – Bulk submission v1.3.docx*
[GLOSSARY]	Business Glossary, version 1.1, 16/06/2015 *Poison Centre study – Business Glossary v1.1.docx*
[DATA_MODEL]	UML data model for the harmonised format *PC data model – Submission.jpg* (Diagram) *PC data model – Mixture details.jpg* (Diagram)
[XML_SCHEMA]	XML schema for the harmonised format *PC XML schema.doc* (Word generated by XMLSpy) *PC XML schema.html* (XMLSpy HTML export)
[BASIC_APP_SPEC]	Basic application - Specifications *Basic application specifications.docx*
[QUEST_MS]	Questionnaire for Member States Appointed Bodies *PoisonCentresQuestionnaire4MS2015_10-02-2015_EN.pdf*
[QUEST_MS_24]	Attachment for question 24 in Member States Appointed Bodies questionnaire *PoisonCentresQuestionnaire4MS - Question 24.pdf*
[QUEST_IND]	Questionnaire for industry *PoisonCentresQuestionnaire4Industry2015_10-02-2015_EN.pdf*
[ANSWERS]	Consolidation of answers to the questionnaire *PoisonCentresQuestionnaire4MS - All answers - Charts and pivots.xlsx*
[ANSWERS_MSAB_Q19]	Consolidated answer to MSAB question 19 *PoisonCentresQuestionnaire4MS - Question 19 Consolidation.pdf*
[ANSWERS_MSAB_Q24]	Consolidated answer to MSAB question 24 *PoisonCentresQuestionnaire4MS - Question 24 Consolidation.pdf*

1.5 Abbreviations

Abbreviations used in this report are listed below in alphabetic order.

Table 1-3: Abbreviations

Acronym	Definition
CA	Certification Authority
DMS	Document Management System
EAN	European Article Number (International Article Number)
EEAPCT	European Association of Poison Centres and Clinical Toxicologist
MS	Member State
MSAB	Member State Appointed Body
PC	Poison Centre
PCS	Product Categorisation System
PKI	Public Key Infrastructure

Acronym	Definition
SDS	Safety Data Sheet
UFI	Unique Formula Identifier
UML	Unified Modelling Language
UCI	Unique Company Identifier
UFI	Unique Formula Identifier
UPI	Unique Product Identifier
XML	eXtensible Markup Language
XSD	XML Schema Definition

2 Project approach

The project has been developed and implemented in 4 phases, each one having specific objectives, work packages and deliverables:

First phase *Analysis of the current situation* includes activities for launching the project, collecting business and users requirements, and analysing the selected existing EU national/regional databases. During this phase, the project aimed to cover the following questions: What is the current body of knowledge with regards to the harmonisation of information for Poison Centres? How is the process of submitting information carried out in the selected Member States? Which submission systems are currently in place and how they function? Which data is requested from submitter by the national authorities?

Understanding of the current situation is a prerequisite to defining an harmonised submission format. The approach followed for this analysis and its results are described in section 3.

Second phase *Preparation of a harmonised XML format* aims at defining the most appropriate XML format that can be used in the context of the submission of information according to Article 45 of CLP.

The harmonised format is defined in detail in section 4.

Third phase *Development of a basic application* for input of data comprises activities for the specifications, development and testing of a software application to be used by submitters and Poison Centres.

In practice, this phase is directly dependent of the previous one since the software technical specifications must include the definition of the harmonised XML format.

The basic application is discussed in section 5.

Fourth phase *Analysis of options for secure electronic data exchange* starts from the results of the previous phases with the objective to describe pros and cons of different architectural alternatives in order to exchange confidential data between EU Poison Centres.

The options for secure data exchange are presented and assessed in section 6.

3 Analysis of the current situation

This section presents the results of the analysis of the current situation.

The analysis and comparison of existing Member State specific systems has been performed following an approach based on **desk research**, **questionnaire-driven consultation** and structured **phone interviews** with the following benefits:

- It allows the consultation of a wide group of stakeholders through a questionnaire process.
- Distinct questionnaires with specific questions can be prepared for each type of stakeholder.
- The pre-validation of the questionnaire with a small group of key stakeholders assures that all important topics are covered and that the questions are well understood.
- A follow-up of the responses to the questionnaire is performed through interviews, focusing on a subset of stakeholders with a valuable contribution/insight and ready to contribute.

This phase must also allow to:

- Review the systems currently used by the Member State Appointed Bodies.
- Assess which information is currently requested by Member State Appointed Bodies from submitters.

3.1 Methodology for stakeholder consultation

The stakeholder consultation process was carried out using **structured questionnaires** and **interviews**.

3.1.1 Structured questionnaire

The process for preparation of the questionnaire included the following steps:

1. Creation of the questionnaire.
2. Validation of the questionnaire through a review cycle with the Commission services and a small group of key stakeholders.
3. Identification of the stakeholder contacts.
4. Contact the stakeholders by email to invite them to participate to the consultation. A 15 working day time span is given to reply. A reminder is sent after 10 days with a deadline extension to 20 working days.
5. Collect the replies and answer questions during the consultation period.
6. Close the questionnaire.
7. Analysis of the replies.

Two structured questionnaires designed for the consultation process with Member States Appointed Bodies (MSBA) [QUEST_MS] and industry [QUEST_IND] were launched using the online EUSurvey tool[5] from 11th February 2015 until 11th March 2015.

An invitation to participate in the survey was sent to responsible authorities in 28 Member States and all regional Poison Centres (PC) of France, Germany, Italy, Poland and United Kingdom. In addition this was discussed at the meeting of the REACH and CLP competent authorities (CARACAL).

[5] https://ec.europa.eu/eusurvey/

22 institutions from the following 19 Member States responded to the survey. They are listed below in alphabetic order of the country.

- Austria: Poison Information Centre Vienna, Austria Gesundheit Österreich GmbH (Austrian Health Institute).
- Croatia:
    - Institute for Medical Research and Occupational Health, Poison Control Centre.
    - Croatian Institute for Toxicology and Anti-doping (CITA).
- Cyprus: Department of Labour Inspection (DLI) Ministry of Labour, Welfare and Social Insurance.
- Estonia: Estonian Poisoning Information Centre (Health Board) – EPIC.
- Finland: Finnish Safety and Chemicals Agency (TUKES).
- France: Centre antipoison et de toxicovigilance de Nancy.
- Germany: Bundesinstitut für Risikobewertung (BfR) (Federal Institute for Risk Assessment).
- Hungary: National Center of Public Health.
- Ireland: National Poisons Information Centre of Ireland.
- Italy:
    - Region of Pavia: Poison Control Centre and National Toxicology Information Centre, Toxicology Unit, IRCCS Maugeri Foundation.
    - Region of Florence: Poison Control Centre Azienda Ospedaliero Universitaria Careggi (AOUC).
    - Region of Puglia: Poison Center, University Hospital OO.RR. Foggia.
- Lithuania: Poisons Control and Information bureau ao the Health Emergency Situations Centre of the Ministry of Health.
- Poland: Bureau for Chemical Substances.
- Netherlands: Nationaal Vergiftigingen Informatie Centrum, NVIC (National Poisons Information Centre).
- Norway: Norwegian Environment Agency, Products and Chemical Registration Section.
- Romania: National Institute of Public Health Romania.
- Slovakia: National Toxicological Information Centre (NTIC), University Hospital Bratislava.
- Slovenia: Chemicals Office of the Republic of Slovenia (CORS).
- Spain: Instituto Nacional De Toxicologia Y Ciencias Forenses (INTCF) - Spanish Poison Centre.
- Sweden: Swedish Poisons Information Centre.

The geographical repartition of MSCA respondents is shown on the map below.

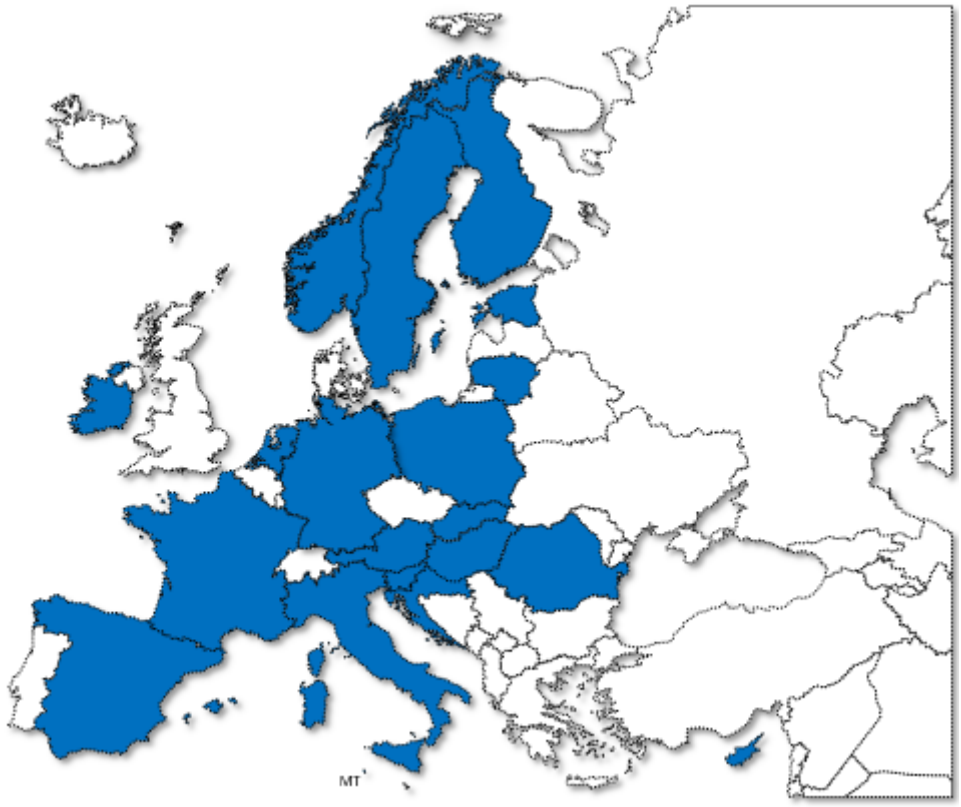


Figure 3-1: MSCA respondents to the questionnaire

The following 7 industry associations were also invited to distribute the invitation to answer the questionnaire to their company members:

- CEFIC, the European Chemical Industry Council - http://www.cefic.org/
- A.I.S.E., International Association for Soaps, Detergents and Maintenance Products - http://www.aise.eu/
- FECC, the European Association of Chemical Distributors - http://www.fecc.org/fecc/
- CEPE, the European Confederation of Paint, Printing Ink and Artists' Colours Manufacturers Associations - http://www.cepe.org/efede/public.htm
- EIGA, the European Industrial Gases Association - https://www.eiga.eu/
- UEAPME, European Association of Craft, Small and Medium-size Enterprises - http://www.ueapme.com/
- ECPA, European Crop Protection Association - http://www.ecpa.eu/

160 industry representatives (companies and associations) responded, providing feedback from a companies of various sizes and from different sectors. The profile of industry respondents will be detailed in section 3.3.1 below.

The geographical repartition of industry respondents is shown on the map below.

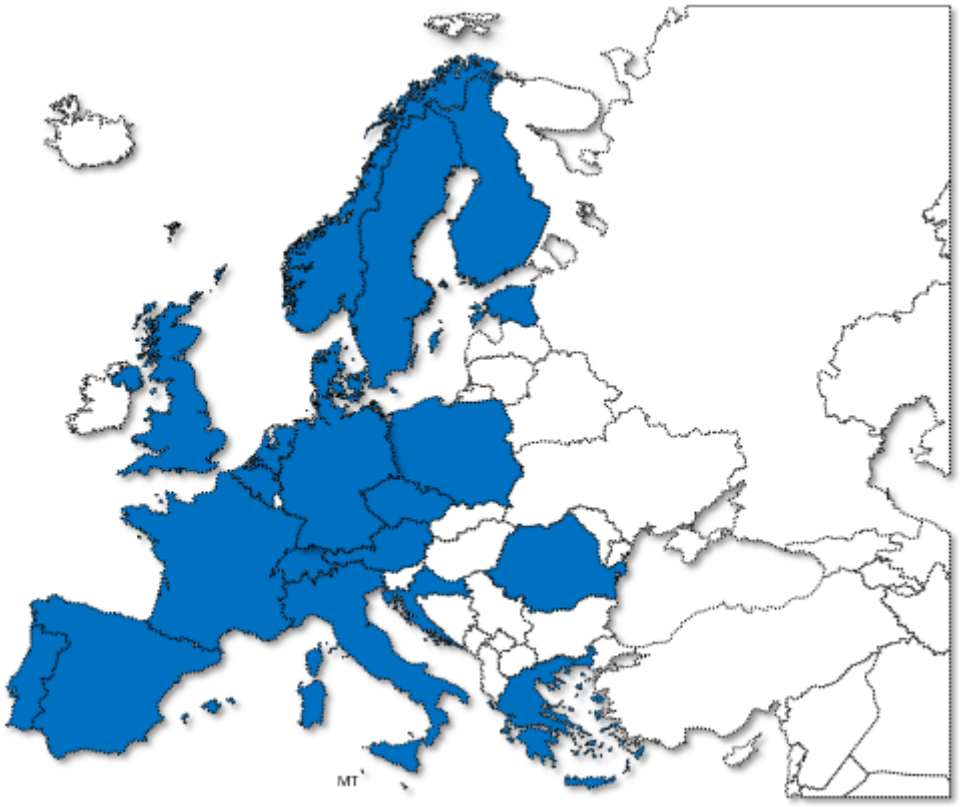


Figure 3-2: Industry respondents to the questionnaire

Answers to the questionnaires from Appointed Bodies and industry are discussed in section 3.2 *Existing practices in Member States for notification submission process* and 3.3 *Industry perspective* respectively.

3.1.2 Interviews

As a result of a first screening of the received filled questionnaires, 8 Member State Competent Authorities (Germany, Netherlands, France, Spain, Poland, Lithuania, Finland and Norway) and 11 companies were interviewed.

The selection of companies has been made to ensure a balance between sector of activity, company size and country as shown in Table 3-1.

Table 3-1 Selected interviewed companies criteria

#	Chemical sector	Size	Country
1	Paints, Coatings & varnishes	Less than 50	Netherlands
2	Fragrances	50-99	UK
3	Agrochemicals	100-199	Germany
4	Consumer chemicals & cleaning products	Less than 50	Portugal
5		200-499	Italy
6	Speciality & fine chemicals	500-1000	Italy
7	Basic chemicals & polymers	More than 1000	Germany
8	Adhesives & sealants	More than 1000	France
9	Printing inks	200-499	UK
10	Oil refining & biorefinary	500-1000	Netherlands
11	Regeneration of waste oil	100-199	Italy

3.2 Existing practices in Member States for submission process

Information provided by Member State authorities in their answers to the survey about the submission mechanism and the underlying IT systems have been gathered and consolidated in a supporting document [ANSWERS].

The following sections focus on particular aspects of the existing process and provides an inventory and classification of IT systems.

3.2.1 Process for the submission of information

As mentioned in the introduction, the CLP Regulation does not specify which information have to be submitted by a submitter to Appointed Bodies, nor how this should be done. Each Member State is free to define its own requirements for the structure of the data and the submission process.

Analysing the responses received from the Member State authorities requires sorting them according to the following criteria:

- **Authority receiving** the submissions. There are two cases:
    - The **Poison Centre (PC)** is the (legal) authority/appointed body for receiving information about products from companies. Information may then be either distributed to or accessed by authorised government institutions (e.g. Ministry of Health, local chemical safety authorities, etc.)
    - A **government authority**, like the Ministry of Health, is the legal authority/appointed body for receiving information about products from companies, which are then either distributed to or accessed by the Poisons Centres (PC).
- **Content of the submission**: Which information has to be notified.
- **Format** of the submission.
- **Submission mean**: How the notification is submitted.
- **Information storage**: How the notification is stored. There are two distinct situations:
    - The submissions are stored in a unique database.
    - The submissions are replicated in several databases.
- **Information access**: Who may access the information.

This information is available in Table 3-2 below for each of the 19 institutions that participated to the survey[6].

[6] Member States are sorted in alphabetic order.

Table 3-2: Submission process

Member State	Receiving authority	PC?	Submission content	Format	Submission mean	Information storage	Replica?	Information access
Austria	Environment Agency Austria	No	SDS(†)	File	Email	SharePoint database	No	Poison Centre
Croatia	Croatian Institute for Toxicology and Anti-doping (CITA)	No	SDS	File	Email	SDS Registry	No	Poison Centre
Cyprus	Department of Labour Inspection (DLI)	No	Requested data(‡) + SDS	MS Excel form + File	Email or post mail	n.a.(*)	No	Poison Centre
Estonia	Estonian Poisoning Information Centre (EPIC)	No	SDS	File	Email	Database / Chapters 2 and 9 of SDS manually keyed in	No	Poison Centre
Finland	Finnish Safety and Chemicals Agency (TUKES)	No	SDS	File	Email	Database / Chapters 1, 2 and 3 of SDS manually keyed in	No	Poison Centre
France	Institut National de Recherche et de Sécurité (INRS)	No	Requested data + SDS	Web form	Online (Declaration-Synapse)	Database (BNPC)	No	Poison Centres / Ministry of Health / Health security agencies (InS, Anses)
Germany	Federal Institute for Risk Assessment (BfR)	No	Requested data	XML (generated with a 'basic application') or PDF form	Web upload or email	Database (GIFAS)	Yes	Poison Centre / Statistics with Federal Ministry

Member State	Receiving authority	PC?	Submission content	Format	Submission mean	Information storage	Replica?	Information access
Hungary	National Centre of Public Health	No	SDS + Label	Web form + File	Online (OSZIR)	Registry of notified products	No	Poison Centre
Ireland	National Poisons Information Centre of Ireland (EPIC)	Yes	Requested data + SDS	MS Word form + File	Email or CD by post mail	Document Management System / Metadata and indexing information added manually	No	Poison Centre
Italy	National Institute of Health	No	Requested data	Web form	Online	ISS database	Yes	Poison Centre
Lithuania	Environmental Protection Agency	No	Requested data	Web form	Online, email or post mail	Database (AIVIKS/ICISEM)	No	Poison Centre
Netherlands	National Poisons Information Centre (NVIC)	Yes	Requested data + SDS	PDF file	Online	Database	No	Poison Centre
Norway	Norwegian Environment Agency	No	Requested data + SDS	PDF or XML format	Online	Product Register and SDS database (Product Information Bank)	No	Poison Centre
Poland	Bureau for Chemical Substances	No	Requested data + SDS	Paper document / Web form / SDS in PDF	Online (ELDIOM), email or post mail	Database	No	Poison Centre / Enforcement bodies / MSAB

Member State	Receiving authority	PC?	Submission content	Format	Submission mean	Information storage	Replica?	Information access
Romania	National Institute of Public Health	No	SDS	File	Email, CD or hard copy via post mail	n.a.	No	No one yet. Poison Centres when IT in place
Slovakia	National Toxicological Information Centre (NTIC)	No	SDS	File	n.a.	Database	No	No one yet
Slovenia	Chemicals Office of the Republic of Slovenia (CORS)	No	Requested data	Web form	Online (ISC)	Database	No	Poison Centre
Spain	Instituto Nacional De Toxicologia Y Ciencias Forenses (INTCF)	Yes	Requested data + SDS	XML + File	Specific application to generates the export file (XML format), with attached PDFs. Files are sent on CD by post mail	Database (INTCF)	No	Poison Centre
Sweden	Swedish Poisons Information Centre	Yes	Requested data	File	Email or on a USB stick/ CD/DVD by post mail	Database	No	Poison Centre

Notes:

†: SDS in the 'Submission content' column means that the information requested is the product Safety Data Sheet.

‡: Requested data in the 'Submission content' column means that the information requested is specific.

*: n.a. in a table cell indicates that the information is not available or could not be deduced from the answer provided.

The following initial conclusions can be inferred from the above table:

- As the 'Submission content' column reveals, several Member States request only the product SDS as valid submission. The others request that some specific information is provided, generally accompanied with the SDS. The following section will detail this case, but it is correct to state that product SDS is almost universally required by Appointed Bodies.
- Most of the Appointed Bodies to whom industry must submit the information are not Poison Centres and a mechanism thus needs to be put into place in each Member State to allow Poison Centres personnel to access the data relevant to their duties. That mechanism is generally providing networked access to the database.
- The vast majority of systems is "centralised"; that is, the submissions are stored into and accessed from a unique database. In a few Member States the decision has been made to disseminate the data in several regional databases; this is for instance the case in Germany.
- If several Member States already have online IT systems in place for the submission of information by industry, quite a few have not and only rely on simpler electronic exchange of documents (email) or even post mail.
- There exists a great variety in solutions in every aspects of the submission process, and particularly in two key areas: the submission mean and the submission format. They will be detailed in sections 3.2.6 and 3.2.7.

3.2.2 Information requested from submitter by Member States

This section consolidates the answers to question 19 of the Member State survey.

> Question 19: *Which data have to be submitted by notifiers? Please, specify. If you use any special form(s), please send us an example of the form.*

Table 3-3 below summarises which information is requested by a Member State when the SDS is not the unique information required. Where possible a reference is made to the submission document/file that must be used by submitters.

The data requirements have been grouped and summed up in a unique table. This information has been used to design the proposed data model for electronic submission that will be detailed in section 4 *Harmonised submission format* below.

Table 3-3: Information requested by Member State beyond SDS

Member State	Submission content	Details / Comment / Reference
Cyprus	Requested data + SDS	A specific Excel form is used to encode a submission. The SDS is requested as well.
France	Requested data + SDS	Trade name; Product codes; Company details; Submitter details; Uses; Quantitty; Packaging; Marketing dates; Physical properties; Components; Labelling
Germany	Requested data	A specific macro-enabled Excel form to generate a XML document or a PDF form (with less information than the Excel/XML) The Excel/XML format caters for multiple submissions.

Member State	Submission content	Details / Comment / Reference
Hungary	SDS + Label	The Safety Data Sheet in Hungarian and the draft label also in Hungarian (the latter one is only required for hazardous substances).
Ireland	Requested data + SDS	Product name; Authorisation number, if available e.g. for plant protection products and biocides; Registered use, if applicable e.g. for plant protection products and biocides; Mechanism of action, if relevant e.g. for plant protection products and biocides; Composition, including all ingredients to 100%; Name and contact details for company submitting the data; Safety Data Sheet or Information about risk and safety phrases, and some physiochemical data such as appearance and molecular weight; Information regarding absorption, distribution and half-life, acute toxicity data, long term toxicity data, short term toxicity data, reproductive toxicity data; The signs and symptoms of poisoning, any diagnostic measures, immediate treatment and antidotal treatment if available
Italy	Requested data + SDS	Product name; Use; Producer; Distributor; Physical properties; Components; Toxicological information
Lithuania	Requested data	Name; market name; composition (within the limits of the MSDS); quantities; classification and labelling; field of usage; toxic, ecotoxic, physical properties and safety measures. No detail is given as to which properties must be notified.
Netherlands	Requested data + SDS	The PC accepts a Safety Data Sheet (SDS) with additional information on the composition of the product.
Norway	Requested data + SDS	Company: Company name, address and contact persons. Product: Trade name; hazards classification (health, fire and environment); industrial code for use and product description; 100% composition (CAS or EC number and exact weight in %); some physical information (consistency, pH, density)
Poland	Requested data + SDS	Name of product; EAN code if available; information whether it is: biocidal product, detergent, nano form; composition (that given in the SDS at least); classification; use sector; category of use (ECHA descriptors); SDS as attachment
Slovenia	Requested data	Data from Safety Data Sheet (including complete SDS electronic file), partial composition (substances , w. conc.), areas of use

Member State	Submission content	Details / Comment / Reference
Spain	Requested data + SDS	Product name; category; pH; composition (quantitative and in percentage ranges); hazard classification; uses; presentation (solid/liquid/gas, colour, packaging size and format); ID of manufacturer; notifying company; marketing company (company name, address, phone, email, contact person, etc.); date of submission; internal product reference number
Sweden	Requested data	A Word file is available for the submission. It is mostly unstructured as most of the requested information (i.e. uses, packaging, physical data) is free text.

It is notable that most Member States require that the product SDS is attached to the submission, also when more detailed information are requested. It is worth noting that SDS may be accepted as part of the submission of information because part of the data requested are available in this document. However, SDS rarely contain information on the complete composition of mixtures and so are generally not conformant to the information requirement set out in the Regulation and are not completely adequate for Poisons Centres' needs.

3.2.3 Submission data requested by the current national process

This section consolidates the answers to question 24 of the Member State survey. The question specifically requested that respondent indicate which data elements listed in the current Commission working paper are requested and whether additional data would be required.

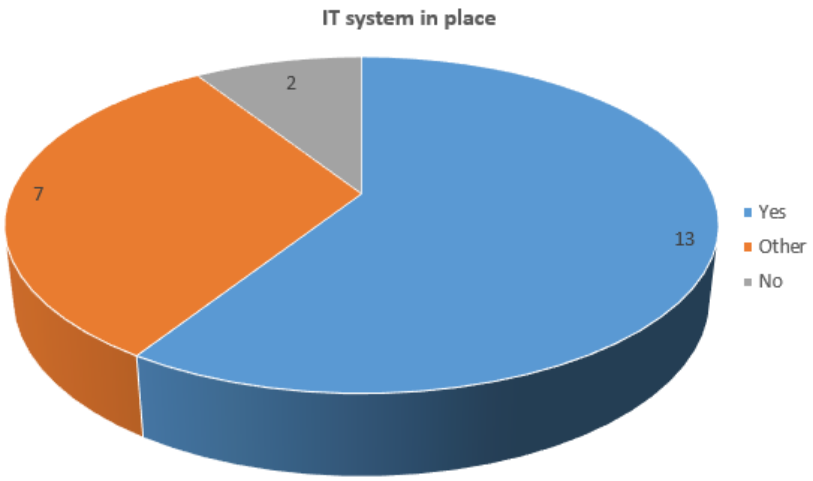
> Question 24: *In the attached Excel sheet the information to be submitted is summarized according to the current Commission working paper. For each section please indicate if that data is required in your current process and/or if you ask for additional data from the industry.*

These data requirements have been added to the table constructed the previous section and are available in [ANSWERS_MSAB_Q24].

The consolidated information has been used to design the proposed data model for electronic submission that will be detailed in section 4 *Harmonised submission format* below.

3.2.4 IT systems for submission

According to the answers, 13 out of the 22 Member State authorities that responded indicated there exists an IT system in place for receiving information on hazardous mixtures.



The two Member States that replied 'No' are:

- Estonia. No dedicated system is in place for receiving information: SDS are sent by email and partly encoded manually into a database by the authority.
- Ireland. No dedicated system is in place for receiving information: submissions (MS Word files and SDS) are sent by post mail and stored in a Document Management System (DMS) with metadata and indexing information added manually.

Seven respondent replied 'Other' and provided the following comment:

- Croatia (2 answers received): The submission (SDS) is submitted in electronic form via e-mail or some another electronic media (CD, USB stick ...) via post mail, and are then transferred to the electronic SDS registry. The nature of that system is not specified.
- Cyprus: The information is submitted either by email or by post. Files sent by email are kept confidential in a "password protected folder". Hard copies sent by post are securely stored in the Department's Archive.
- Sweden: The companies are required to send their product information (one MS Word file for each product, either by email, on a USB stick or on a CD/DVD) along with a table providing simple metadata for the notified products (company name, manufacturer name, product name, date.) The nature of the underlying storage system is not specified but it can be assumed this is a simple Document Management System with elementary search capability (using the provided metadata provided.)
- Romania: There is no IT system for submission in place as of today and one is expected to be functional in mid-2016.
- Austria: SDS are sent by email or post mail and stored in a Document Management System.
- Finland: Submissions in PDF format are sent by e-mail and information from sections 1, 2 and 3 of the SDS are manually keyed in into a database.

Table 3-4 shows the information from the angle of the submission system for the 19 Member States that have responded.

Table 3-4: Submission mechanism

Submission mechanisms	Total
Online	6
Online / Email	1
Online / Email / Post mail	2

Submission mechanisms	Total
Email	4
Email / Post mail	4
Post mail	1
Unknown	1
Grand Total	**19**

In other words:

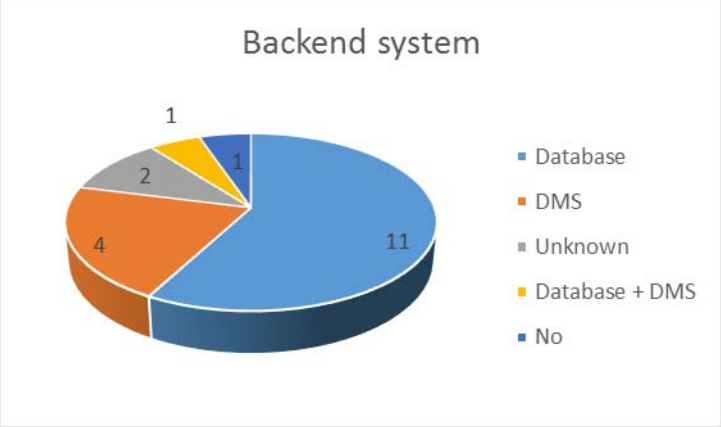
- 9 Member States have an online submission system. Some also do accept email and/or post mail submissions (when the submission is a document such as a SDS.)
- 8 Member States receive submissions by email. Some also accept post mail submissions.
- 1 Member State receives submissions by post mail.
- 1 Member State provided unclear answer.

3.2.5 Backend IT systems

As indicated in previous sections, there is a wide diversity in the submission systems in place in the EU. When considering "backend systems", the systems where data is stored and processed, only two main options exist: database and document management system (DMS).

Table 3-5: Backend IT systems

Backend system	Total
Database	11
DMS	4
Unknown	2
Database + DMS	1
No	1
Grand Total	**19**



3.2.6 Brief description of IT systems

As shown in section 3.2 and in particular Table 3-2: Submission process, a wide variety of IT systems exist. It is possible to classify the systems according to several criteria as follows.

Implementation model

We can distinguish two distinct implementation models:

- Custom development: The application and its database results from a custom development, specific to the organisation.

- Standard or off-the-shelf application: The application relies on an existing product available on the market – for instance, a Document Management System such as SharePoint – with some adaptations/configuration to make it suitable for the task of the Poison Centre.

Availability of a submission front-end to industry

- No frontend: No application frontend is available to industry. The information is therefore submitted by other means such as emails, CD-ROM, etc.
- Web portal: The application provides a web frontend accessible on the Internet. Industry representatives can login into the system and manage the information for their company.

It is noteworthy that none of the existing IT systems seem to offer a machine-to-machine interface (such as web services) for industry to automatically upload submissions.

Information collected

The information collected is another criteria that helps classifying the existing situation.

- Safety Datasheet (SDS) only: The collected information is limited to the SDS of the product. In most cases the SDS is sent as a PDF document, with the exception of Norway that accepts SDS in the SDSComXML format established by the eSDSCom Alliance[7].
- Custom data: The data to provide is explicitly defined by the national body in charge of collecting the information. This takes the form of specific fields on-screen when there is a web portal or of PDF forms or Excel sheets (with possible extraction of the data in XML) otherwise.

  The SDS is also provided additionally to the custom data in many cases.

Architecture of the system

- Central system: industry submits the information to a central system. That system is also queried by the Poison Centres when they require information about a product.
- Central system with dissemination to Poison Centres: industry submits the information to a central system. Data is then sent to the Poison Centres that store it in their local system (the latter is queried when information about a product is needed).

3.2.7 Strengths and weaknesses of the current approach

This section summarises the strengths and weakness commonly given in answers to question 31.

> Question 31: *What are the weaknesses and strengths of the current approach with regard to receiving information from importers and/or downstream users placing hazardous mixtures on the market? Please, elaborate.*

Expressed strengths and weaknesses do not apply globally to all Member States as they depend on the exact procedure in a Member State, but they enable to identify a number of topics that require attention in the harmonisation process.

Weaknesses perceived by the responding Member States in the various current national approaches include

- The poor quality of the submitted data. (AT, CR, DE, ES, FR, LI, NL, SK, SE)

[7] http://www.esdscom.eu/english/sdscom-xml/

The information is often incomplete or poorly filled (notably in the SDS).

The lack of structure prevents automated checks, performing consistent searches or presenting the information in a clear way.

Downstream users do not always have access to the complete formulation of the product and are at pain submitting complete information.

- Issues with mixtures in mixtures and the lack of a clear procedure for reporting such products. (DE, ES)
- The difficulties to collect confidential data (including concentration limits). (CY, LI)
- The lack of proper product identification. (FR, NL)

  This weakness notably prevents consistently versioning the product information.
- The lack of knowledge of, or support from, industry concerning their obligations and possibilities to notify. (CR, CY, ES, DE, SE)

  The companies, especially the importers and/or downstream users, are not necessarily well aware that/if they have to notify the Member State authority.

  When the submission of information is not mandatory the companies do not always know that they can voluntarily notify the Member State authority.
- Industry can sometimes object to send different information to different Member States. (ES)
- The lack of a well-defined timeframe to notify the Member State authority (e.g. before the product is placed on the market). (CY)
- The workload required to process the information received from industry, notably when multiple input formats are accepted. (ES, LI)
- The necessity to train and support industry, e.g. for the use of Excel templates or to generate valid XML files. (DE, ES)
- The difficulties in putting in place a secure procedure for information exchange and controlling the identity of the notifying company. (CY, SE)

On the positive side the following strengths of some current national approaches are cited

- SDS are easy to send for industry. (FI)
- Commonly used formats are accepted, thus lowering the costs for industry. (IE)
- The submission procedures are usually simple for companies. (NL)
- When a website is used the information can be processed automatically, making it quickly accessible. (NL)

3.3 Industry perspective

3.3.1 Profile of respondents

160 companies and/or associations replied to the online questionnaire.

Their distribution per country is given in Table 3-6 below. Responses have been given from 20 countries and more than 80% of the answers have been given by the top 7 countries (half by the top 3). It is interesting to note that the first seven countries in this list are also the top registrants under REACH in almost the same order[8].

[8] The overview of REACH registrations by countries is available at http://echa.europa.eu/regulations/reach/registration/registration-statistics/overview-all-countries. The first

Table 3-6: Industry respondent per country

Country	Total	Ratio
Germany	53	33%
France	17	11%
The Netherlands	15	9%
Italy	15	9%
United Kingdom	13	8%
Belgium	10	6%
Spain	9	6%
Switzerland	4	3%
Austria	3	2%
Portugal	3	2%
Sweden	3	2%
Denmark	2	1%
Finland	2	1%
Poland	2	1%
No name-place companies	*2*	1%
Greece	2	1%
Czech Republic	1	1%
Croatia	1	1%
Romania	1	1%
Norway	1	1%
Estonia	1	1%
Grand Total	**160**	**100%**

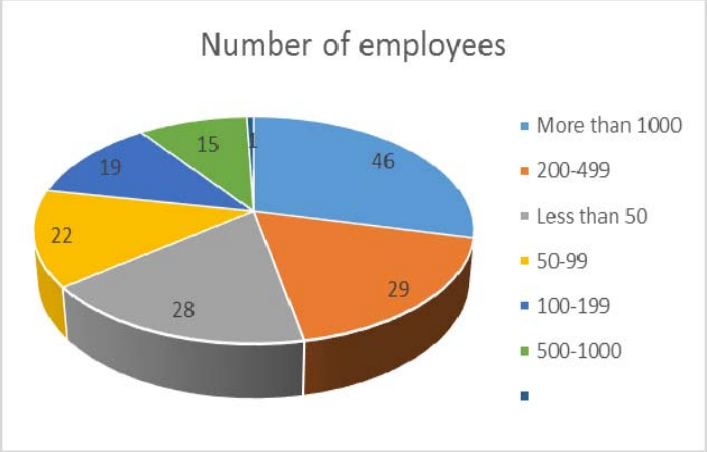
Responding companies can also be sorted by their size, as shown in the following table compiled from the answers to question 8.

Question 8: *What is the number of employees of your company?*

seven countries are Germany, United Kingdom, France, The Netherlands, Italy, Belgium, Spain with 77 percent of the registrations.

Table 3-7: Company size

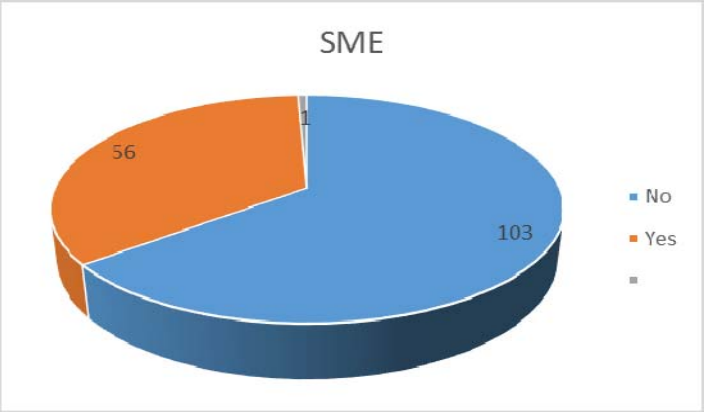
Number of employees	Total
More than 1000	46
200-499	29
Less than 50	28
50-99	22
100-199	19
500-1000	15
Not specified	1
Grand Total	**160**



Two third of the respondent were non-SME as reported below.

Table 3-8: SME

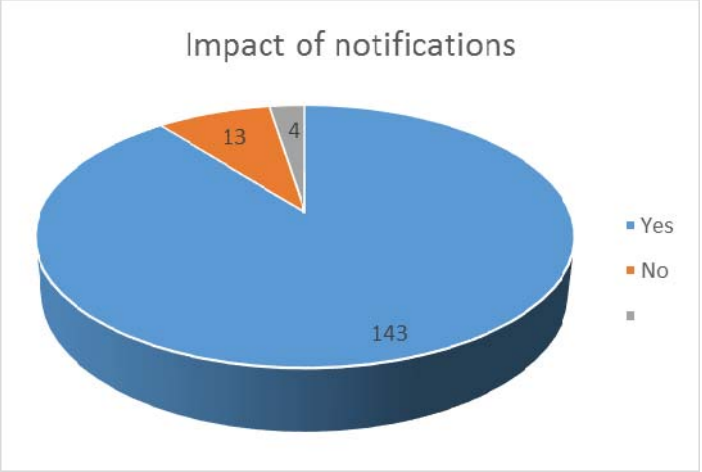
SME	Total
No	103
Yes	56
Not specified	1
Grand Total	**160**



The vast majority of respondents (90%) indicated that they are impacted by the submission of information to the Appointed Bodies.

Table 3-9: Impact of submission process

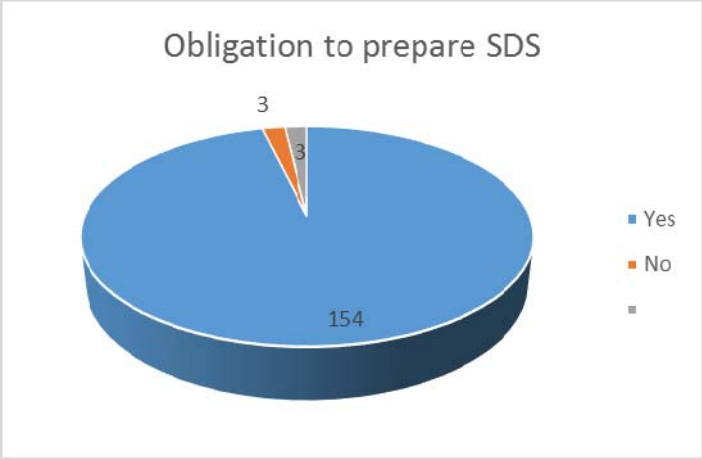
Impacted by submissions	Total
Yes	143
No	13
Not specified	4
Grand Total	**160**



Moreover, almost all companies that responded are required to prepare SDS. This is an important information considering that the majority of Member States require the SDS as (part of) the information to submit.

Table 3-10: Obligation to prepare Safety Data Sheets (SDS)

SDS	Total
Yes	143
No	3
Not specified	3
Grand Total	**160**



3.3.2 IT systems used by companies

Virtually all companies have an IT system of some sort *to prepare their SDS* and the vast majority use commercially available software systems. The table below has been compiled from the answers to question 12.

> Question 12: *Do you use your own homemade IT system (developed specifically for the needs of your company) for generating Safety Data Sheets (SDS) or do you prepare your SDS with generally available software (e.g. MS Excel) or use sophisticated commercially available software system (e.g. SAP)*.

Table 3-11: IT system to prepare SDS

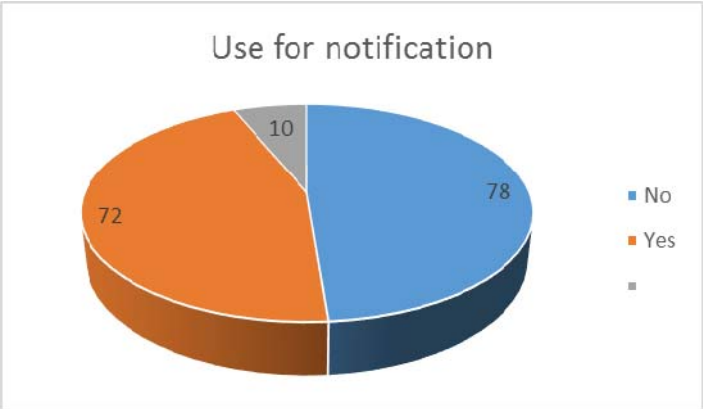
IT system to prepare SDS	Total
Single answer	
Sophisticated commercially available software system (The most cited being SAP EH&S, ChemGes, EXESS)	131
Homemade IT system	9
Generally available software (e.g. MS Excel)	7
No software or IT system	4
Not specified	2
Multiple answers	
Sophisticated commercially available software system Homemade IT system	3
Sophisticated commercially available software system Generally available software	2
Homemade IT system Generally available software	2
Grand Total	**160**

Interestingly enough, half of the companies declared that their IT system does not allow generating data for submission to the Member State Appointed Bodies.

Question 16: *Can the software used by your company to generate SDS also be used to generate data for notifications to MS Appointed Bodies?*

Table 3-12: Can the software be used to generate data for submissions

Use IT to prepare submissions	Total
No	78
Yes	72
Not specified	10
Grand Total	**160**



3.3.3 Most relevant issues and difficulties encountered

Question 26 of the survey asked for the three most relevant issues and difficulties encounter by industry in generating and submitting information to Member State Appointed Bodies.

The answers are compiled as follows.

Table 3-13: Most relevant issues

Most relevant issues and difficulties encountered	Total
Lack of a Unique Formula Identifier (UFI)	19
Lack of a Unique Product Identifier (UPI)	13
Lack of a Unique Company Identifier (UCI)	5
Lack of a Product Categorisation System (PCS)	9
Versioning of information submitted to the MS Appointed Bodies (Poison Centres)	48
Difference between Member States with regard to the level of detail on the composition	112
Differences between the Member States on the type and content of information to be submitted	86
Diversity of IT format(s) of information to be submitted	113
Different national procedure for submission of information	28
Other	19

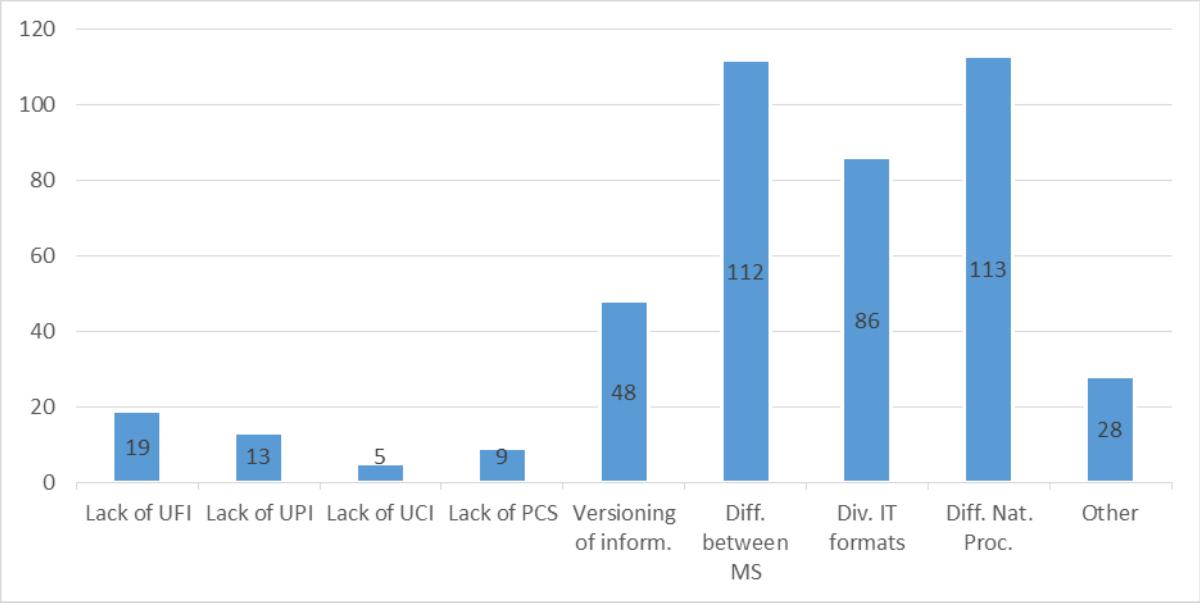


Figure 3-3: Most relevant issues

3.3.4 High-level requirements for input of data in a basic application

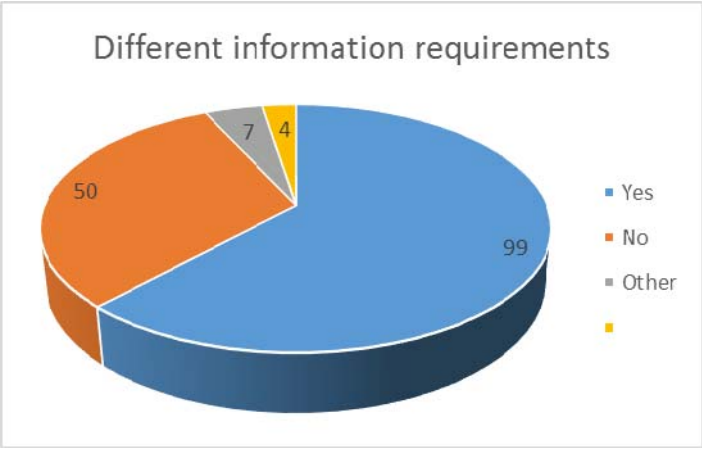
Several questions in the industry questionnaire concerned the general requirements in relation to the input of data in a basic application.

As depicted by the table and chart below, two-third of respondents were interested in seeing different information requirements for consumer mixtures and industrially used or professionally used mixtures. The data is compiled from answers to question 21.

> Question 21: *Would you find it useful if information requirements are different for consumer mixtures, and industrially used or professionally used mixtures?*

Table 3-14: Different information requirements

Different information requirements	Total
Yes	99
No	50
Other	7
Not specified	4
Grand Total	**160**

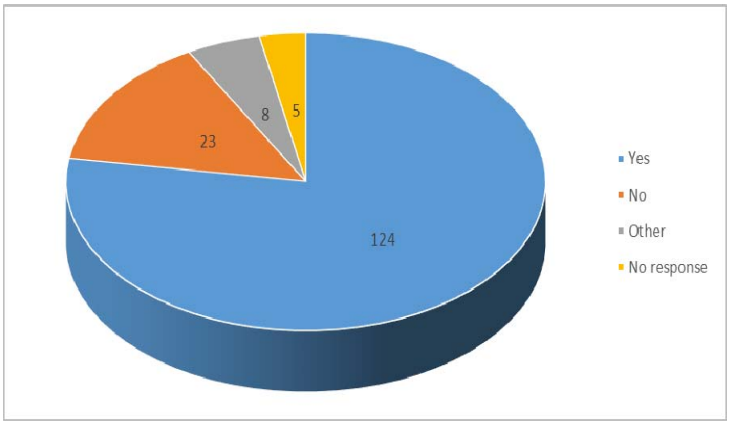


Three-quarter of the respondents saw a need for the preparation of a detailed guidance/practical guide translated into all official EU languages on how to use the basic application.

> Question 29: *Do you see a need for preparation of a detailed guidance/practical guide translated into all official EU languages on use of the basic application?*

Table 3-15: Guidance in the tool

Guidance in the tool	Total
Yes	124
No	23
Other	8
Not specified	5
Grand Total	**160**

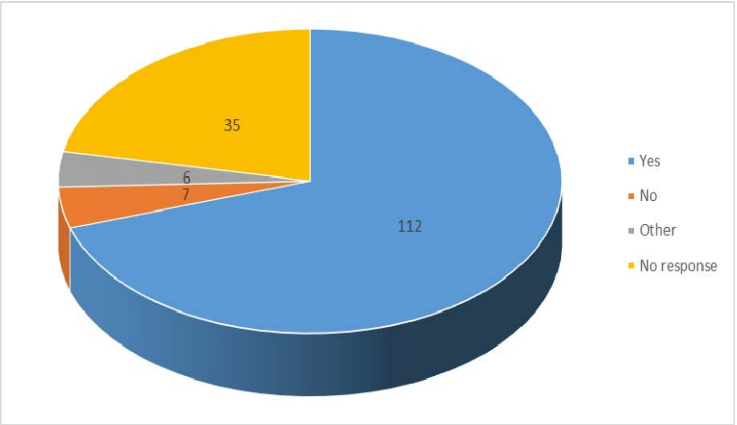


A majority of respondents showed an interest in the possibility of bulk submission. This can be put in parallel with the fact that several Member State provide such mechanism. The chart below is compiled from the answers given to question 30.

> Question 30: *Would you be interested in a bulk notification (e.g. submission of multiple notifications in one go)? If yes, do you have any practical suggestions?*

Table 3-16: Bulk submission

Interest in bulk submission	Total
Yes	112
No	7
Other	6
Not specified	35
Grand Total	**160**



3.3.5 High-level requirements for submission of information to MS

Other questions in the industry questionnaire focused on general requirements in relation to the submission.

As depicted by the table and chart below, 90% of respondents seemed to be interested in having the possibility to notify in one language only: in English in all Member States.

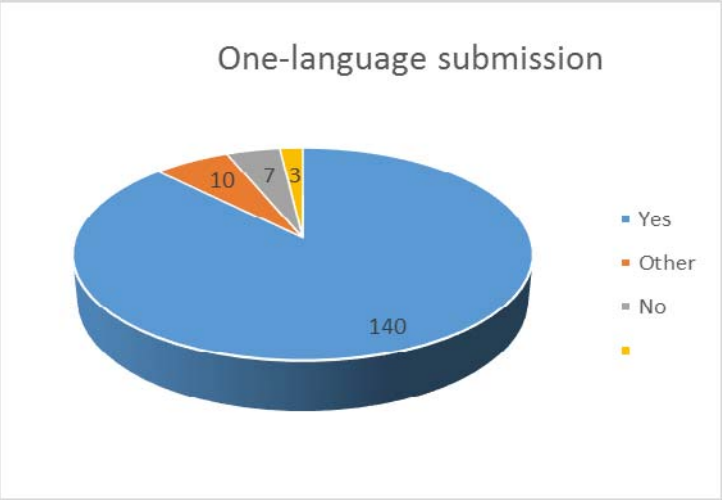
> Question 33: *Would you like all submissions to be done in one language?*

Studying the answers in detail shows this is more nuanced than it seems. The submission in English is obviously preferred but the following interesting notes are given:

- SDS can be given in the Member State's language(s).
- Data should be selected from codes (such as list of risk phrases) allowing for multi-lingual display of a single submission.

Table 3-17: One language submission

One language submission	Total
Yes	140
Other	10
No	7
Not specified	3
Grand Total	**160**



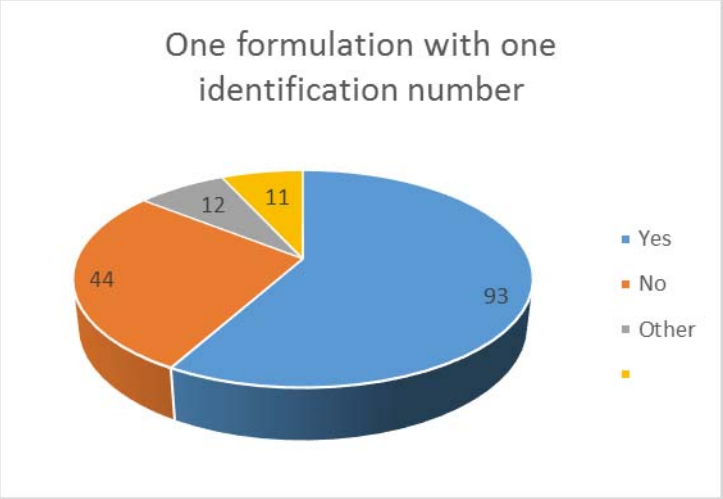
A question was asked about the preference to register one formulation with one identification number only.

> Question 34: *Would you prefer to register one formulation with one identification number only? Please, elaborate.*

The table and chart below show the answers to question 34. Studying the provided elaborations shows that opinions are quite diverse, very probably in direct relation to the industrial sector.

Table 3-18: One formulation with one identification number possible

One formula identifier	Total
Yes	93
No	44
Other	12
Not specified	11
Grand Total	**160**



3.3.6 Central submission system and dissemination

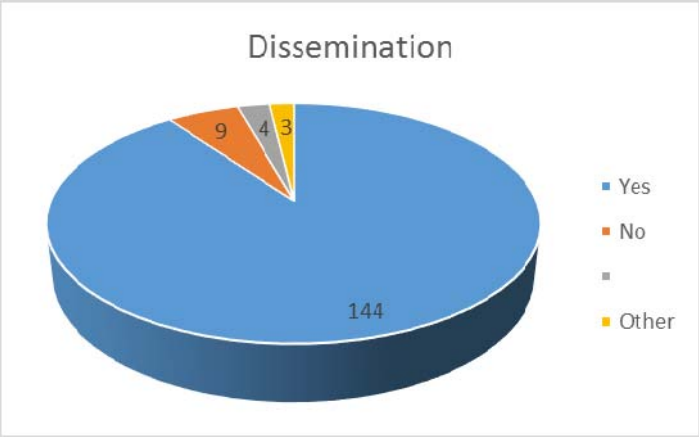
Finally, a question tackled the possible interest for a central submission system that would disseminate information to the competent authorities.

> Question 35: *Would you prefer one registration to be disseminated to all relevant Member States Appointed Bodies?*

As depicted in the chart compiling the answers to this question, industry preference is overwhelmingly (90% of preference) for a central submission system.

Table 3-19: Dissemination

Dissemination of submissions to PC	Total
Yes	144
No	9
Not specified	4
Other	3
Grand Total	**160**



Studying in detail the 'No' and 'Other' answers shows that objections are the following:

- Industry not seeing it feasible to provide information in a single document because of market differences, for instance because the composition ranges may vary between countries.
- Security and confidentiality reasons.
- Question on the legal foundation for a central system since the requirements in the MS are different and regulated on a national level with national IT tools.

Industry preference for a central system can be put in relation with their answers to other questions:

- As shown in section 3.3.3, by far the three most relevant issues and difficulties encountered by industry are: (i) the diversity of IT format(s) of information to be submitted, (ii) the difference between Member States with regard to the level of detail on the composition, and (iii) the differences between the Member States on the type and content of information to be submitted.

  It is obvious that a central submission system will directly address these important concerns.

- Additionally, it has been shown in section 3.3.5 that industry is highly interested in the possibility to submit in one language only.

  This is also a feature that is more easily provided via a central system where requested information can be organised to facilitate encoding in one language for most of the data and cater for the proper encoding of multi-lingual information where need be. This is a direction that is now already proposed by the Basic Application discussed in section 5 below.

4 Harmonised submission format

The data requirements for the submission of information relating to emergency health response referred to in article 45 of the CLP Regulation are presently defined in a Working Paper drafted by the Commission services in charge for CLP Regulation. An amended version of the paper discussed at the 18th CARACAL meeting on 23-24 June 2015 [CA/48/2015] has been used as reference for the definition of the data and their semantics.

The harmonised format in XML has been defined following a two-step approach. First, the relevant business entities, their properties and their relations have been modelled using the UML language[9] as will be shown in the Data model section. Then, this model is transformed into the XML language, which will be detailed in the XML schema section.

This approach has the following benefits:

- The initial focus is put on business entities and their relations, not the targeted XML representation. This avoids influencing the design with constraints coming from a particular technical representation.
- Data model diagrams (UML class diagrams) can be easily understood by all project stakeholders.
- The data model is in itself documentation for the format.
- The data model can also be used to model database schemas or generate application code.

4.1 Data model

The data model defines all business entities and their relations; the main entities being *Submission*, *Mixture* and *Product*.

The complete UML model of the harmonised format is depicted in two class diagrams in the appendix *UML model of the harmonised format*:

- The first class diagram is centred on the *Submission* entity.
- The second diagram is centred on the *Mixture* entity.

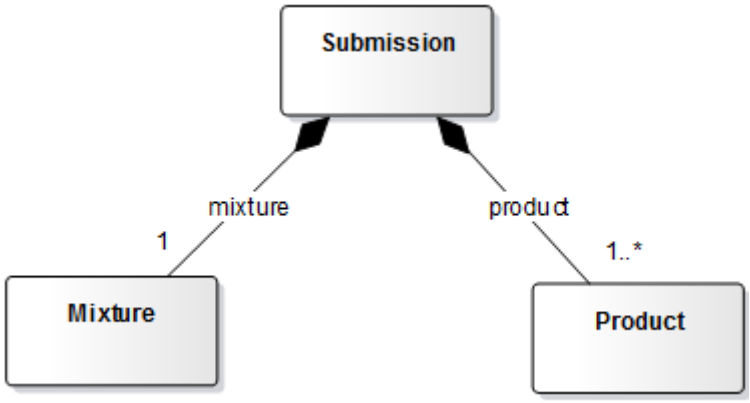
The data model is a formal representation of the data requirements set out in the Working Paper [CA/48/2015]. The following points deserving particular explanations will be detailed below.

- A submission is about one mixture.
- Submissions can be grouped into a "submission bundle".
- A submission is bundled by one submitter for one Member State.
- A mixture is defined by its components and its classification and labelling.
- There exist different kinds of mixture components.
- Extension to voluntary submissions of non-hazardous mixtures.
- Existing models have been used or provided inspiration where possible.

A submission is about one mixture

As depicted below, the *Submission* entity groups together information about the mixture and its products.

[9] UML (Unified Modelling Language) is a general-purpose notational language for specifying software, and notably data model using object-oriented concepts.

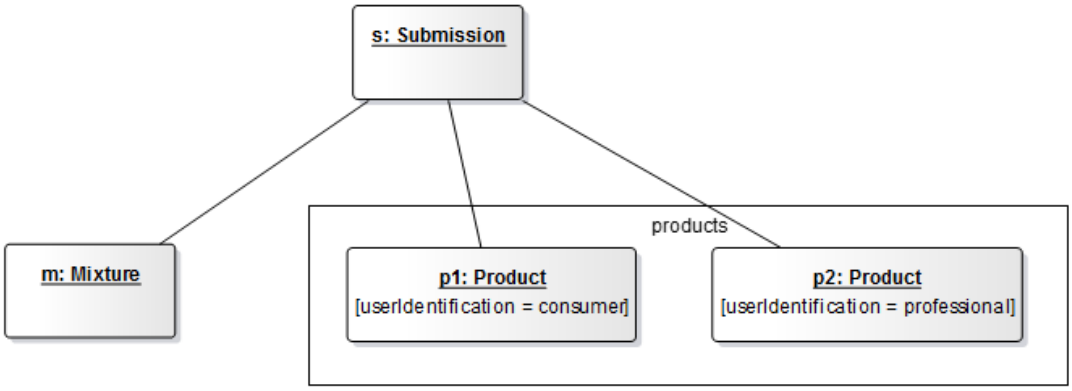


The model thus clearly separates concepts:

- The *Mixture* entity groups together all information relevant to the description of the mixture "chemical properties": its physical and chemical properties (physical state, colour, pH), its composition and its classification. The *Mixture* entity also includes the UFI property: the unique formula identifier of the mixture's formulation (i.e. its composition).
- The *Product* entity gathers information related to how the mixture is placed on the market: the trade name(s), the product identifier(s) and the product packaging. The *Product* entity also includes key properties about its use: the *user identification* (indicating consumer, professional and/or industrial uses) and the *product category*[10].

A *Submission* groups one *Mixture* with one or several *Products* and thus allows for flexible combinations to reflect commercial reality. For instance:

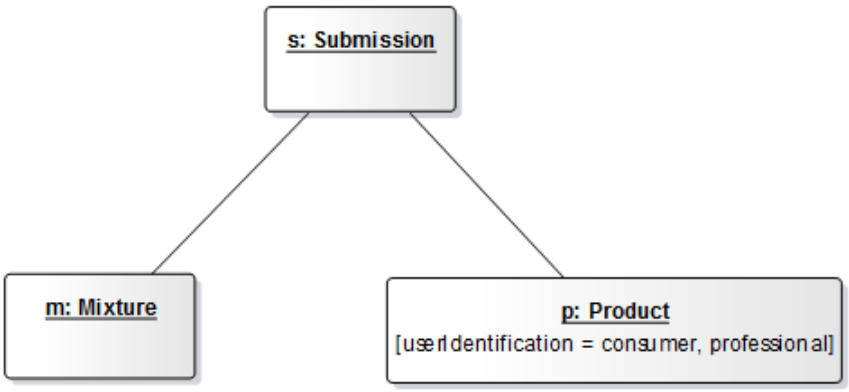
- One mixture may be sold for different uses. This is supported by allowing the declaration of several products, as illustrated below: the first product, *p1*, is sold for *consumer* use and the other, *p2*, for *professional* use.



Distinguishing the products (*p1* and *p2*) in this way is necessary only if the other product's properties, such as trade names or packaging, are different. For instance, if *p1* is sold in 1-liter buckets under the name 'Red paint' and p2 is sold in 5-liter barrels under the name 'Heavy-duty red for pros'.

Should the mixture be sold as exactly the same product for both markets, the submission can be simplified as illustrated below: a product can be given multiple *user identification*s, in this example, consumer and professional.

[10] The product category is expected to be eventually represented using the PCS (Product Category System) that is still under development. The data model introduced the *ProductCategory* enumeration class to model this, but enumeration remains empty until the categories will be defined. This is expected to become available by end of 2016.



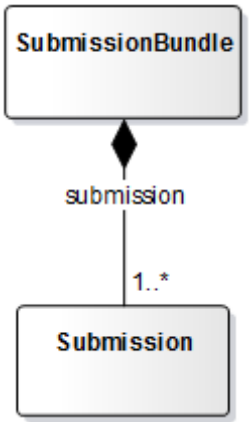
- One mixture may be sold under different names. This is supported by allowing the encoding of several trade names for a product.
- One mixture may be sold in different quantities (i.e. volumes or weights). This is supported by allowing the encoding of one of several packaging details for a product.

The data model thus caters for the flexible definition of all products related to the submitted mixture.

Submissions can be grouped into a "submission bundle"

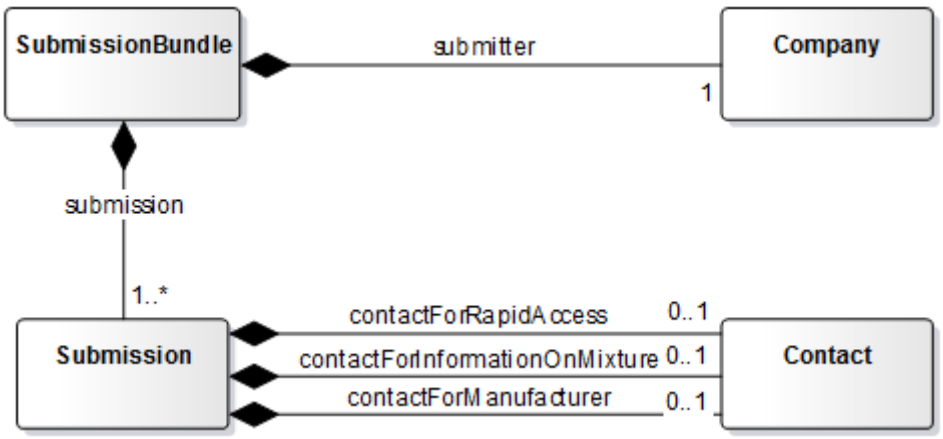
In support of submitters who market several mixtures in the same Member State, the data model includes the concept of "submission bundle" (also named "bulk submission"). A submission bundle is a set of submissions individually respecting the information requirements but originating from a common submitter. It is a mean to easily send multiple submissions at once.

As illustrated below by an snapshot of the data model, the *SubmissionBundle* entity formally defines the concept of a set of *Submissions*.



A submission bundle is thus to be understood as a set of submissions individually respecting the data requirements and originating from a common submitter.

The model acknowledges that while a submission bundle is prepared by one submitter, each submission may require the notification of distinct contact information. This is depicted in the diagram below.



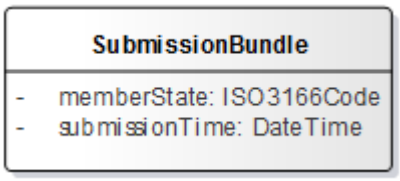
A submission for one mixture will be a *SubmissionBundle* including a single *Submission*.

Finally, it is important to mention that the concept of bundling submissions must not be confused with that of the "group submission" introduced in the Working Paper [CA/48/2015]. The latter concerns variants of a product or products in which a component is described by a generic identifier such as "fragrance" or "colouring agent" that can, under certain specific conditions, be considered as a single mixture and thus be submitted with one submission.

A submission is bundled by one submitter for one Member State

The above diagram already showed that a submission is prepared by one submitter modelled by the *Company* entity. A submission is also aimed at one and only one Member State.

This is modelled by the *memberState* property in the *SubmissionBundle* entity.



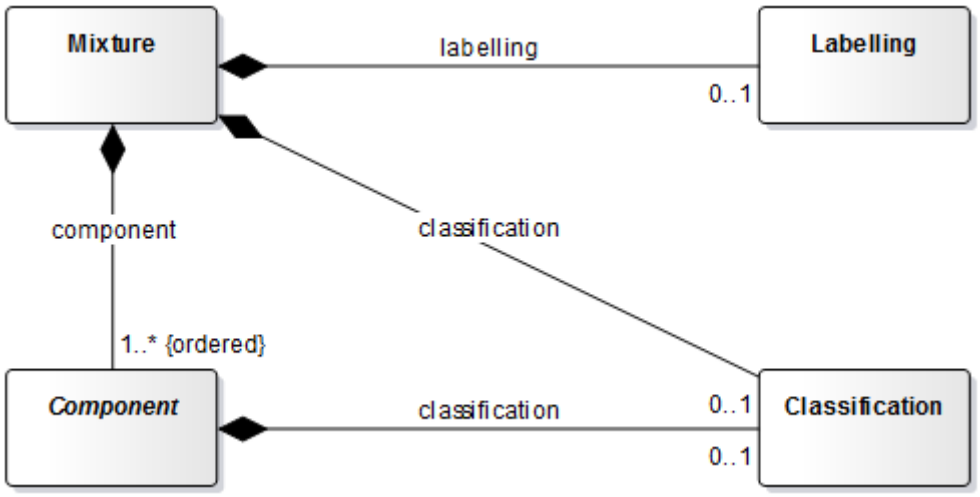
This is in line with the requirements provided in the Commission Working Paper and current practices.

Should the need to expand the format to allow submissions valid for several Member States, the following will need to be changed:

- Allow encoding several Member States instead of one.
- Separate the Member State specific data elements and allow their repetition for each concerned country. This is for example the case of the *Submitter* information and the *Contact* points. It could also be the case of trade names or other product information.

A mixture is defined by its components and its classification and labelling

The diagram below shows the main entities that together model a *Mixture*: the mixture's *Components* and its *Classification* and *Labelling*.



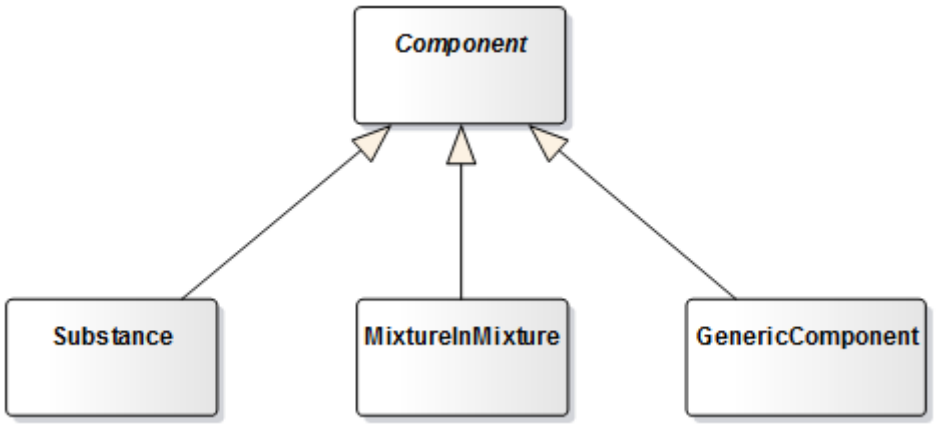
It is worth noting that the mixture's *Classification* and *Labelling* are optional. This is in support of the possibility to encode voluntary submissions for non-hazardous mixture. Any actual format derived from this model will have to make sure that classification and labelling information are duly provided when the mixture is hazardous.

The model also caters for the fact that each mixture component (modelled by the *Component* entity) may be given its own classification.

Different kinds of mixture components

A mixture component is either a substance, a mixture in mixture or a "generic component" (i.e. a substance described with a generic identifier such as "colouring agent").

This fact is modelled using inheritance: a derived entity such as *Substance* inherits the properties of its parent entity *Component*. Thereby, *Substance* gets the *concentration* property that has been defined at the level of the *Component* entity.



Each derived entity then receives its specific properties. For instance, *Substance* has properties that model the notion of index number[11], EC number, CAS number and chemical name, where *GenericComponent* is completely known via its type ("fragrance" or "colouring agent".)

Extension to voluntary submissions of non-hazardous mixtures

The data model supports voluntary submissions of non-hazardous mixtures via a dedicated "hazardous" property in the *Submission* entity and the optional nature of the *labelling* and *classification* relations in the *Mixture* entity. In practice:

[11] The index number in Annex VI to CLP. For instance, formaldehyde has index number 605-001-00-5 in that annex.

- For the submission of hazardous mixtures, the hazardous property will be set to True, and labelling and classification must be provided.
- For non-hazardous mixtures, the hazardous property will be False, and labelling and classification may not be provided.

Inspiration from existing models

When developing the data model for the future harmonised format, consideration has been taken of the prior existence of similar formats/models, including IUCLID and the format developed for the Cosmetic Products Notification Portal (CPNP).

While it is true that re-using (part of) existing models would foster interoperability, it is also clearly apparent that such re-use is in practice not possible. Studying the data models and the underlying requirements in details undoubtedly reveals that sharing models or definitions is not possible as they differ in too many ways.

First, as it clearly appears from the above explanations of the data model, the data requirements are very specific and the proposed data model adheres to these requirements. There is not an existing data model that could fulfil such specific requirements such as catering for the notion of mixture in mixture or providing the required flexibility in the definition of a product.

If entire data models cannot be re-used, maybe simpler concepts can. Unfortunately, this also is not as easy as it could appear before analysis. The following are clear examples where re-use of definitions or basic concepts is not possible:

- A concept of "product categorisation system" (PCS) is always necessary but the categories are always different depending upon the context, preventing direct re-use.

  Consider for instance the four-level categorisation system used in the Cosmetics portal that defines the following first-level values: 'Skin products', 'Hair and scalp products', 'Nail and cuticle products' and 'Oral hygiene products'. These categories, perfectly pertinent in the cosmetics domain, cannot be re-used as such in our context.

- There exists no common definition or standard for the concept of "product packaging".

  IUCLID provides its definition of packaging type[12], with the following values: aerosol can, air spray, bag / sack, blister, bottle, box, can / tin, case, jerry can. Although useful, this list falls short of the packaging routinely used at Poison Centres that we must consider for this application.

  A similar analysis has been performed with the package definition used by the Cosmetics portal. The portal proposes packaging values that are closer in the cosmetics context to the notion of applicator, and cannot be readily re-used here.

- The same study has been performed for the physical state values, with the same result. Physical states defined by other applications in other contexts do not fit the needs expressed by Poison Centres where, for instance, fine-grained distinctions for the solid state is required.

The SPC editor[13] is close to what we try to achieve here. Still, the SPC schemas cannot be readily re-used either because of important requirements specific to Poison Centres: the need to submit information in several languages in multi-lingual countries[14] or when English is accepted in addition to the national language. That

[12] Values defined in section 14.3.9 "Packaging" which is part of the BPR (Biocidal Products Regulation) endpoints.

[13] An application made available by ECHA for preparing files to submit to the Register for Biocidal Products (R4BP).

[14] For instance, Belgium where submissions must be in French and Dutch (and possibly in German).

specific requirement prevents the re-use of the schema defining the hazard and precautionary statements. Other specificities such as the way substances are identified or the structure of the composition also prevented direct re-use of the SPC schemas.

Tying everything together

All the notions discussed in this section are tied together in the two class diagrams visible in appendix UML model of the harmonised format. These diagrams not only show the entities and their relations as above, they also include the definition of all properties.

The model represents one submission (bundle)

One word of caution needs to be written before closing this chapter and moving to the next. The data model discussed above models the format of one submission bundle file. It is not directly suited (optimised) for the storage of the data in a database. For instance, this models obviously requires that the submitter information is provided in every submission file. This is something that one normally wants to avoid when storing the data in a relational database to avoid duplicated records. In such case, one should ideally store the company information once and refer to it via a unique key, for instance the company's VAT number.

Of course, the path between this model and one optimised for database storage is short and not complicated. Points of attention when designing a database must be:

- Submitter information, to avoid duplication of information as mentioned.
- Deciding whether certain entities are collapsed into a single table. For instance, if *Submission* and *Mixture* will be grouped together or kept as separate entities.
- Addressing the modelling of the generic *Component* entity that is derived into the *Substance*, *MixtureInMixture* and *GenericComponent* entities.

4.2 XML schema

One of the main goals of the study is to facilitate the exchange of information between Poison Centres by defining a standard format for the electronic exchange of information, the format of choice being XML.

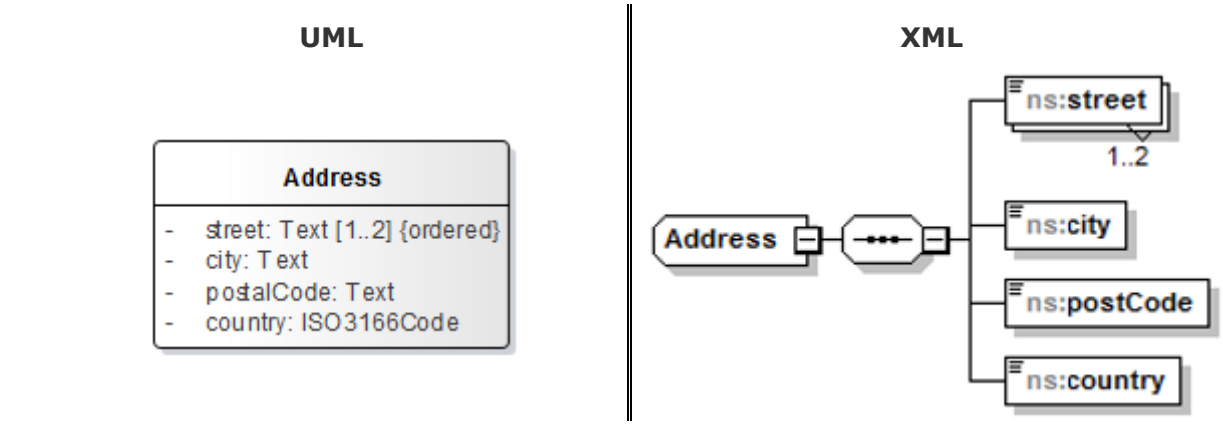
Having agreed on the data structure from a business perspective, i.e. on the model expressed in terms of the key business entities, their properties and their relations, the data model is used as direct input to the preparation of XML schemas.

The following rules have been followed when mapping the model in UML to a schema in XML and will be detailed below.

- A UML entity is mapped to an XML type.
- A composition of entities is mapped to a complex child element.
- A namespace is defined for the XML schema.
- Versioning of the XML schema will be possible.
- The XML schema defines a single root element to instantiate in XML documents.
- The XML schema defines uniqueness constraints.
- The XML schema defines business rules with assertions.

A UML entity is mapped to an XML type

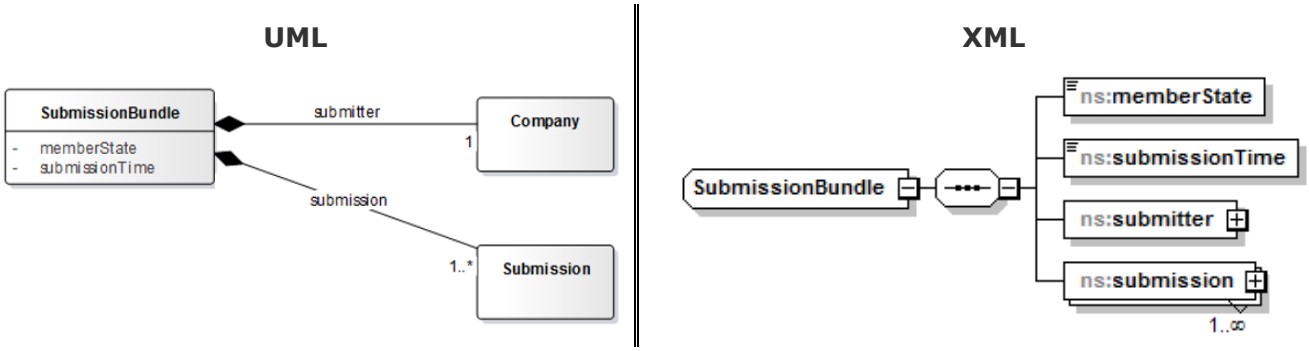
For instance, the *Address* entity is mapped to the *Address* complex type.



The simple properties are mapped to simple child elements. For instance, the *street* properties in the *Address* entity are mapped to the *street* child elements in the *Address* XML element.

A composition is mapped to a complex child element

For instance, a SubmissionBundle includes a submitter and one or several submissions. The *submitter* composition in the UML model corresponds to the *submitter* child element in the XML schema. The same applies to the submssions.



This approach is applied recursivelty to all entities. A diagram showing most of the elements is available in appendix XML schema for the harmonised format.

XML schema namespace

The XML schema has its own namespace: `eu:europa:ec:grow:pc:1`.

This way should types defined in this schema be used in some other schema, they will be identified without ambiguity by their namespace.

An XML namespace is typically constructed from the URL of the domain name of the organisation endorsing the schema, completed by sub-levels if necessary, and a schema short name:

- The Europa URL http://ec.europa.eu/ gives the namespace prefix: `eu:europa:ec.`
- The relevant DG acronym is appended: `grow`.
- The schema name is appended: `pc`, for Poison Centre.
- Finally, the schema version complete the namespace: `1`.

Schema versioning

Schema versioning will be linked with the schema namespace: a version number is part of the namespace:

`eu:europa:ec:grow:pc:1`

Versioning the namespace allows supporting future non-backward compatible changes to the schema definition: when a major, non-backward compatible change is made to a schema file one must change the version ID in the namespace. A non-backward compatible change is one that is not structurally compatible with the previous version: adding elements or types, changing elements or types in non-compatible ways: e.g. adding child elements, going from optional to mandatory, changing the order of elements. By changing the namespace, one is sure to invalidate all existing documents that make use of a previous version as needed.

When a minor, backward compatible change is made to a schema file the schema namespace must not change as a document valid under the new version remains valid with the new version. Typical examples of backward-compatible changes are adding optional elements or attributes, adding enumeration values to a type, making a pattern less strict, going from mandatory to optional.

Still, one ideally wants to indicate some "minor" version numbering for backward compatible changes. This is done by adding the *schemaVersion* attribute to the root element. The *schemaVersion* attribute values are determined by an enumeration such as

```
<xs:simpleType name="SchemaVersion">
  <xs:restriction base="xs:token">
    <xs:enumeration value="1.0"/>
  </xs:restriction>
</xs:simpleType>
```

When a new, backward compatible version is created, a value is added to the enumeration, for instance 1.1. Software manipulating instance documents are then able to distinguish between minor versions by reading the *schemaVersion* attribute in the document root element.

A single root element

The XML schema defines a single element from which XML instance documents can be created and validated: *submissionBundle* of type *SubmissionBundle*.

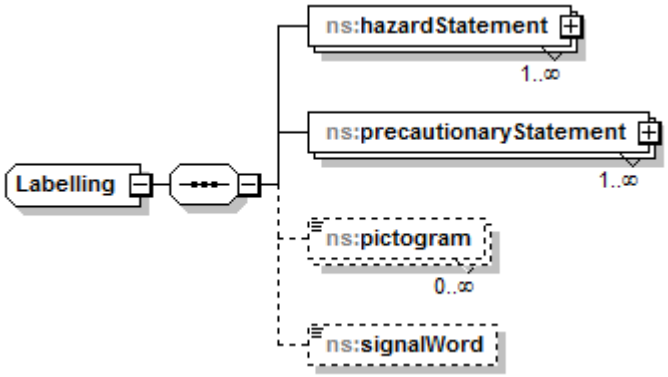
An XML instance will thus start as:

```
<?xml version="1.0" encoding="UTF-8"?>
<submissionBundle xmlns="eu:europa:ec:grow:pc">
```

Uniqueness constraints

Where appropriate, the XML schema defines uniqueness constraints on repeatable elements.

For instance, the Labelling element notably includes a set of hazard statements and precautionary statements.



It is better to enforce their uniqueness to avoid unnecessary repetitions as happens in the XML snippet below.

```
<labelling>
     <hazardStatement code="H205"/>
     <hazardStatement code="H272"/>
     <hazardStatement code="H205"/>
     <hazardStatement code="H272"/> <!--repeated-->
</labelling>
```

The following unique constraints are enforced by the schema definition:

- UNIQUE_USER_IDENTIFICATION: A user identification cannot be repeated in a product.
- UNIQUE_LABELLING_HAZARD_STATEMENT: A labelling hazard statement code cannot be repeated in the mixture labelling.
- UNIQUE_PRECAUTIONARY_STATEMENT: A precautionary statement code cannot be repeated in the mixture labelling.
- UNIQUE_PICTOGRAM: A pictogram code cannot be repeated in the mixture labelling.
- UNIQUE_HAZARD_CATEGORY: A hazard category code cannot be repeated in the mixture classification.
- UNIQUE_HAZARD_CATEGORY_IN_COMPONENT: A hazard category code cannot be repeated in a component classification.

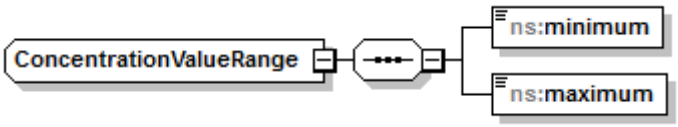
Note that one must repeat the uniqueness rule on hazard categories because the constraint must be defined in the element where the repetition occurs, *Mixture* and *Component* respectively, and cannot be defined within the *Classification* element.

Assertions

The XML schema has been created using the XSD 1.1 standard[15]. The key justification for using this relatively recent[16] standard is its introduction of assertions.

Assertions provide a powerful validation feature to XML. Indeed, while XSD 1.0 provides *basic, type-related validation on single elements*, XSD 1.1 adds assertions, *rules-based validation of business rules involving more than one element*.

Consider for a first example the concentration range element.



The range has a *minimum* value and *maximum* value, and an implicit rule that the minimum value may not be greater than the maximum.

Validating such simple business rule is not possible with XSD 1.0 validators, leaving the following sample as valid XML:

```
<concentrationRange>
     <minimum>12</minimum>
     <maximum>10</maximum>
</concentrationRange>
```

With XSD 1.1, one may add an assertion to the definition of the type, stating that

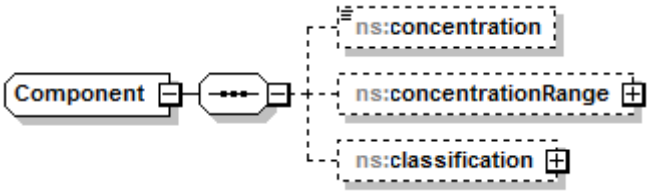
[15] See the W3C web site for complete information about this standard: http://www.w3.org/XML/Schema and http://www.w3.org/TR/xmlschema11-1/.

[16] XSD 1.1 exists since 2012 only.

```
minimum <= maximum
```

An XSD 1.1 validator will immediately reject the above XML code as invalid because it fails to pass the assertion test.

Assertions can also be used to ensure structural correctness. For instance, a component concentration may be given by its exact value or a range of value. This is modelled as follows:



- The concentration and concentrationRange elements are optional.
- An assertion ensures that one or the other is present, never none or both[17].

This approach is more solid than relying on "variant records" or using XML options, both techniques having drawbacks in modelling clarity and code cleanness (once the XML structures are translated into a programming language such as Java.)

These examples show that assertions can be used to validate values or structure. The following assertions are available in the XML schema:

- ASSERT_SUBMISSION_REASON: Asserts that the submission reason is either new or update.
- ASSERT_CONCENTRATION_EXACT_OR_RANGE: Asserts that a component concentration is given either by its exact concentration value or a value range (not both.)
- ASSERT_MIN_LOWER_THAN_MAX_IN_RANGE: Asserts that the lower value is smaller than the upper value in a concentration range.
- ASSERT_SUM_MIN_BELOW_100: Asserts for the mixture components that the sum of exact concentrations and lower values in ranges is below or equals 100.
- ASSERT_CONTACT_RAPID_ACCESS: Asserts that the contact information for rapid access is provided in case of limited submission.
- ASSERT_INDUSTRIAL_USE: Asserts that in case of limited submission the user identification in each product of the submission is 'industrial'.
- ASSERT_PH_WHEN_RELEVANT: Asserts that pH is given when relevant, i.e. when property *pHIsNotRelevant* is false.
- ASSERT_PH_EXACT_OR_RANGE: Asserts that a pH is given either by its exact value or a value range (not both.)
- ASSERT_MIN_LOWER_THAN_MAX_IN_PH_RANGE: Asserts that the lower value is smaller than the upper value in a pH value range.
- ASSERT_CONCENTRATION_GENERIC_NOT_EXCEED_10: Asserts that the concentration of a generic component does not exceed 10%.

Finally, it is important to acknowledge that XSD 1.1 is not necessarily already supported by the organisations who will implement software using the schema. This is why an XSD 1.0 version of the schema file is also distributed[18]. Users of the XSD 1.0 version will then need to implement the above controls by other means.

[17] The assertion simply is: count(concentration) + count(concentrationRange) = 1.

[18] The XSD 1.0 version is identical to the XSD 1.1 except for the <assert> element that are commented out.

Tying everything together

The complete schema documentation is available as a separate document [XML_SCHEMA].

5 Basic application

The second main task of the study is to develop a simple application for the purpose of creating or viewing one submission in the XML format.

The use cases of the basic application are:

- Create a submission and save it as an XML document.
- View a submission that exists as an XML document.
- Update a submission and save it as an XML document.
- Validate a submission: if the XML document is not valid, the basic application will indicate which fields are incorrect.
- Print the submission information.

The basic application has some important features or constraints: it is not connected to a mixture database and is not intended for the creation of a submission bundle.

1. The software is a one-submission encoding tool that runs as a "stand-alone" application and is not establishing connections to external programs such as substances or mixtures databases, or back-end systems to generate submissions.

   Indeed, establishing such connections was not included in this study due to the great variety of back-end systems and/or substance/mixture management systems deployed by industry and Poison Centres. It is important to note though that generating submissions from back-end systems is a desirable goal for which a prerequisite is the definition of the harmonised format and XML schema achieved by the present study. Generating submissions will require the development of dedicated IT interfaces and application software.

2. As explained above, the harmonised XML format for submission to Poison Centres supports the encoding of several submissions within a single XML document using the concept of "submission bundle". The basic application will allow creating, updating and viewing one submission at a time.

   When opening an XML document to view a submission, if the document includes several submissions the application will allow the user to select which one he wants to consult.

The basic application is also not a database of mixtures and it cannot store multiple submission or provide search capability over submissions.

The basic application is thus a support mainly helpful in several contexts:

- For **submitters to encode their submissions** to the Poison Centres according to the defined format.

  It is clear though that the basic application is not intended to be used for the preparation of submissions of dozens or hundreds of mixtures in several Member States. Companies faced with that challenge will have to develop (or buy) software that will **generate** the submissions from their mixture database using as a reference the proposed solution and the XML schema.

  The scope of use of the basic application is likely to be small or medium enterprises (SME) that have few submissions to prepare and where the submissions are not often updated. Such small enterprises cannot afford the development of aforementioned software system, but can certainly set up the limited management of documents necessary to **encode** the submissions and keep them as XML files.

- For Poison Centres to easily **view and control the received submissions**.

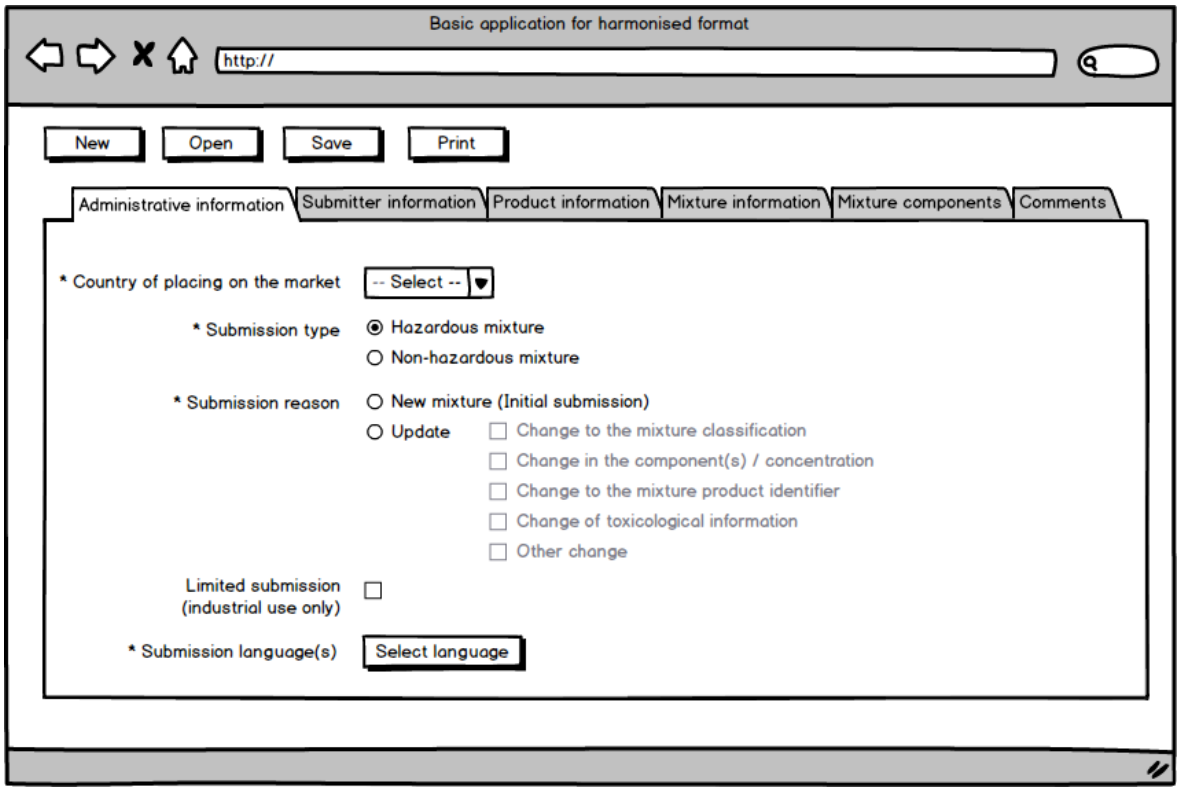
Here again, usage of such application is limited by the number of submissions to process. The basic application can certainly help viewing a submission file received by email or via some other file transfer mechanism. It still could be used if the received submission files are stored in a file systems using an indexation mechanism (e.g. per submitter), but such approach will quickly show its limits.

Poison Centres will eventually have to develop the database into which submissions in the harmonised format can be stored and the appropriate screens to search and view the submissions[19].

5.1 Application specifications

The specifications of the basic application are available in a separate document [BASIC_APP_SPEC].

Below we only reproduce the application main screen.



5.2 Application deployment topologies

The basic application may be deployed in two ways:

- The first and obvious scenario is to deploy the application as an online service[20] on an intranet or even on the internet. This kind of deployment is most suitable for larger companies or institutions, because it provides a single installation and maintenance point, while serving the needs of multiple users. Once loaded in the user's browser, the application executes locally; the server requirements are consequently very small and can be accommodated by existing infrastructure.

[19] Screens that can certainly be inspired by the basic application.

[20] This is often called a SaaS approach: Software as a Service.

- Or, the application can be packaged as a desktop application and distributed to users. This approach is generally suited to smaller user base where distribution and maintenance issues can be managed.

On-line service

The application is hosted on a web server accessible from any PC connected to the internet via a well-known URL; for instance https://hosting/organisation/pc-editor.

The server-side requirements for providing the application are rather small:

- A web server such as Apache[21] is enough to host the application. There is no need for a full-fledged application server running back-end services, nor for a database server to store data.

  The application being light, it is possible to host it on existing infrastructure besides other similar applications.

The client-side requirements for running the application are minimal:

- Internet connection.
- Recent web browser with JavaScript enabled.

  The JavaScript condition is an essential requirement: such modern, rich web application will not run in browser where JavaScript is not enabled or an older browser with flawed implementation of JavaScript.

  The application will run in Firefox and Chrome, and in recent versions of Internet Explorer (above and including IE10.)

On start-up the browser will load the necessary resources: the page, the stylesheets, the JavaScript code and the images (e.g. the pictograms). All processing takes place in the browser and there is no server-side validation.

Saving a submission as an XML document also takes place locally, without involving the web server in any way. There is no copy of the submission sent to a central place over the internet and all saves are local.

There is thus no confidentiality or security issue related to using the tool: information is encoded locally and saved on the filesystem of the user's PC; it is never exchanged over a network and cannot be eavesdropped. Obviously, securing the storage of the saved XML documents and their exchange with other parties remains the responsibility of the user. The latter topic will be the subject of the next chapter Secure exchange of data.

On the other hand, users may be familiar with other web applications that store data on a central, back-end server and so forget to save their submission in a local file. This is why we advise displaying a start-up disclaimer message similar to this:

> "Although this tool is web based, your data is never transferred by this tool over the network for security and confidentiality reasons and is not automatically saved. The data you enter and decide to save is only stored in your own file system either on your local disk or on your network drives.
>
> Therefore, please use the Save button to store the editor content on your local hard drive before you leave this application or close your browser window."

Desktop deployment

For smaller setups, or easier installation, the application can also be packaged as a desktop application. The resulting bundle consists of:

- An installer.
- An embedded recent Chrome browser.

[21] http://httpd.apache.org/ABOUT_APACHE.html.

- An embedded minimal Node.js server.
- A shell executable to launch the browser, start the server and launch the application.

Packaging the application as a desktop application brings some additional benefits:

- It ensures a single, controlled, browser version as the runtime environment.
- It enables full offline operation.
- By associating a specific extension to the document format, e.g. ".xpc" instead of simply ".xml", the application can be registered to automatically open the files of the given type.

On the other hand, this approach requires that every version of the application is distributed. This can for instance be achieved by providing the application package for download on the internet. It is also possible to distribute the software via CD for users who do not have internet connection (even if this is probably very uncommon nowadays, especially considering that such connection will be eventually required to submit the file.)

Making sure the first version is distributed is generally never an issue. Problems may arise though when subsequent versions need to be distributed to the user community: users may not be obliged, or may simply forget, to install the most recent version, which can provoke interoperability problems, especially when file format changes are involved. This is why the XML schema includes a versioning mechanism: a version of the application will always create XML documents for a specific version of the schema and software processing submissions must always verify the version of incoming submissions.

Comparing the deployment solutions

In the following table we briefly compare both deployment approaches

Table 5-1: Comparing deployment topologies

Criteria	On-line	Desktop
Server requirement	Limited (e.g. Apache/Tomcat)	None
Client requirement	Small: internet connection, browser	Access right to install an application
Distribution	Not needed	Internet download
Maintenance	Centrally managed	Re-distribution necessary
	Easy, transparent and immediate bug fix or improvement	Delay to bug fix or improvement. Not transparent.
Security	No difference with desktop approach as data is not exchanged over the internet	No security concern involved in used the tool.

The basic application will be available in both topologies.

It is our advice though to favour the on-line approach for the following reasons:

- The facility in distribution and maintenance largely outweigh the hosting costs (which are limited).
- The on-line approach is as secure as the desktop tool since it does not require exchange of any data with a server over the internet.
- Version management is better controlled.

The desktop solution remains a very valid approach for users who cannot run modern, recent versions of browsers for organisational reasons.

5.3 Other tools

In this section we assess the possibility that other useful tools, not covered in detail in this study, could be created and made available to the benefit of the user community[22].

XML format validator

The basic application may serve at validating an XML document in a visual way, but we believe that an XML validator tool could be useful as well for the following reason.

- It will validate all submissions in a submission bundle at once.
- It will provide a clear list of errors instead of a visual hint that a data field is wrongly formatted.
- It can be easier or faster to use.
- If well designed it can be integrated in other back-end systems that process submissions.

Such format validator could be made available over the internet or as a simple desktop tool.

Document generation library

The existence of the harmonised XML format and the eventual obligation to submit data to Poison Centres in that format will require that industry develops (or purchases) software capable of **generating** submission files from their back-end systems.

Where the back-end applications are various in nature and their internal data models specific, the submission format is by nature the same for everyone. It is thus possible to envisage the creation of a **file-generation library** that will provide services for the generation of valid submission documents:

- The library will have a clear interface and provide business-oriented methods like `Submission.addProduct` or `Component.setConcentration`.
- The library interface can specify all business rules via appropriate Exceptions.
- The library interface can be implemented for all mainstream platforms, for instance Java and .NET, and thus be easily integrated by industry and Poison Centres in their systems for the purpose of generating files.
- If widely adopted such library brings further benefits:
    - It reduces the occurrence of bugs since there is, ideally, a single implementation of the file generation module.
    - It facilitates maintenance as any change to the format is accompanied by a new version of the library.

Obviously, if such idea should be pursued, the question of who will bear the cost of the library specifications and development for the target platforms would have to be considered.

[22] The specification and development of the tools mentioned here are outside the boundary of this study. They are mentioned only for the sake of interest.

6 Secure exchange of data

In this chapter we address the third task of the study, the analysis of options for secure electronic data exchange to support collaboration between local Poison Centres, taking into account the confidentiality of the information exchanged.

First, we will define the term "secure exchange" and see what it concretely implies in section *Security concepts*. We will also introduce useful notions in section *Data exchange patterns and topologies* that will be used to compare options.

Then, we will discuss several concrete data exchange mechanisms that Poison Centres could use to securely exchange data. This is done in section *Secure data exchange between Poison Centres*.

Finally, we believe that although the matter of securing exchange of data between Poison Centres is important, one can hardly leave industry out of this reasoning as they are partners concerned in the first place by the confidentiality of their submissions. Mechanisms involving all stakeholders are thus discussed in a final section in this chapter of the study.

Before starting this analysis we must note that our focus is solely the secure **exchange** of data between Poison Centres or Appointed Bodies and that we are not addressing here the topics of **storing** and **accessing** that data in a secure way, an obligation that is the responsibility of Appointed Bodies as per Article 45 (2) of the CLP Regulation: "The appointed bodies shall provide all requisite guarantees for maintaining the confidentiality of the information received".

6.1 Security concepts

First, we need to define unambiguously what is meant by "secure electronic data exchange."

Broadly considered, the notion of "security" in the realm of ICT (Information and Communication Technology) can be broken down in the few concepts briefly introduced below.

Table 6-1: Security keywords

Authentication	Making sure that only authenticated users gain access to resources (application, data). This is routinely achieved by the usual user-password mechanism and other authenticating techniques such as finger print recognition.
Integrity	Making sure one can detect that data has been altered (by transfer errors or maliciously) while being transferred; in other words, ensuring that the received data is the one being sent by detection of alterations. This is typically done using checksums and hash phrases.
Confidentiality	Making sure that the data can only be seen by the users it is meant for. In a connected world this entails two different things: first, ensuring that the data cannot be read by an un-authorised eavesdropping third party while being transferred over a communication network; second; ensuring that data cannot be read by un-authorised users once it has been stored in a file system of a database. Confidentiality is achieved by data encryption.
Non-repudiation	Making sure that the sending party cannot deny having sent a message. Non-repudiation is provided by using electronic signatures.

In the context of the present study we are principally concerned by the **confidentiality of the data** and our focus will be on that important matter. When useful we will come back to the other notions in the arguments below.

Confidentiality can be ensured in several ways:

- In person delivery. Personally handing over a confidential file to his intended recipient is obviously secure but is hardly a practical mechanism, especially in our context. One must inevitably rely on some communication channel to transfer the file. Such channels can be made secure or are to be considered unsecure.
- Using secure communication channels. When using a communication channel that is considered (and ideally is proven) secure, one does not need to encrypt the file since confidentiality of the file transfer is guaranteed by the channel itself. Examples of secure communication channels are:
    - VPN (Virtual Private Networks).
    - File upload over HTTPS (HTTP Secure)[23].

  As a matter of precaution files are often encrypted even when sent over secure channels.
- Encryption of the data when using unsecure communication channels. When relying on an unsecure communication channel, and the internet certainly falls in that category, one must encrypt the file to guarantee its confidentiality.

In our context we must thus mainly address the question of **sending encrypted files over an unsecure communication channel**.

Encryption comes in two flavours: symmetric and asymmetric.

Symmetric encryption

With this kind of encryption, the encryption key and decryption key are the same. A common example is the encryption feature provided by the Zip tool: one can easily encrypt the files in the Zip archive by giving the tool an encryption key. A user willing to consult the files inside the Zip archive has to give the tool the encryption key for decryption.

Symmetric encryption resolves the data confidentiality issue but one immediately sees its limitation: data confidentiality is guaranteed as long as confidentiality of the encryption key is. The confidentiality problem has thus been moved from the data to the encryption key.

Solutions for the secure exchange of the encryption key need thus to be devised to ensure the confidentiality of the data. Typical solutions include, some being unsecure:

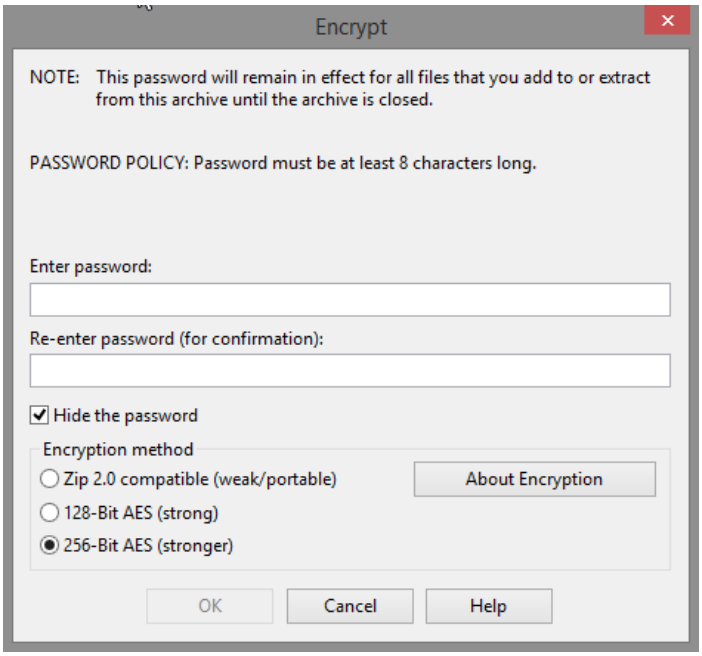
- Sending the encryption key in the same message as the encrypted data. This is what we do when we send an encrypted Zip archive and the key in the same email. This is of course not secure and amounts at having not encrypted the data at all.
- Sending the encryption key in a separate message, still using the same communication channel. This is what we do when we send an encrypted Zip archive and the key in separate emails. This is somewhat more secure, but it will not prevent a dedicated attacker to correlate both emails and reconstruct the data.
- Sending the encryption key in a separate message, using a different communication channel. This is what we do when we send an encrypted Zip archive by email and communicate the key via a phone call or an SMS. This

[23] It is a matter of discussion whether a file upload over HTTPS can completely be considered confidential. HTTPS ensures encryption of the file between the sender's browser and the receiver's web server. There is a segment of the transfer, between the web server and the storage, where the file is no longer encrypted.

approach is the most secure one can achieve with symmetric encryption while remaining simple to use and not being too constraining for the users involved in the data exchange.

If symmetric encryption is used, the most appropriate solution is to **send encrypted message and encryption key over separate communication channels**. The data channel obviously is a communication network such as the internet over which (large) files are easily transferred and the key channel ideally is the telephone network.

To conclude this discussion on symmetric encryption, it is important to remember that its strength directly depends on a) the strength of the encryption key and b) that of the encryption algorithm. It is obvious that easy-to-guess encryption keys are subject to brute force attacks and must be avoided: users must be trained in choosing long enough and not easy to guess keys. As illustrated by the screen below, encryption tools such as the aforementioned Zip archiving tool may still provide weak encryption methods that are very easily broken. One should **always select the strongest method available**[24].



Some common strong encryption tools are listed in the table below.

Table 6-2: Encryption tools

Tool	Platform	URL
7-Zip	Windows/OS X/Linux	http://www.7-zip.org/
VeraCrypt	Windows/OS X/Linux	https://veracrypt.codeplex.com/
AxCrypt	Windows	http://www.axantum.com/AxCrypt/

Asymmetric encryption

This kind of encryption has notably been developed to address limitations of symmetric encryption related to the need to securely exchange encryption keys. With asymmetric encryption the key is split in two: one part, called the **public key**, can be freely and publicly distributed; the other part, called the **private key**, must remain

[24] This is even truer if the data encrypted must remain secure in that form for a long period of time: the stronger the encryption method, the longest the guarantee. (This said knowing that encryption methods have always been broken in the past; think of DES and triple-DES. It is just a matter of time before they are.)

private to the key owner. Keeping the private key private is the core of the guarantees provided by asymmetric encryption[25].

With respect to confidentiality, the guarantee is that a file encrypted with a public key can only be decrypted with the private key. So, contrary to symmetric encryption, having the encrypted file and the key (in this case, the recipient's public key) is of no use to decrypting the file: only the recipient can decrypt the file with his private key. Another strength provided by asymmetric encryption is the possibility to verify the sender's identity and non-repudiation: if a document is encrypted with the private key (which only his owner possesses), anyone can ascertain this with the public key. This mechanism thus provides genuine digital signature.

Asymmetric encryption thus fully addresses the issue of key distribution. It is not yet widely used though because of other factors relating to the complexity of setting up a public key infrastructure, the trustworthy generation of the public-private key pair and its relative poor performance (compared with symmetric encryption).

A trustworthy public key infrastructure indeed requires that the public key is actually generated by (or for) the person who claims owning that key. It would of course be disastrous if one would encrypt data with a public key generated by someone impersonating the legitimate recipient. For that very reason, key pairs are part of a chain of trust and are signed by trusted Certification Authorities (CA). One speaks in that context of **digital certificates**: a file containing a public key and signed by a commonly authority.

Today, only large institutions have the capacity to securely manage the keys and relying of such infrastructure is something that goes beyond the capacity of small actors or individuals. Poison Centres being part of, or being strongly related to, larger Member State administrations are expected to have that capacity.

It is critical to note that in our context, where data encryption is our goal, it is enough that the recipient generates a public-private key pair. The senders do not have to have their own key pair. The only burden on the recipient is to have a system capable of encrypting the data with the recipient's public key.

To conclude this brief discussion of asymmetric encryption, a few important facts still have to be pointed out.

- It must be remembered that its strength directly depends on the fact that the private key retains the characteristic of being private. Since a private key is actually a file, keeping it private heavily depends on a) it being not easily accessible and b) the strength of the code or password protecting file access.
- In addition, key pairs are generated using large prime numbers. The larger they are the strongest the keys[26]. It is thus advised to use long keys as well.
- Finally, public-key infrastructure come with management challenges that have to be resolved. Digital certificates have a validity and must be renewed. Yet, they must be kept by their owner to continue decrypting files or messages encrypted with an old public key if the data has not been saved in unencrypted form[27].

Summary

The following conclusions are summing up this section on the security concepts:

[25] The infrastructure necessary for the use of asymmetrical encryption is often called Public Key Infrastructure (PKI).

[26] The mathematical root of public-key cryptography is the fact very large numbers cannot be factored in a reasonable time and that the key pairs are generated by multiplying two large prime number.

[27] This similar to symmetric encryption: the encryption key must be kept in a safe place unless the encrypted document is saved in unencrypted form. This is often the case that encryption serves only at securing the transfer of documents, not their storage. In the latter case, keys have to be securely kept as long as the encrypted data.

1. The data to exchange has to be encrypted when relying on unsecure networks and possibly also, as a matter of precaution or to secure storage, over secure networks.
2. Data encryption imposes the secure exchange of keys for symmetric encryption or the use of digital certificates for asymmetric encryption.
3. Symmetric data encryption is as strong as the encryption key and the encryption algorithm. One must thus use strong keys and rely on the strongest encryption method available today.

   Asymmetric encryption is as strong as the actual secrecy of the public and the length of the numbers used to generate the key pair.
4. Asymmetric encryption and public key infrastructure provide solid foundation for secure data exchange but requires the intervention of a Certification Authority third party for the trustworthy generation of the necessary digital certificates. Digital certificates also need to be correctly managed, especially with respect to expiration, something that must be carefully considered when putting a public key infrastructure in place. In our context, where we only need encrypting data, only the receiving side needs having a digital certificate, something we expect to be in the power of all Poison Centres.

Before discussing practical implementation, we will first briefly turn to the definition of data exchange patterns and topologies.

6.2 Data exchange patterns and topologies

In this section we introduce terminology related to the pattern and topology of data exchange systems.

6.2.1 Data exchange patterns

Patterns provide guidance for application integration by documenting best practices: they are accepted solutions to recurring problems within a given context.

The next paragraphs briefly describe a few of these patterns of interest in our context.

Addressing

The decision on addressing will primarily depend on how much control do we want to exert in the submission systems over who is allowed to participate in the message exchange:

- Fixed: The list of applications (or recipients) is hard-coded. Each message goes to the same set of submission systems (or recipients).
- Distribution: A broker, i.e. an intermediate application, maintains criteria on which systems are a good match for a specific request.
- Publish-subscribe: The broker broadcasts the request using a publish-subscribe channel (see below). Any national submission system that is interested is allowed to subscribe to the channel.

Publish-subscribe

A "publish–subscribe" is a messaging pattern where senders of messages ("publishers") do not send the messages directly to receivers ("subscribers"). Instead, published messages are characterized into classes, without knowledge of what, if any, subscribers there may be. Similarly, subscribers express interest in one or more classes, and only receive messages that are of interest, without knowledge of what, if any, publishers there are.

Under this model, subscribers typically receive only a subset of the total messages published. The process of selecting messages for reception and processing is called filtering.

The main advantages of a "publish-subscribe" pattern is that publishers are loosely coupled to subscribers, and need not even know of their existence. With the topic being the focus, publishers and subscribers are allowed to remain ignorant of system topology. Each can continue to operate normally regardless of the other. Furthermore, the pattern provides the opportunity for better scalability.

Meta-data only

Under this pattern only the key metadata that are considered critical to support key "search" use cases for Poison Centres are initially exchanged. These meta-data will have to be identified based on typical incidents and how their agents are looking for submissions before responding to the public.

In principle the key search terms could be included, such as the trade name, the unique formula identifier, the product categorization code, the user identification, the company name, the rapid access contact details, etc.

The full messages are exchanged only on demand.

It should be stressed, that such a pattern is for consideration only if the size of the data is very large compared to the meta-data and when rapid access to the full data can be delayed until the full dataset is available[28].

Examples

Based on the patterns presented above, the following could be considered[29]:

- Under the "publish-subscribe" pattern, each national submission system identifies the national systems of interest to their Poison Centres and submits "subscription" request either directly to them (decentralized) or to a central EU node (hybrid), also specifying the mode (e.g. "meta-data" only or "full" content). For example, the Austrian system may decide to subscribe to Germany for receiving full submissions, to Switzerland for meta-data only, and ignore the submissions from Greece.
- Under the "meta-data" pattern, a query made by a Poison Centre agent to the local national system will first look in the local database across all subscribed metadata and return a list with submissions fulfilling the search criteria. Such a query will be fast enough, since no remote access is required. Only when the agent requests to see the full contents of a specific submission, the national system will submit a request to the remote system and wait for the result. Caching mechanisms could also be foreseen for submissions related to incidents frequently reported to Poison Centres.
- A submission system may also have the option to "upgrade" from "meta-data" only pattern to "full content" (e.g. Austria upgrades their subscription to Switzerland). In this case, it is important that the exchange supports an automated way to bring the requesting submission system up-to-date with all the submissions submitted by the publishing system until that time ("full sync").

6.2.2 Data exchange topologies

The next paragraphs briefly describe available data exchange topologies.

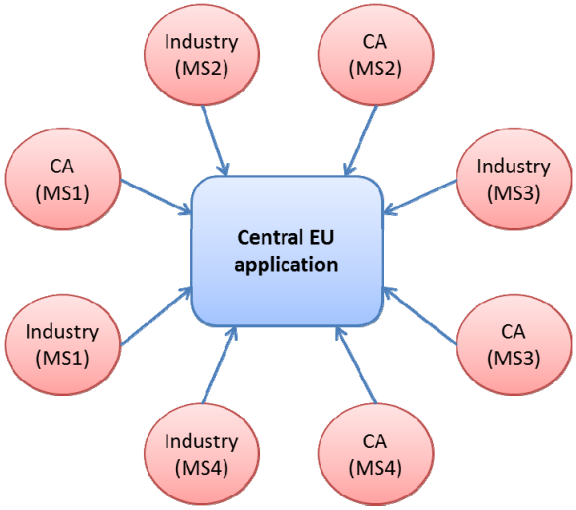
Centralized approach

In a fully centralized system there exists a single submission application for all Poison Centres. All relevant stakeholder entities (e.g. industry, Competent Authorities,

[28] The delay can remain small depending upon the implementation.

[29] These are just example to illustrate how practical scenario can easily be qualified using typical data exchange patterns.

Commission Agents) are registered in this system and need to access it directly in order to perform each task.



This approach brings some benefits, notably:

- Easier access for Poison Centre to all submissions, including those submitted to other Member States.
- Reduced administrative burden for industry from one single submission of a product which is placed on the market in several Member States.
- Reduction in data management work.
- Possibility to perform data analysis at the European level.
- Central management and control of processes.
- 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.
- A centralized system is also able to support the Member States that do not have the resources to put in place their own IT system.

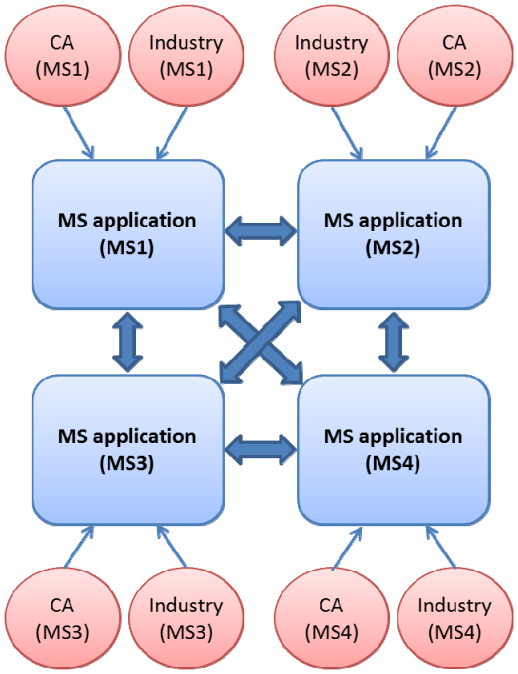
On the other hand however, a centralised topology raises other important issues.

- It poses a major issue for the Member States that currently operate, or are planning to operate, an IT solution to cover their national needs. A centralized solution may have to compromise on a "least common denominator" and this could be unacceptable for some Member States who have already made investments on their own IT solutions and could see features deemed important for them to not be implemented.
- A central system probably will impose that submissions are also made in English. Small and medium sized enterprises (SMEs) may be disadvantaged if they have to translate submissions into English.
- Considering the great number of mixtures on the European market, a centralised database could be too large to maintain at a cost deemed reasonable by the parties involved. In general, the question of its deployment and long-term operating costs will have to be resolved.
- Aside from its cost, the "responsibility issue" will also have to be addressed. A central system obviously will need to be available at all time to serve emergency searches. The delegation of the responsibility of its non-availability when needed to answer life-or-death questions is a legal problem that will have to be resolved. It lies today on the shoulder of each authority who can decide on its own which practical measures or procedures are implemented to address

it. Poison Centres may not want to see that responsibility delegated or lose that control.

Decentralized approach

In a decentralized topology there is no central submission application. The solution comprises of individual national submission applications that communicate between each other with the use of a commonly accepted interface. This interface could be implemented as an agreed set of web services that use an agreed XML format to communicate the messages foreseen.



The main benefit of this approach is that existing national systems can continue operating albeit with an adapter module that would ensure that outbound messages are formatted according to the agreed standard and incoming ones are converted to the internally consumed format.

This approach also has its limitations:

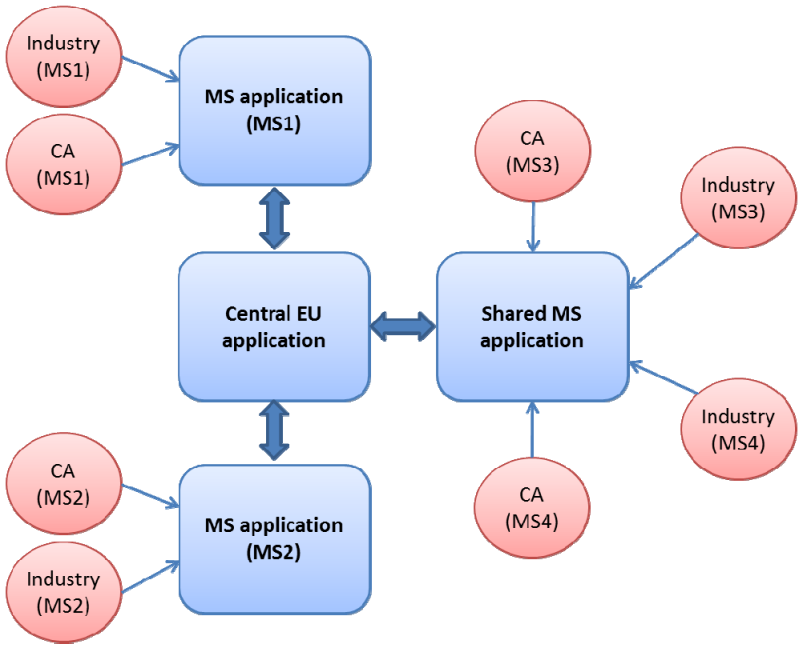
- Exchanging data with other partners requires establishing an explicit channel. This is manageable when the number of parties remain small but can become a problem as soon as that number increases, especially considering that communications must be secured.
- Submissions have to be sent many times. If a new partner is added, submissions need being resent once more.
- Monitoring and reporting at European level is not easy to fulfil.
- Member States that do not have the resources to put in place their own IT system are left with their problem.

Hybrid

The hybrid topology attempts to bridge the gap between the centralized and decentralized ones by keeping the best aspects of both without their main drawbacks.

The hybrid approach is based on the "message broker" architectural pattern for message validation, message transformation and message routing. It mediates communication amongst applications, minimizing the mutual awareness that applications should have of each other in order to be able to exchange messages, effectively implementing decoupling.

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 node.



This topology offers multiple options, one being illustrated here: The central node can be implemented as a simple broker, 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. Yet, it may not support the submission of data by industry, something that remains the prerogative of Member State authorities.

Or, the central node can be extended to offer the submission service, storing all submissions centrally and allowing Member States to obtain the submissions concerning them using the now familiar "publish-subscribe" pattern.[30]

This topology provides several advantages and will be discussed in greater detail in the coming sections.

6.3 Main available tools

Now that we are armed with the basic concepts relevant to encryption and understand some of the core principles underpinning data exchange platforms, we turn to a discussion on actual, practical tools that can be used to concretely resolve our need to securely exchange data between partners.

We know that the underlying communication channel will be the public internet, alternative such as private network being too expensive to deploy and operate. We believe there are only a few practical solutions available to exchange data over the internet, some being standard, off the shelf and other requiring specific development:

- Email
- File transfer
- Internet-based application

[30] The picture illustrates the fact that national Member State endpoints can either be implemented as systems specific to a single Member State or grouped in systems commonly used by multiple Member States. At the level of the central node what would be needed is the configuration of the endpoint that corresponds to each Member State, regardless of whether or not these endpoints are physically distinct.

We will now discuss them and show how they can be made secure to meet our requirements.

Email

Electronic mail, most commonly referred to as email, is a method of exchanging digital messages from an author to one or more recipients. Email has the following main characteristics:

- Email messages have a body and possibly attached documents.
- Sender and recipient are known by their email address in the form john.doe@email.org.
- The transmission of electronic mail within the internet uses the Simple Mail Transfer Protocol (SMTP), defined in several Internet standards, and is intrinsically insecure. That is, email messages are transferred in clear over the public internet.

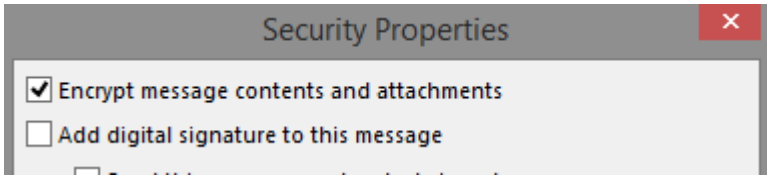
Email communication can be secured either using symmetric encryption or asymmetric encryption.

Relying on symmetric encryption has the following consequences:

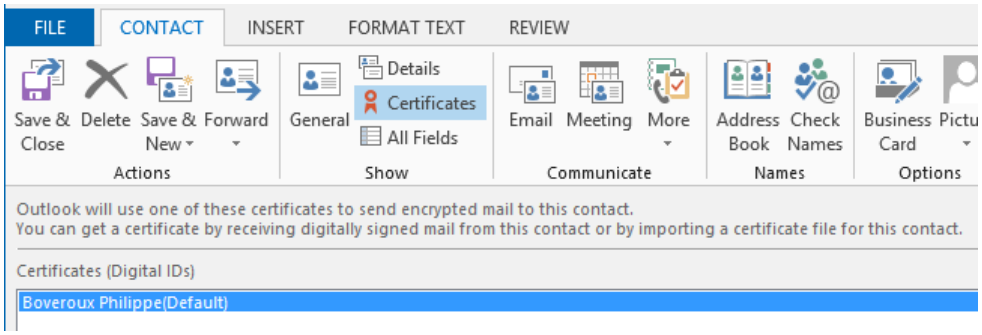
- As explained when introducing the concept, symmetric encryption can be used to encrypt documents attached to an email message. It cannot encrypt the message body which should thus never contain confidential information if this solution is used.
- With symmetric encryption, the sender must 1) encrypt the document(s) with the secret of his choice and 2) securely send the key to all recipients. The dispersion of the secret key can be perceived as an issue, especially if the document has to be stored in encrypted form, the key serving only for punctual decryption when accessing the content.

On the other hand, asymmetric encryption has other implications

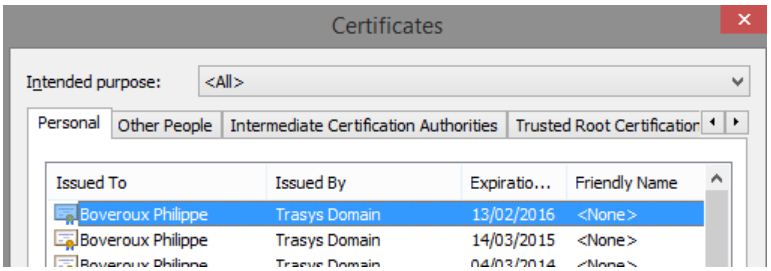
- Public key infrastructure tool is embedded in most email agents; notably in the widely used MS Outlook. The tool can encrypt the message entirely, message body and attachments.
- When integrated in the email agent, encryption and decryption is transparent: selecting 'Encrypt message' will encrypt the email with the recipients' public keys; an encrypted email destined to you is immediately decrypted, its content and attachments shown in clear. (Saving attachments creates a local unencrypted version.)



- Recipients' public key are typically stored in contacts. The sender thus generally has to manage his contact's digital certificates in his contacts. The example below shows the Outlook contact of one the document's author.



- Sender's private key are kept in a secure key store on the user's PC. For instance with MS Windows, in Internet Explorer's certificate stores. The example below shows the private key of one the document's author.



In conclusion, email communication can be easily secured using commonly available tools. It essentially requires proper management of the secret keys or digital certificates.

File transfer

Transferring files via another mechanism than email usually requires setting up FTP (File Transfer Protocol) servers. With the advent of cloud services, transferring files is now almost as easy as exchanging emails.

> Note: In this discussion we leave aside the question of whether transferring confidential, even in encrypted form, via an external cloud provider is secure. This is a question each organisation must answer for itself weighing pros and cons. We consider here that relying on a cloud provider is acceptable. Should it not be the case, it is possible to return to the old FTP solution, but it then requires some infrastructure capabilities that may be beyond that of Poison Centres.

With the file transfer mechanism, one party – sender or receiver – sets up a repository accessible to the other party via its location, i.e. its URL on the internet[31]. The other party may then either download the documents stored by the sender or upload documents destined to receiver(s).

Assuming the receiver sets up the transfer repository and a symmetric encryption scheme, the sender must then 1) encrypt the document(s) with the secret of his choice, 2) upload the encrypted document , and 3) securely send the key to the receiver who will download and decrypt the document. If the sender is in charge of setting up the transfer repository, the process is the same with the slight difference that multiple receiving parties may be given access to the repository to download the documents.

Using asymmetric encryption, one can obviously follow the exact same procedure: encrypt document with the receiver's public key and load it on the transfer site where the receiver can take it before decrypting.

[31] This URL will typically look like https://www.dropbox.com/sh/ueowngbw08s/pkPh2aQ3JGa?dl=0

This is not as transparent as with a modern email agent and we do not know of any cloud-based solution that would provide the same level of user-friendliness.

As we can see, a file transfer mechanism does not seem to bring any benefit over mere email exchanges. There is one though: emails have a limit to the size of attachments (typically a few gigabytes, GB) that file transfer does not have, allowing easy exchange of very large documents.

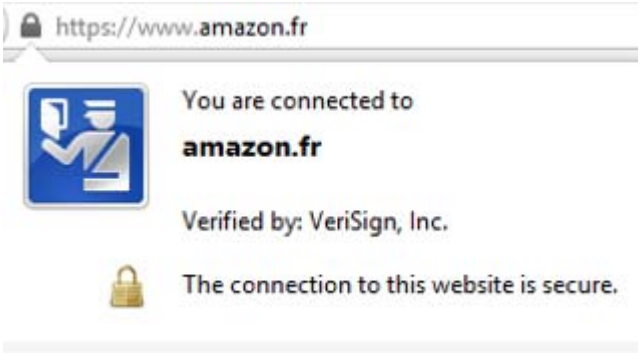
Internet-based application

Internet-based application is the third and most sophisticated solution. The development of such application allows to cater for very specific requirements in various ways. Yet, it must rely on one premise: securing the communication channel between client and server by using HTTPS. (in other words, communication over plain HTTP is not secure.)

HTTPS (also called HTTP over SSL or HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer (SSL). The main motivation for HTTPS is authentication of the visited website and to protect the privacy and integrity of the exchanged data.

HTTPS indeed provides the following guarantees:

- The server-side can be authenticated and thus trusted. It is easy to verify the server's identity: the browser allows consultation of the server's digital certificate on every https connection as highlighted in the site's URL.



- The data exchanged by the client and the server during a session are encrypted.

The cryptography mechanisms of HTTPS are those of a public key infrastructure where only the server side has a digital certificate.

The client side can be either

- A web client such as a browser that has all necessary mechanisms to enter in a secure session with a secure server. This is what we routinely do when performing e-commerce transactions over the internet.

  One can thus design secure web applications where all data encoded in forms by a user (data fields as well as uploaded documents) can be securely transferred to the server.

- Another software application programmed to use the Transport Layer Security protocol to establish secure connections with the server.

  One may thus develop applications that will automate secure data transfer between a client application and the server.

An important feature is transparency of the security: once the secure connection is established (and this is the responsibility of programs), securing the exchanged data

takes place "on the fly" and is performed by the client and server application without user's intervention.

An important limitation is that HTTPS is "one-way": only the server has a digital identity and can be authenticated using the standard mechanisms of the public-key infrastructure. Establishing "two-way" security is possible technically but requires that:

- The client-side infrastructure supports the secure protocol.
- The client (user or application) has a digital certificate of his own.

Two-way security is generally limited to messaging systems where all parties must be authenticated, often in situations where a communicating party may act as client and server.

Note that email being an Internet protocol/application it is technically possible to design an internet-based application that securely sends encrypted emails to recipients. It will require, as seen above, that the recipients' public key are stored in the application's digital key store, but will allow the possibility to securely exchange any electronic message with a well-managed list of recipients.

Summary

The table below sums up the implications in relation with using a certain type of encryption with the proposed tools.

Tool	Symmetric encryption	Asymmetric encryption
Email	Secures attachment	Secures email body and attachments
	Secret key must be sent via a separate channel to every recipients	The digital certificate (public key) of every recipient must be known by the sender
	Requires manual encryption and decryption steps	Transparent with email agent including a PKI feature or plug-in
	Recipient keeps the secret key if document must remain encrypted	Sender keeps his private keys if an email older than his current certificate must be read again (and have not been separately saved in unencrypted form)
		Allows authentication of sender is message is signed

Tool	Symmetric encryption	Asymmetric encryption
File transfer	Secures document files	
	Always exchange of very large documents	
	Secret key must be sent via a separate channel to every recipients	The digital certificate (public key) of every recipient must be known by the sender
	Requires manual encryption and decryption steps	Requires manual encryption and decryption steps
	Recipient keeps the secret key if document must remain encrypted	Sender keeps his private keys if a document older than his current certificate must be read again (and have not been separately saved in unencrypted form)
		Allows authentication of sender is file is signed
Internet application	Not relevant	Transparent encryption by client for server
		Client is any program capable of establishing an HTTPS connection with a server
		The mainstream client is the internet browser
		Allows the development of applications that automate data exchange
		Two-way authentication is possible but technically and administratively more challenging.
		Encrypted emails/messages can be sent to a managed list of recipients.

6.4 Secure data exchange between Poison Centres

In the previous sections we have defined the security concepts necessary in our context, we have briefly introduced the main communication patterns and topologies that we can rely upon, and we have discussed the concrete case of three tools/platforms that can be used to exchange data over the internet, our target communication platform.

Actual options for the secure exchange of data between Poison Centres can now be proposed using the these concepts.

The options must be weighed according to common criteria that we believe must be:

- **Number of expected messages**. For a small number, one can expect that manual intervention remains a manageable possibility. This is certainly no longer true when that number grows large. (Of course, such threshold will be Poison Centre dependent.)

- **Number of partners in communication**. Should Poison Centres exchange data with their neighbouring countries[32] only or will all Poison Centres.
- **Variability of the number of partner**. Are the communicating partners very stable (neighbours only) or does it depend upon changing conditions, possibly on a mixture per mixture basis.
- Obligation to **involve user control in the communication**, for instance to verify data before sending.
- Necessity to establish **bilateral secure connections** (which we suspect is the case), that is channels where data flows both ways.
- **How the request for data is made**. Do we anticipate that a Poison Centre having the need for a submission available in another Poison Centre will request the file (via a direct phone call or by posting a request to an application) and receive it after a certain processing delay? Or do we foresee a genuine subscription mechanism whereby a Poison Centre could register its interest in certain mixtures submitted to another Poison Centre and receive the data automatically?
- **Urgency of the communication**. Two different types of communication must be considered in the business of Poison Centres:
    - **Urgent** exchange of information in case of incident. The exchange must be fast and efficient (in a few minutes) and concerns a limited amount of data. Key requirements for this kind of communication to succeed are the non-ambiguous identification of mixtures/products, fast communication channels and clear communication protocols.
    - **Non-urgent** exchange of information. In this case, time to access and provide the information is not a factor, nor is the size of the data exchanged.

One certainly directly sees that a distinction appears between approaches where manual intervention of a user is required and system where data exchange must be automated and software application become necessary.

In the discussion we will focus on email and internet application, ruling out the file transfer approach because 1) its pros and cons are generally the same as email, 2) it is somewhat less user-friendly when using asymmetric solutions, and 3) we do not need to exchange documents that cannot be attached to emails.

Criteria	Email	Application
Number of messages	The number of messages must remain low	Can handle as many messages as needed (provided the application is scalable)
Number of partners	Must be handled using distribution lists. Number is not an issue in our context, yet managing the list can pose problems	Can handle as many partners as required. They will likely be controlled by application configuration to easily add/remove communication points
Partner variability	May be handled by distribution lists if the criteria are not dynamic	Can handle distribution in a flexible way (based on rules implemented in the application)

[32] Where Poison Centres are regionalised they obviously must at least be able to exchange data inside the country.

Criteria	Email	Application
User control	Sending email generally requires user control but is possible to automate their generation and delivery	User control can be introduced in an application, possibly explicitly via a workflow
Bilateral secure connections	Email is a one-way channel: a sender sends a document to a receiver. Of course, bilateral connections are achieved by inverting the roles. In practice it means that digital certificates are exchanged both way	As we have seen, two-way security is complex to achieve. Can we find a way to simplify this? More below
Request for data	If the request for information is limited, it can be processed manually, files extracted and encrypted and sent by email. Otherwise, the management burden is too heavy and automated options must be investigated	An application can be programmed to provide sophisticated way of requesting data of interest based on queries. One can for instance declare an interest in mixtures of a certain submitter and aimed at the industrial market. (This is a simple query, more complex could be foreseen.)
Urgency	Manually encrypting an email for a recipient urgently requiring information is likely to introduce delays, even if protocols are easy and personnel is trained and drilled.	Accessing an application remotely to query the information that is urgently needed is possible (see above point). Still, dealing with fast queries can remain problematic if query interfaces are not designed to cover such cases.

We see that as soon as the number of messages is important and some flexibility / automation is required, the only remaining option remains a specific internet application.

We thus face two difficulties: securing many bilateral connections and devising a way to request for data in some automated way. We will briefly discuss them before coming back to the matter of time-critical, urgent requests.

Securing many bilateral connections

If N partners participate in bilateral communications, each partner needs to set up (N – 1) channels. Applying this to the 35-40 Poison Centres in EU, each Poison Centre may have to set up 34-39 bilateral connections.

This can become a difficult task to surmount when we need the communication to become secure over the public internet. It remains possible though that Poison Centres exchange their digital certificates and configure data exchange application, either using their email systems or developing their own application to send data to their counterparts in other countries. They will of course have to deal with the management of the certificates; especially, devise procedure for their renewal before certificate expiration. The only way to overcome the explosion of connections is to share the data and store it at some central place. This is what regionalised Member State do already: the submissions are received by one "lead" Poison Centre and made available to the others, which requires only N – 1 secured, one-way connections.

Automating data inquiry

This point goes slightly beyond the scope of the study. Yet, it is interesting to note that if one wants to automate data exchange of a part of the data available, a smart way to inquire for the data of interest is necessary. (If a complete data set is always transferred between Poison Centres, then this question is irrelevant.)

It is not a far-fetched thought to imagine that a small XML query language could be devised based on the proposed format to model data inquiries.

Below a possible example for an inquiry about consumer mixtures submitted by The Mix Inc. and having H318 labelling hazard statement.

```
<query>
  <submitter>
    <name>The Mix Inc.</name>
  </submitter>
  <product>
  <userIdentification>consumer</userIdentification>
  </product>
  <mixture>
  <labelling>
    <hazardStatement code="H318"/>
  </labelling>
</query>
```

Provided that systems can interpret such request and perform the request to compile the matching mixture in an XML data bundle, one can start thinking of ways of interactions between Poison Centres.

Time-critical, urgent requests

Poison Centres already have procedures in place to efficiently respond to incidents, when calls are made to their emergency line in case of intoxication. Here we devote some thoughts on the urgent electronic exchange of information at the request of another Poison Centres.

The envisaged scenario is the following one: a Poison Centre processing an emergency call realises that information on the mixture is not available in their database (no matching UFI or trade name is found); instructions to the caller can be given based on the communicated information on the label (pictograms) but uncertainty remain and it appears that the mixture is likely marketed in another country. In this case, a call to the relevant Poison Centre may be necessary.

Phone calls will certainly remain a typical mean of obtaining information in such a situation, but time can be lost in explaining the context orally to the colleague on the line (something that may need to happen in a non-native language.

If the called Poison Centre is in possession of relevant information, it can be passed orally but it may be necessary to send it electronically as well. Under pressure, preparing manually encrypted emails may cause delay and error. An efficient approach could be the development of an automatic email delivery platform: an application configured with the email address of all Poison Centres and with their public keys that will extract the relevant data in the form of an XML document, place it in an email, encrypt it and send it to the caller.

To conclude on this particular topic, it must be remembered that establishing electronic data exchange procedures between Poison Centres to deal with emergency require:

- That operational procedures are established to deal in a Poison Centre with a remote emergency call and the execution of the secure data transfer.

- A reliable communication mean. Email is routinely used today and is generally an efficient transfer mechanism. Yet, one should not forget that email does not come with a guarantee of service: the urgent email may arrive too late.

This is thus another situation where centralisation of the data can bring benefits as it eliminates most of the communication overhead.

6.5 Secure data exchange for all stakeholders

The discussion of the previous section is limited to Poison Centres and already shows that establishing automated, secure, two-way exchange channels is a daunting, not to say impossible task. Note that all the words are relevant here:

- Automated: we speak of system-to-system data exchanges, not about the casual manually prepared email used to send an encrypted submission.
- Secure: the communication channel must be the internet secured by appropriate technical means, that is HTTPS.
- Two-way (or bilateral): each partner is a sender and a receiver.

What happens if we bring industry into the equation: we add a multitude of client applications that need to connect to the Poison Centres' servers to send their submission. At first sight, this is not a problem since Poison Centre servers are expected to exist already and industry submissions do not make the communication between Poison Centres more complex.

With such approach however, industry has to separately connect to as many Poison Centres applications as the number of Member States where the mixture submitted is marketed. This is a process industry has been asking to simplify via a unique submission valid for all concerned Member States. Additionally, as has been indicated when considering industry's perspectives, simplification requests have been made in other areas, notably the harmonisation of the data requirements and the possibility to submit information in bulk, i.e. one document including several submissions.

The latter requests are now met by the availability of an harmonised XML format supporting bulk submission. That format is a foundation to establishing an electronic submission scheme from industry to the Appointed Bodies. As indicated when describing the format in details, a submission document is valid for one submitter and one Member State, in accordance with the applicable legal provisions.

Industry's request to be given a possibility to submit the information once for all Member States where a mixture is marketed remains. Leaving aside the necessary changes to the format to support this, we can think of two ways to respond to industry's request:

- Industry submits a submission aimed at all concerned Member States to one of them. The Poison Centre receiving the submission dispatches it to the other Member States / Poison Centres.

  This approach is not fair to Poison Centre in charge of dispatching. It also introduces points of failure in the distribution if the dispatcher fails in his task. The main advantage of such approach is that it relies on the infrastructure in place: there is no need for any additional system.

- Industry submits a submission aimed at all concerned Member States to a central application managed for instance by ECHA or the Commission where Poison Centre can access to the data that concerns them; possibly uploading the data into their own system.

  This solution is fair to Poison Centres and is robust, but it requires the development of a central application to receive and store all industry submissions. Poison Centres are free to continue using their own database into which the submitted data can be loaded as they wish and submission will continue to be available at Member State level.

This approach, qualified as "hybrid" when introducing data exchange topologies, bridges the gap between pure centralized or decentralized solutions by keeping the best aspects of both without their main drawbacks. It presents the following advantages to an overall submission and data exchange scheme:

- Industry partners can be identified and authenticated in a common, EU-wide manner; in a way similar to what happens in REACH-IT. This brings several advantages, notably a likely decrease of false submissions and an ease on the burden that today falls on Poison Centres to verify the origin of submissions. The central part of the system could allow multi-national corporations to sign up once yet providing information specific to particular Member States where relevant.
- Industry can submit information about a mixture once and provide country specific information in one place, effectively meeting one their most important demand for simplification. Additionally, the data can be easily completed when market conditions changes; for instance, if a mixture is marketed in a country where it was not, a mere update to the mixture's market information is enough.
- Poison Centres have a central place where information about hazardous mixture is consolidated at the EU level. This is seen as an efficient way to deal with the challenges brought by an open market where citizens can easily bring mixtures abroad and emergency calls may concern mixtures unknown to a Poison Centre.
- Appointed Bodies or Poison Centre must not be forced to renounce to their local systems. Data replication schemes can be developed to transfer relevant data from the central database to a local Poison Centre's database. Such transfers can easily be configured to support different requirements regarding the rate of duplication (e.g. immediate, daily) of submissions to the central system or the filtering of the transferred data according to various selection criteria (e.g. one country, several countries, all countries; hazardousness).

  On the other hand, Member States may decide to rely only on the central system[33].
- True relations between submissions can be established and mixture history can be reconstructed at levels not possible before.
- Data query and aggregation is possible at levels not possible before. Moreover, the data query interface being centralised, it can be seen as way to easily retrieve information in case of emergency calls when the mixture is unknown to the contacted Poison Centre.
- EU reporting / statistics can be established. With this respect, it is likely that the introduction of the notion of UFI will allow searches and reports not possible before; especially when put in relation to a central repository.
- Such central system could on the long term serve as repository of other figures, notably those related to emergency calls. (This requires willingness from Poison Centres to share the data and some harmonised format and upload mechanism.)

This "hybrid" approach, also seen as a "one-stop-shop" solution, is recommended as the long term solution that better serves the requirements of all stakeholders: industry can benefit from a single-submission approach and Poison Centres benefit from a larger pool of data from which they can extract for local processing any information they see fit to fulfil their duties.

[33] Note that this creates a single point of failure from their perspective and consequently will impose stringer requirements on the availability of the central system since it must not only be available for submissions (an action that can suffer a delay) but serve for incidents (actions that cannot accept delays).

6.6 Conclusions

The existence of the harmonised data exchange format naturally brings forward the question of improved data exchange, automated or not, between partners. We have tried here to provide some theoretical background for an overview of practical options/solutions for the secure exchange of data.

On the short term Poison Centres will need to adapt their software to process submissions in the harmonised format; and those who do not have IT solution in place already will need to develop one. Industry on the other end will have to develop extensions to their current systems to generate the submissions in the requested format; or may use the basic application if they have a small number of mixtures to submit.

With respect to exchange of information between Poison Centres, it is likely that ad-hoc, manual, e-mail based options will be pursued on a short term basis. Such ad-hoc solutions will probably rapidly show their limits, especially for large Poison Centres.

The need for a better, common and practical approach for securely exchanging data between Poison Centres in automated ways, coupled with the perceived benefits of having an intermediate submission platform where industry can push its submissions and Poison Centres can pull the data of interest, will possibly lead to the implementation of such platform which in our view is an ideal approach, maximising the most critical requirements of all parties involved.

- From industry perspective: a central place where to submit information for all relevant countries via one submission per mixture, eliminating most of the difficulties faced today that are due to the variety of formats and submission processes.
- For Poison Centres: the possibility to access a larger pool of information provided in the harmonised format guarantying their quality and homogeneity, yet retaining the possibility to maintain their local repository.
- For all parties involved: better authentication, lessening administrative burden; the possibility deriving from the aggregation of data to provide more sophisticated query and data reporting.

A UML model of the harmonised format

The model is split into two diagrams, once centred on the *Submission* entity and the other on the *Mixture* entity.

Figure A-1: Business Model - Submission

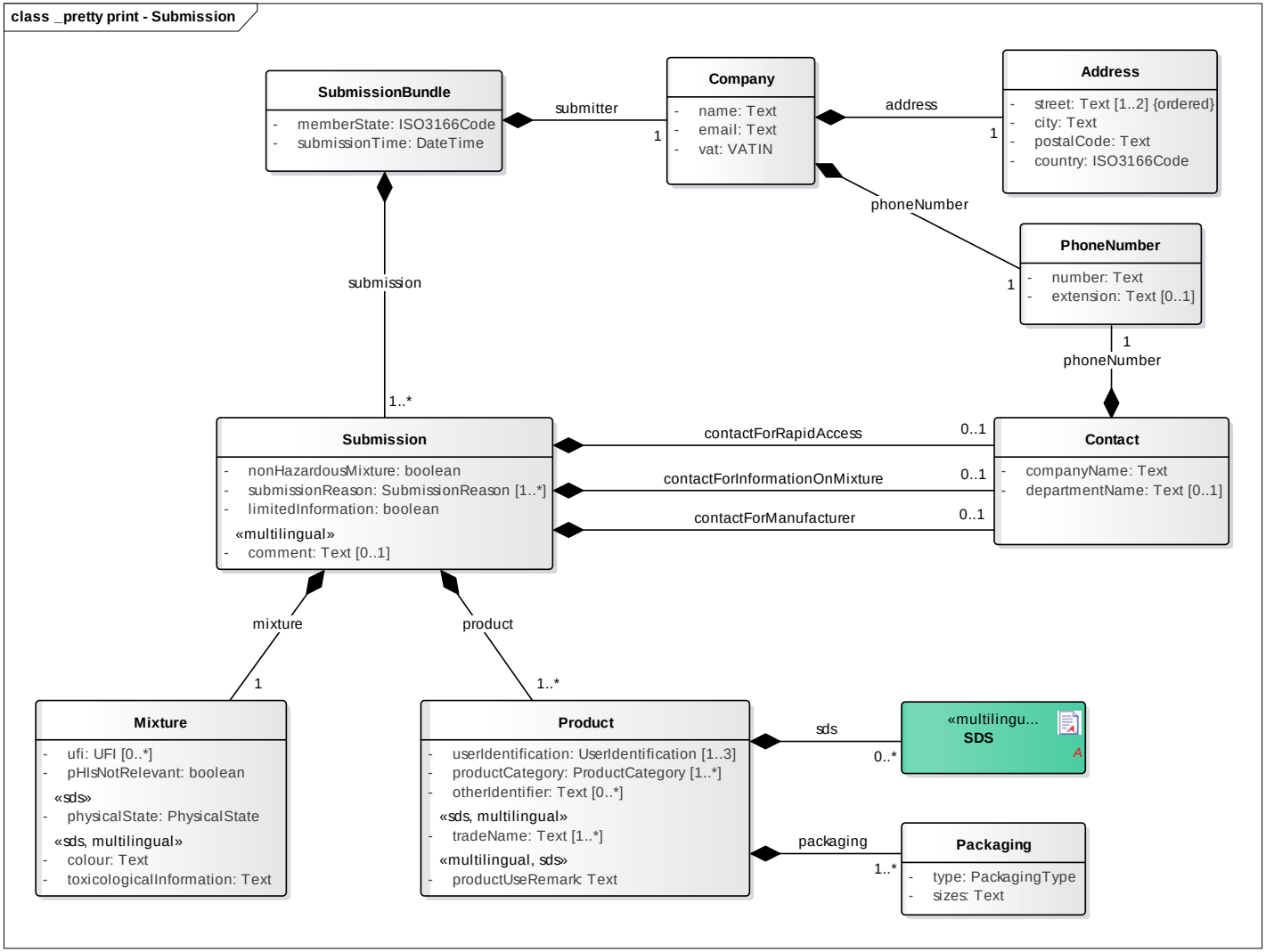
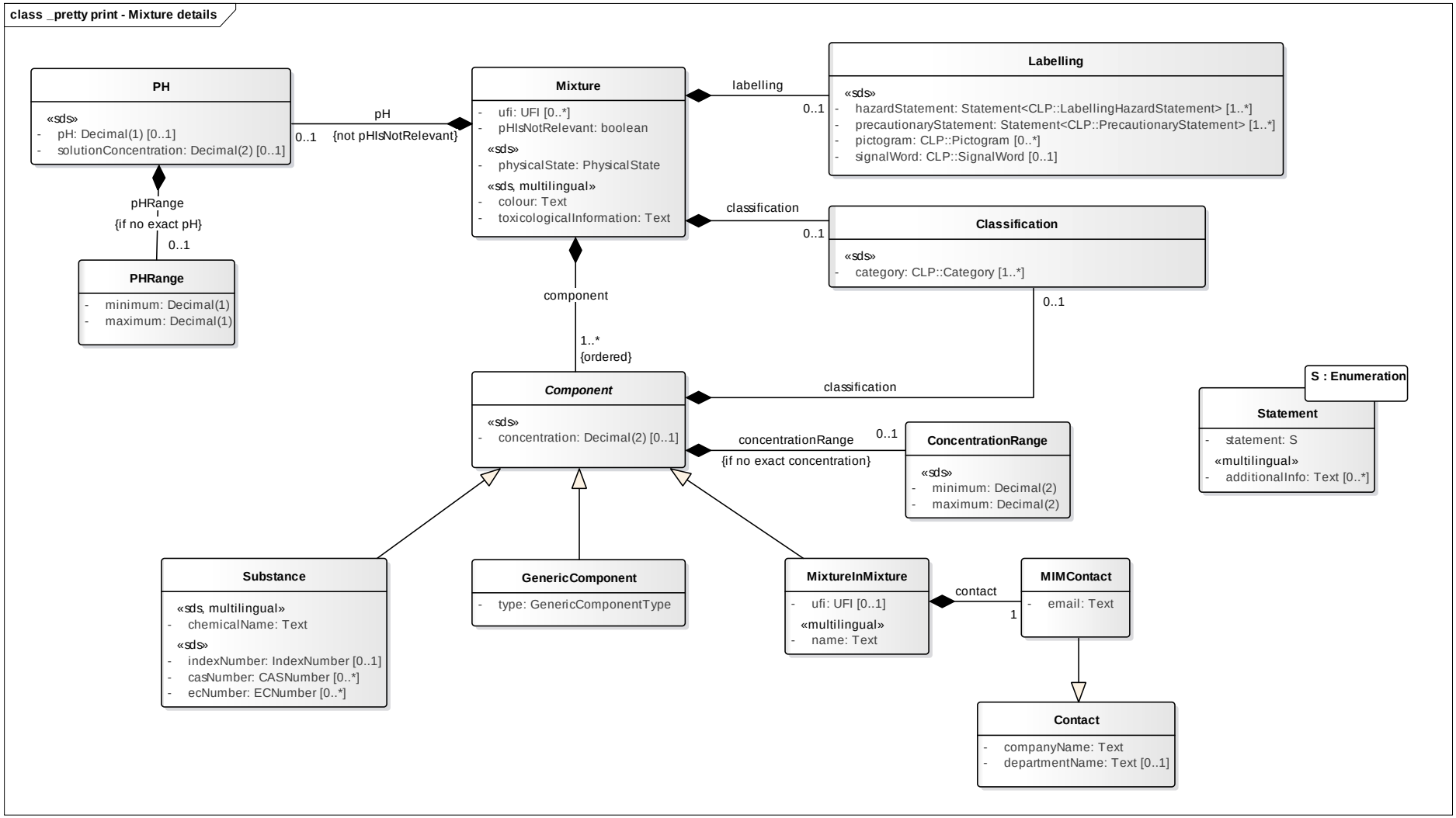
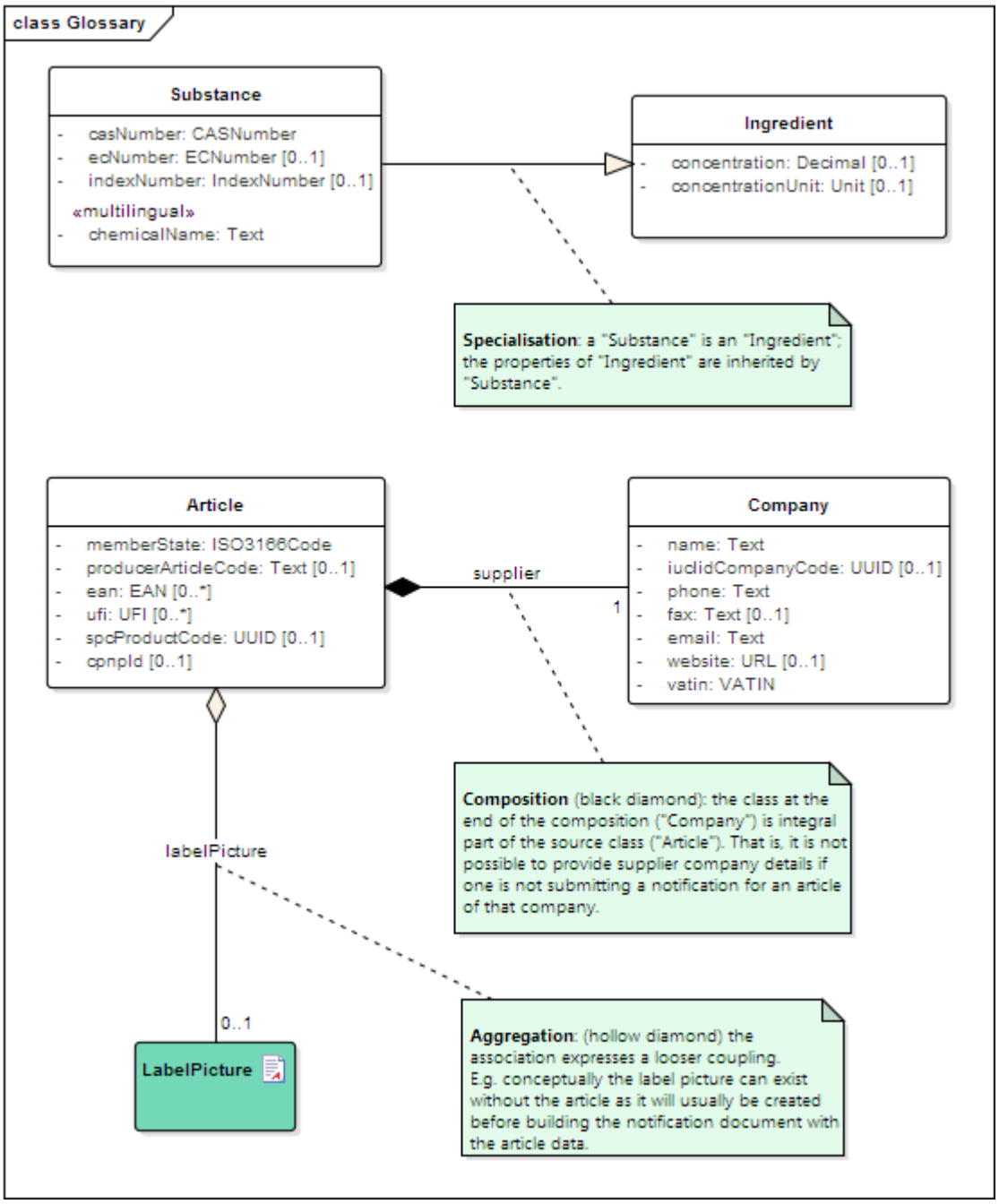


Figure A-2: Business Model – Mixture details

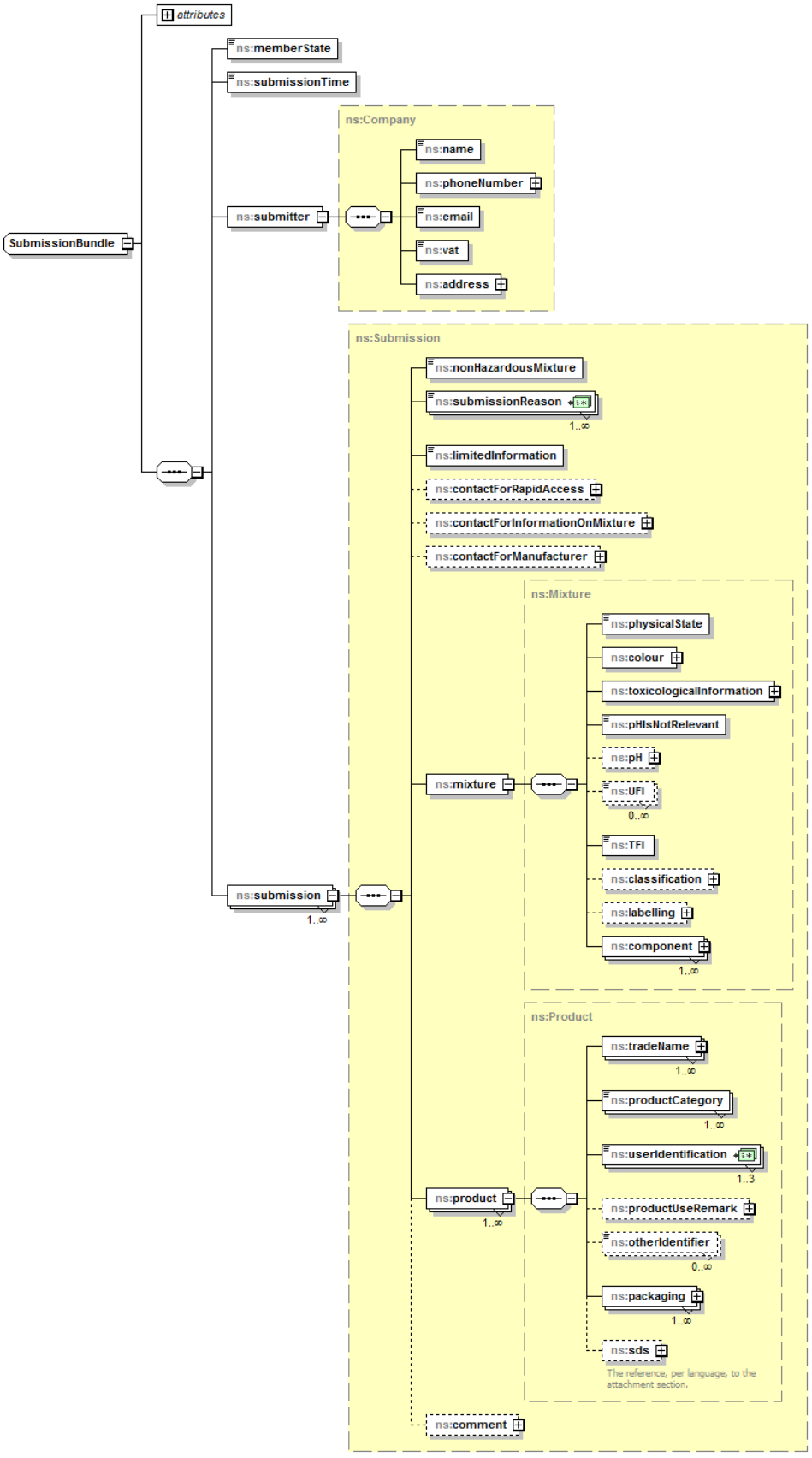


The figure below briefly explains relevant types of associations in UML class diagrams.



B XML schema for the harmonised format

The image bellows depicts the structure of the XML schema with most of the main complex elements unfolded. The complete documentation of the XML schema is available in [XML_SCHEMA].



C Annexed documents

The following documents are annexed to this Final Report:

Table C-1: Annexed documents

Questionnaire for Member States Appointed Bodies	*PoisonCentresQuestionnaire4MS2015_10-02-2015_EN.pdf*
Questionnaire for industry	*PoisonCentresQuestionnaire4Industry2015_10-02-2015_EN.pdf*
Attachment to question 24 in Member States questionnaire	*PoisonCentresQuestionnaire4MS - Question 24.pdf* Question 24 was "In the attached Excel sheet the information to be submitted is summarized according to the current Commission working paper. For each section please indicate if that data is required in your current process and/or if you ask for additional data from the industry."
Consolidated answers to question 19 in Member States questionnaire	*PoisonCentresQuestionnaire4MS - Question 19 Consolidation.pdf* Answers from Member States that demanded confidentiality (in their answer to question 6) have been deleted.
Consolidated answers to question 24 in Member States questionnaire	*PoisonCentresQuestionnaire4MS - Question 24 Consolidation.pdf* Answers from Member States that demanded confidentiality (in their answer to question 6) have been deleted.
Consolidated answers to Member States questionnaire	*PoisonCentresQuestionnaire4MS - All answers - Charts and pivots.xlsx* This document exists in two versions: one marked 'CONFIDENTIAL' containing all answers and one stripped from the answers where respondents replied 'No' to question 6.
Consolidated answers to industry questionnaire	*PoisonCentresQuestionnaire4IND - All answers - Charts and pivots.xlsx* This document exists in two versions: one marked 'CONFIDENTIAL' containing all answers and one stripped from the answers where respondents replied 'No' to question 6.