CEN

WORKSHOP

AGREEMENT

CWA 17513

May 2020

ICS 03.100.01; 13.200; 35.240.99

English version

Crisis and disaster management - Semantic and syntactic interoperability

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No.:CWA 17513:2020 E

Contents

European foreword

This CEN Workshop Agreement (CWA 17513:2020) has been developed in accordance with CEN-CENELEC Guide 29 'CEN/CENELEC Workshop Agreements – The way to rapid consensus' and with the relevant provision of CEN/CENELEC Internal Regulations – Part 2. It was approved by a Workshop of representatives of interested parties on 2019-04-29,the constitution of which was supported by CEN following the public call for participation made on 2019-04-01. However, this CEN Workshop Agreement does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

Results incorporated in this CEN Workshop Agreement received funding from the European Union's 7th Framework Programme for Research, Technological Development and Demonstration under Grant Agreement (GA) N°607798 and N°607078. This CEN Workshop Agreement (CWA) is based on the results of the DRIVER+ and EPISECC research project. The final text of CWA 17513:2020 was submitted to CEN for publication on 2020-03-27.

The following organizations and individuals developed and approved this CEN Workshop Agreement:

— Austrian Institute of Technology GmbH/ Georg Neubauer, Maria Egly, Patrick Zwickl;

— Austrian Red Cross/ Thomas Seltsam;

— German Aerospace Center/ Angela Uschok;

— HITEC Luxembourg S.A./ Harold Linke;

— Public Safety Communication Europe Forum/ David Lund;

— Riskaware Ltd/ Robert Gordon;

— Netherlands Organization for Applied Scientific Research/ Erik Vullings;

— Frequentis AG/ Thomas Obritzhauser;

— SBA Research gGmbH/ Kevin Mallinger, Markus Klemen, Andreas Ekelhart;

— The Main School of Fire Service/ Tomasz Zwęgliński;

— Thales SIX GTS France SAS/ Laurent Dubost; and

— University of Split/ Snjezana Knezic, Martina Baucic.

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CEN-CENELEC policy on patent rights is described in CEN-CENELEC Guide 8 “Guidelines for Implementation of the Common IPR Policy on Patent”. CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk.

Introduction

Current and future challenges, due to increasingly severe consequences of natural disasters and terrorist threats, require the development and uptake of innovative solutions that are addressing the operational needs of practitioners dealing with crisis and disaster management. This document is based on the results of DRIVER+ and EPISECC and defines requirements on how to achieve organizational and cross border interoperability on semantic and syntactic level for crisis and disaster management.

DRIVER+ (Driving Innovation in Crisis Management for European Resilience) was a European research project funded under the 7th Framework Programme (FP7) that aimed to improve the way capability development and innovation management is tackled. EPISECC (Establish a Pan-European Information Space to enhance the Security of Citizens) on the other hand aimed to develop a concept of a common European information space.

DRIVER+ identified four capability gaps that specifically refer to operational interoperability:

— Exchanging crisis and disaster related information among agencies and organizations: Shortcomings in the ability to exchange relevant information among agencies and organizations, such as authorities, first responders and crisis managers.

— Common understanding of the information exchanged in response operations: Limits in the ability to ensure a common understanding of the information exchanged (terminology, symbology) by all crisis and disaster managers involved in response operations.

— Understanding crisis and disaster management capabilities of participating organizations: Lack of mutual knowledge or alignment of operational needs and procedures between different organizations responding to the same scenario.

— Shared awareness of status and planned efforts in crisis and disaster management operations: Insufficient understanding of the overall current and planned response efforts as well as current strategies across organizations during an event.

EPISECC identified similar gaps related to interoperability in line with the ones identified in DRIVER+. Information exchange between agencies and organizations involved in crisis and disaster management is of imperative relevance during all phases of the disaster management cycle. Especially in the response phase of a crisis or disaster exchange it is necessary to ensure adequate response to the triggering event. Information exchange between the involved agencies and organizations need to remain established under any conditions.

The communication between different organizations, regions and countries – with their specific processes and tools – is a major challenge in crisis and disaster management. Both efficient communication and access to critical information is a key requirement for the operation of public safety and security services, as well as in the preparation for and the management of crisis and disasters. The members of this CEN Workshop decided based on the above information to initiate this agreement.

1 Scope

This document defines requirements to achieve organizational and cross border interoperability on semantic and syntactic level for crisis and disaster management. The document provides syntactic requirements on the realization of tool connectors to a platform, standardized protocols, validation of transmitted messages, security issues, message distribution approaches and system resilience. Regarding semantic services recommendations on the establishment of semantic resources as well as the establishment of a semantic mapping and matching are given.

This document is dedicated to support both practitioners and solution providers in the process of the realization of interoperability between IT solutions designed for the application in the crisis and disaster management domain. Practitioners are people who are qualified or registered to practice a particular occupation in the field of security or civil protection, e.g. crisis managers and responders related to all disciplines of crisis and disaster management and response. Solution providers are those that develop and supply technological solutions that fulfil the requirements defined in this document, with the goal to improve operational capabilities of practitioners.

In addition, use cases for the application of syntactic and semantic services are given. Layer models are described and examples of concepts and topologies are provided.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
actor
role played by a user or any other system that interacts with the subject

Note 1 to entry: Part of the syntax of UML.

3.2
capability gap
gap between the current ability to provide a response and the actual response assessed to be required for a given threat or hazard

3.3
data entity
an entity that was declared to be data and therefore is not parsed when referenced

3.4
data model
graphical and/or lexical representation of data, specifying their properties, structure and inter-relationships

[SOURCE: ISO/IEC 11179-3:2013, 3.2.36]

3.5
dictionary
collection of words, terms or concepts with their definition

3.6
envelope
in the context of message handling, an information object, part of a message, whose composition varies from one transmittal step to another and that variously identifies the message's originator and potential recipients, documents its past and directs the subsequent conveyance by the message transfer system (MTS), and characterizes its content

3.7
interoperability
ability of diverse systems and organizations to work together

[SOURCE: ISO 22300:2018, 3.128]

3.8
ontology
formal representation of phenomena of a universe of discourse with an underlying vocabulary including definitions and axioms that make the intended meaning explicit and describe phenomena and their interrelationships

[SOURCE: ISO 19101-1:2014, 4.1.26]

3.9
physical interoperability layer
layer established by a physical channel that allows data transfer from a sender to a receiver both using or being connected to this channel

Note 1 to entry: The CEN Workshop Agreement does not focus on this layer.

3.10
pragmatic interoperability layer
layer that is basis for harmonized actions centered on a shared situational awareness

Note 1 to entry: The CEN Workshop Agreement does not focus on this layer.

3.11
protocol
convention about the data formats, time sequences, and error correction in the data exchange of communication systems

[SOURCE: EN 61158-4-16:2008, 3.3.36]

3.12
public key infrastructure
hierarchy of "certification authorities" to allow individuals and organizations to identify each other for the purpose of doing business electronically

[SOURCE: ISO 17427-1:2018, 3.20]

3.13
semantic mapping
establishment of semantic relations between the elements of separate collections of concepts

Note 1 to entry: This definition is specifically set up to describe the procedure shown in Annex E.

3.14
semantic matching
matching between the concepts of two collections of concepts via a central terminology

Note 1 to entry: This definition is specifically set up to describe the procedure shown in Annex E.

3.15
semantic interoperability
ability of two or more systems or services to automatically interpret and use information that has been exchanged accurately

[SOURCE: ISO 22300:2018, 3.243]

3.16
social/cultural interoperability layer
layer focusing on social and cultural aspects that make coherent cooperation of involved actors as well as coherent use of systems or services by actors possible

Note 1 to entry: The CEN Workshop Agreement does not focus on this layer.

3.17
solution
mean to solve a challenge

Note 1 to entry: In the context of this CEN Workshop Agreement a solution can be composed of one or more processes and one or more tools to execute the processes.

3.18
syntactic interoperability
ability of two or more systems or services to exchange structured data

[SOURCE: ISO 22300:2018, 3.253]

Note 1 to entry: The definition taken from ISO 22300 is also used to explain “syntactic interoperability” as used in this document.

3.19
taxonomy
scheme of categories and subcategories that can be used to sort and otherwise organize itemized knowledge or information

[SOURCE: ISO 5127:2017, 3.8.6.07]

3.20
terminology
set of terms representing a system of concepts within a specific domain

[SOURCE: ISO/TS 17117:2002, 3.1]

Note 1 to entry: A terminology can be set up in different ways, such as a vocabulary or as a taxonomy. The terminology may include definitions of terms.

3.21
topology
ways in which the main elements enabling syntactic and semantic interoperability can be organized

3.22
vocabulary
list of terms, often given in alphabetical order

4 Symbols and abbreviations

— API: Application programming interface

— C2: Command and control communication system

— CAP: Common alerting protocol

— CBRNE: Chemical, biological, radiological, nuclear and explosives

— CGOR: Cooperation group online room

— CIS: Common information space

— COP: Common operational picture

— EDXL: Emergency data exchange language

— EDXL-SitRep: Emergency data exchange language situation reporting

— EMSI: Emergency management shared information

— EPISECC: Establish pan-European information space to enhance security of citizens

— GDPR: General data protection regulation

— HTTPS: Hypertext transfer protocol secure

— JSON: JavaScript object notation

— KML: Keyhole markup language

— MTS: Message transfer system

— MFA: Multi-factor authentication

— msgType: Message type

— NATO: North atlantic treaty organization

— OGC: Open geospatial consortium

— OID: Object identifier

— PKI: Public key infrastructure

— REQ: Requirement

— REST: Representational state transfer

— RSS: Rich site summary

— SOAP: Simple object access protocol

— SWE: Sensor web enablement

— TDB: Triple data store database

— UML: Unified modeling language

— VPN: Virtual private network

— WFS: Web feature service

— WMS: Web map service

— XML: Extensible markup language

5 Requirements on how to reach interoperability

5.1 General

This Section defines the main requirements to achieve organizational and cross border interoperability on semantic and syntactic level for crisis and disaster management. In several cases, alternative approaches to realize interoperability exist, which are partly shown in the Annexes of this document. In addition, the Annexes provide further information going beyond the content of this Section, dedicated to give more insight to the reader.

The principles of the common information space proposed in this CWA derive from other realizations, e.g. from NATO's work on interoperability. It differs through the:

— domain (crisis and disaster management instead of military domain);

— types of links which bind the participating actors (long term exclusively national level type of alliance in the case of NATO and more heterogeneous and opportunistic links in the case of crisis and disaster management); and the

— budgets available for its development.

5.2 Interoperability layers

In line with the NATO Science and Technology Organization, interoperability of solutions can be categorized in five layers [1] (see Figure 1).

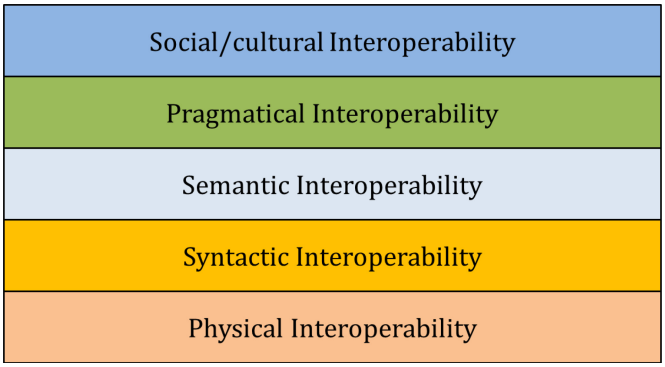

Figure 1 — Layers of interoperability according to the NATO Science and Technology Organization

The definitions of these layers of interoperability are in Section 3. An alternative model is described in Annex A.2. This document is addressing the syntactic and semantic layer.

REQ 1: The actors intending to reach interoperability shall agree on an interoperability layer model for subsequent description of implementation stages. This document recommends using the above model.

5.3 Operational objectives

Interoperability is regarded by practitioners as one of the major capability gaps they are facing in the execution of their duties [2]. This predominant gap includes difficulties in the exchange of information between agencies, as well as in the common understanding of the information exchanged. These aspects relate respectively to the syntactic and semantic layer (see Section 5.2 and Annex A.2).

Concerning the exchange of information, the ability of technical systems to exchange data is crucial both in case of autonomous as well as human-triggered exchange. During cross border or multinational operations the language barrier is recognized as an obstacle in reaching a common understanding.

The main requirements to reach interoperability from an operational perspective are the following.

REQ 2: End-to-end transfer of information between practitioners who operate in different social and operational environments.

REQ 3: Structured transfer of information in different forms, e.g. speech and text.

REQ 4: Fast translation of information, within acceptable round-trip latency times, to allow for human-to-human conversation, to be as effective as face-to-face communication in the same language.

REQ 5: Transfer of information between different forms, e.g. speech to text and video to transcript.

For additional information see Annex A.1.

5.4 Requirements to reach syntactic interoperability

The topology proposed is the message-based interoperability topology (see Figure 2). The main elements enabling syntactic interoperability in a message-based topology are defined below.

— Exchange protocols: Standardized protocols shall be applied to specify how information sent is routed and received. It is common to the protocols that they have a message header and the message content. For more information see Annex C.2.

REQ 6: Actors shall agree on a standardized protocol in the course of process and interoperability platform implementation.

— Message type catalogue: Each message type serves a specific purpose and follows a specific structure which describes how the title, paragraphs, free text areas and data entities (from the data model) are transmitted. Ideally the message types refer to an entity described in a reference data model, but this is not a necessary condition for the use of messages – each message type can refer to a specific data model. The message structure is agnostic regarding the communication channel used to transmit the messages.

REQ 7: Partners shall agree on a common catalogue of structured messages or data structures.

REQ 8: This catalogue shall contain existing standards such as EDXL, CAP, EDXL-SitRep, OGC standards for geo-data (KML, WMS, WFS) and OGC standards for sensor data (SWE). The catalogue can contain specific messages or other type of data agreed between interoperating parties.

— Data-models and domain values: A data model describes what type of entities can be described in a formatted way, how they relate to each other (e.g. a link between a firefighting module and its area of responsibility), and what values can the attributes of entities take (e.g. eye color blue, green, grey, or brown). Each IT system has a data model and domain values. Each type of message precises' the model of entities it can convey. The data model from the sending IT system and the recipients' IT system's data models are usually not the same and a conversion operation to a common data model is needed.

REQ 9: The message structure shall describe the envelope, and the content in terms of paragraph structure, containing texts, multimedia content or data. When data is conveyed by the message, the format shall describe the expected classes their attributes, the possible values and links between classes.

REQ 10: The structure of the messages which are sent shall be verified before routing to the potential recipients.

— Message routing, distribution services: Two approaches on how to realize routing exist – direct addressing or group-based communication.

REQ 11: One of the routing approaches, either direct addressing or group-based communication, shall be selected and implemented.

— The syntactic mapping operation: The mapping is the operation which consists in transforming entities of one data model in entities of another data model. In order to send messages containing structured entities, the sending command and control communication system (C2) needs to map the entities on the message data model, and the reverse operation needs to be done by the recipient of the message to transform the entities of the reference data model into entities of his/her own data model. The mapping operation concerns the entities class, the attributes and the values of these attributes. It can be exact or approximate.

REQ 12: For each type of message, the interoperating parties shall describe, how entities of their own command and control communication system can be mapped (classes, attributes, links and values) on the data model that is supported by the message.

REQ 13: When exact mapping, (one-to-one) is not possible, a default mapping strategy shall be defined.

EXAMPLE The attribute is left empty, or if values are taken in a taxonomy – the attribute value will be the closest hypernym of both values.

For additional information see Annex C.

All the above elements are organized as described in the Figure 2. Furthermore, Annex F shows examples of existing common information spaces and their elements (see Figure F.1).

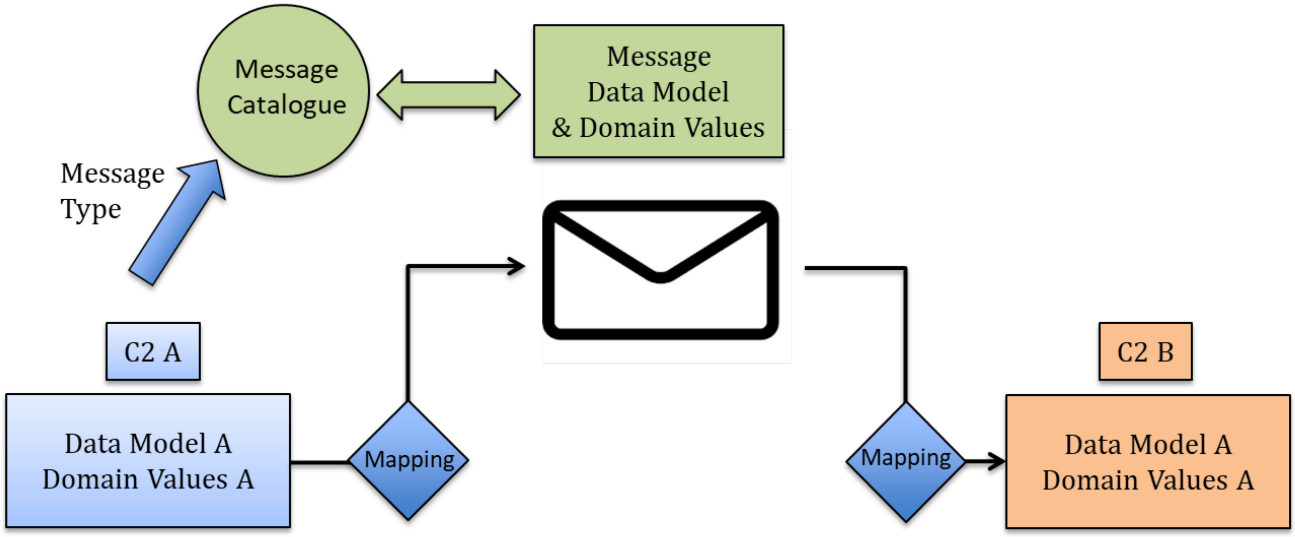

Figure 2 — Message-based interoperability

5.5 Requirements for semantic services

An initial step for the establishment of a semantic service is the definition of a universe of discourse where the semantic service is intended to be applied. In the context of this document the universe of discourse is limited to a domain or subdomain within the field of crisis and disaster management, e.g. management of natural disasters such as floods or wildfires.

Semantic services are necessary to ensure semantic interoperability. Semantic interoperability on this level means that identical interpretation of information exchanged between systems is supported.

The semantic services defined in this document facilitate the direct correspondence of elements expressed in different natural languages (e.g. English and German), which have the same or a similar meaning.

The language considered in this document is free text, containing some remarkable key terms, specific to the universe of discourse.

In order to ensure semantic services, semantic structures need to be provided.

These semantic structures are composed of the below elements.

— Common terminology: A terminology is a list of important terms (e.g. crisis, response phase, first responder). Unless an important effort has been done in harmonizing the various terminologies, various organizations have various terminologies. The variations usually come from languages, domain of expertise, or simply from history.

REQ 14: A common terminology including a harmonized set of terms and definitions shall be defined. This common terminology shall be organized as a vocabulary or as a taxonomy.

— The semantic mapping and matching operation: When a message contains free text paragraph, terms that are part of the common terminology can be mapped in the "System Preparation Phase", because in this phase the organizations have typically enough time to prepare their systems. Automatic matching takes place in the "System Application Phase" (or any other phase after having finished the mapping process) avoiding any additional effort of the actors in this critical phase.

REQ 15: A semantic mapping and matching service shall be provided (see Figure 3). For each term or expression found in a free text section of the received message, this service makes available the closest corresponding term or expression in the semantic domain of the recipient.

REQ 16: When exact correspondence cannot be found during the mapping process, an approximation strategy shall be found. For example, if the central terminology is a taxonomy, the closest related, more generic term shall be used.

— Symbology: In the world of civil protection, information is often represented on a map. The display of entities on map requires a specific symbology, which describes how each class of entity should be represented. The symbology specifies how entities should be represented with icons, and geometric features. This aspect is not addressed by this CWA.

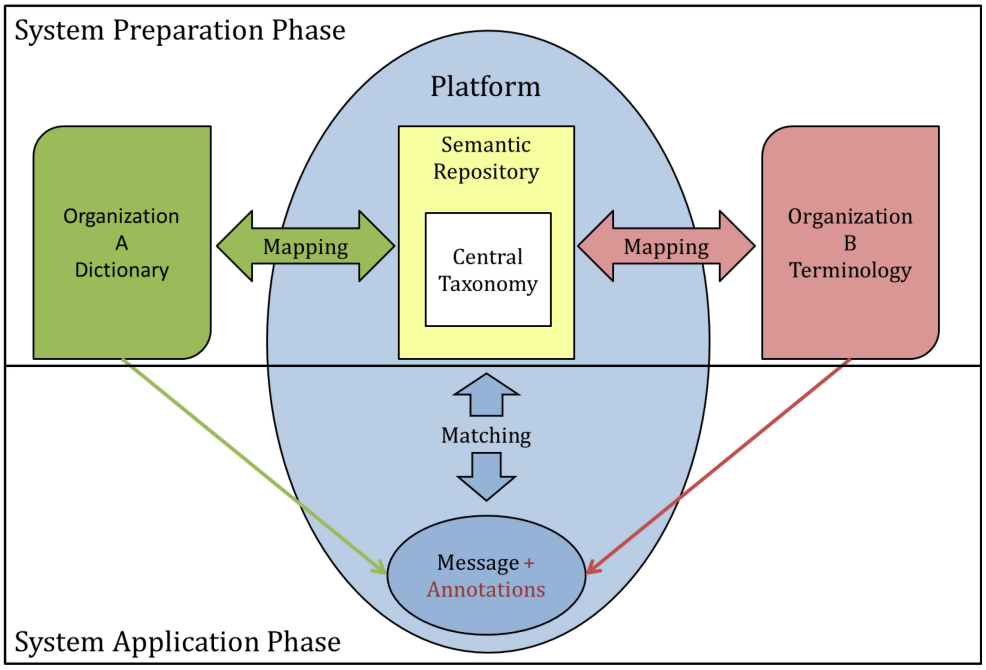

Figure 3 — Example of a scheme of realization of a semantic service

In the *System Preparation Phase* the central terminology is established (e.g. central taxonomy). The terminologies from involved organizations (A and B in Figure 3) are mapped to a central terminology, i.e. semantic relations between the terms of the different terminologies are identified (e.g. exact match, closer match or no match).

In the *System Application Phase* messages are transferred and terms from the central terminology are annotated. Annotation means that the definition of the closest term from the terminology of the

receiver together with the type of matching is given. The semantic repository can be established as a database containing the central taxonomy.

For additional information see Annex D.

5.6 Guide on how to reach interoperability – technical perspective

Organizations shall put in place the below elements to improve their interoperability on semantic and syntactic level.

Syntactic interoperability

1) Identify a group of organizations that intend to be syntactically interoperable with each other.

2) Agree with this group on one or more standardized protocols (e.g. EDXL, CAP) dedicated to support the information exchange during their operations.

3) Adopt an application programming interface (API) to interface the systems of the participating organizations.

4) Develop the ability to receive messages in at least one of the existing information systems. This consists of the following:

    i) Develop connectors to the syntactic layer, specifically on the protocol level (see REQ 8).

    ii) Develop the mapping procedure which enables to transform the data of their own system in the data model required for each of the transmitted messages.

    iii) Develop the mapping procedure which enables to transform the data of the messages they receive into the data model and format of their own information system.

    iv) Test these elements.

Semantic interoperability

1) Identify a group of organizations that would like to be semantically interoperable.

2) Establish with this group a common terminology.

3) Define a process including a semantic mapping sub-process for the preparatory phase and semantic matching sub-process for the operational phase.

4) Test the process and improve both the terminology as well as the mapping process iteratively.

Annex A
(informative)

Operational context

A.1 Audience and key stakeholders

This Annex focuses on the stakeholders and the audience of CWA 17513. It should be understood who is involved in terms of the context of use, the information exchanged and the tool development.

The syntax of UML use case modeling is used, providing a diagrammatic representation of actors and their roles involved in crisis management and response; those involved in defining and executing operations and related procedures. Procedures considered include those related to the use of tools that have to support information exchange requiring semantic and syntactic interoperability. The development and procurement of those tools is also considered.

For the reader to understand this use case model without prior knowledge of UML, it is important to understand the syntax used (see Figure A.1). In simple terms, actors are identified together with the actions that they carry out. Actions may include, or be dependent on, other actions. Generalization helps to define commonality between actors. UML provides a more comprehensive syntax, but these are the only elements used in the following figures.

It has to be noted that UML use cases do not illustrate events, sequences of events or any temporal activity. No specific scenario is described here.

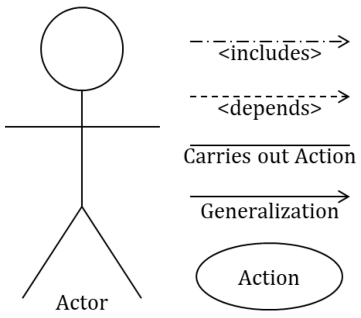

Figure A.1 — Legend

a) Context of use

Practitioners are the focus of the context of Figure A.2. The actor "Practitioner" represents the common interests of semantic and syntactic interoperability. The actor "Practitioner" is a generalization of both role and discipline. "Police", "Fire", and "Medical" response "Practitioner" actors may also carry the roles of "Crisis Managers" and/or "Responders". "Practitioners" may be involved in regular preparation, response and recovery actions. Many more disciplines can be included here.

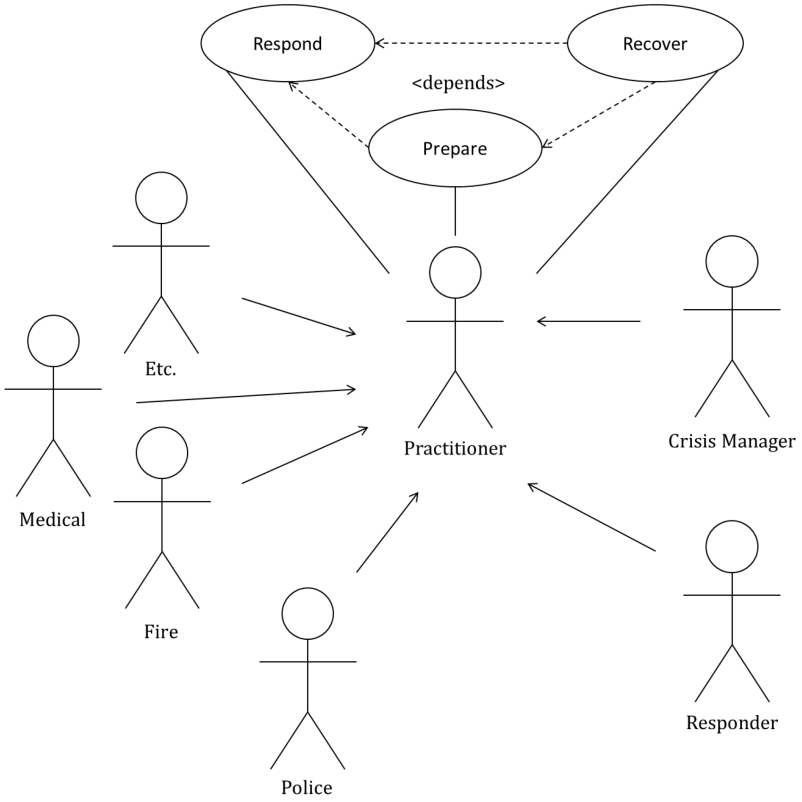

Figure A.2 — UML use case analysis identifying actors and their roles (context of use)

b) Information exchange

The following two roles of practitioners are considered: "Crisis Manager" and "Responder".

The "Crisis Manager" is involved in the process of procuring, and configuring the solutions that have to be semantically and syntactically interoperable. Both "Crisis Manager" and "Responder" will also use the solutions that have to be semantically and syntactically interoperable (see Figure A.3).

Operational policy and procedures are defined by the "Crisis Manager" and used by both "Crisis Manager" and "Responders". In the process of procurement, the "Crisis Manager" may trial different solutions and decides the interoperable syntax and semantic mapping method, often in collaboration with one or more software developers or equipment vendors.

During the actions of "Preparation", "Response" and "Recovery", "Practitioners" will follow the defined operational policy and use technical solutions to "Handle information". "Handling information" includes the actions of "Create", "Send", "Receive", and "Use" within the defined operational policy and processes. "Send" and "Receive" depend on the chosen syntax or its translation. "Use" is highly dependent on the method chosen to achieve semantic interoperability, and any configured semantic mappings used in any translation.

Semantic mappings should be derived from languages actually used, both considering social language and operational language. Social language, the regular day-to-day discussion, differs in different countries and is often varied within a country due to regional dialects and accents. Operational language often differs between responder sectors. Operational language also differs within sectors that are governed in different countries, and even different regions of some countries.

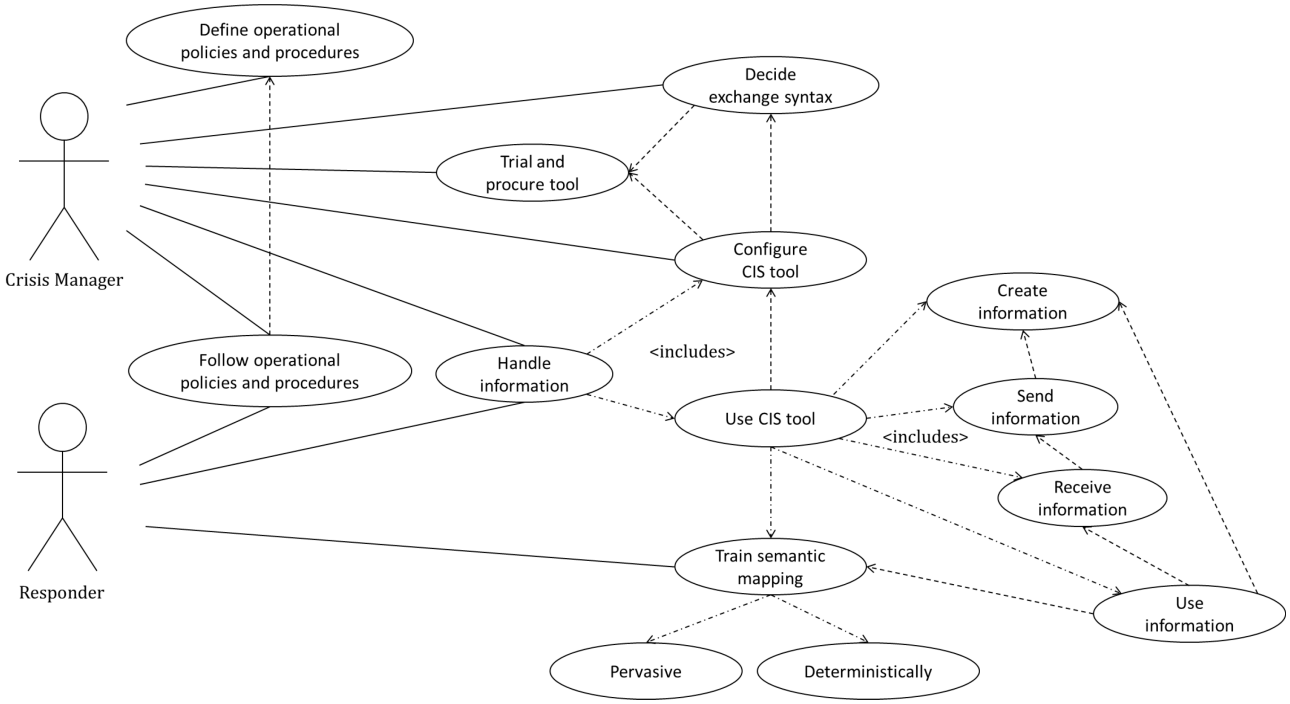

Figure A.3 — UML use case analysis identifying actors and their roles (information exchange)

c) Tool development

As described above, both "Crisis Managers" and "Practitioners" should be involved in the co-creation process to find a solution for semantic and syntactic interoperability (see Figure A.4).

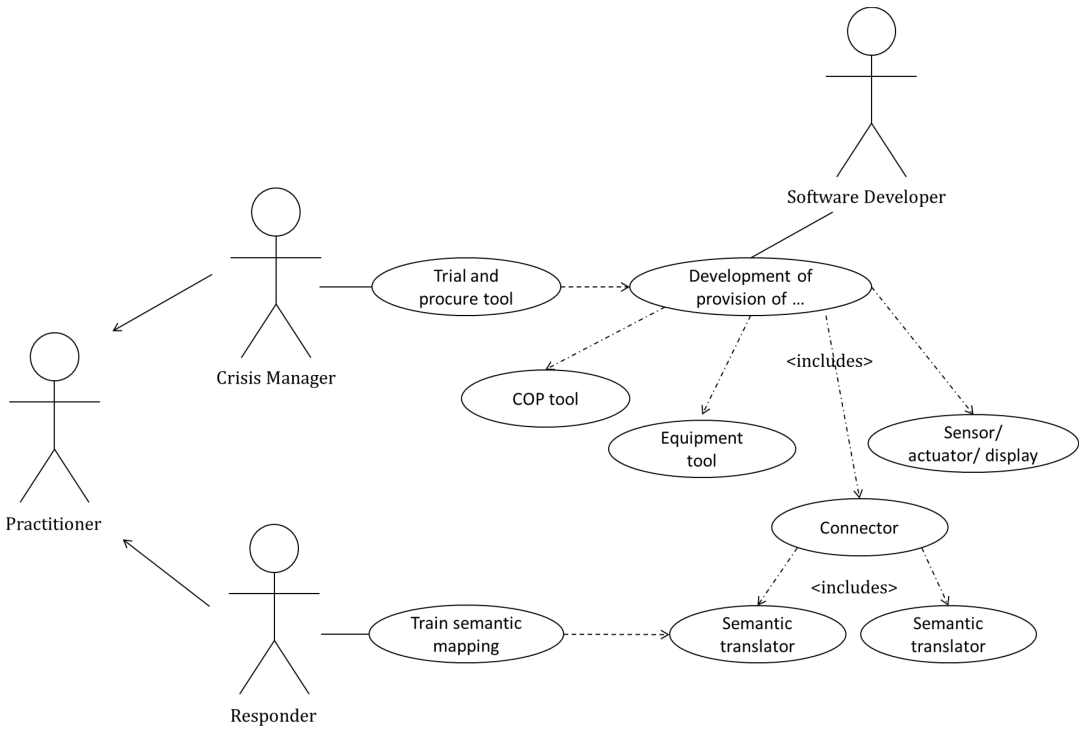

Figure A.4 — UML use case analysis identifying actors and their roles (tool development)

A.2 Layer models

Interoperability is multi-dimensional; it can be technical, organizational, or legal.

— Technical dimension: The amount of available and shared information can have adverse effects in terms of efficiency. As systems are not interoperable, there is a preference for verbal communication, and outdated technologies. New systems to be developed should enable information exchange with legacy systems (as not all of them will be replaced in the near future).

— Organizational and legal dimension: Aspects revolve around the mandate and willingness to share such information between levels of government or agencies ("need to know" policies) remain low, with confidentiality issues laid down as a limiting factor. The relevant information to be shared should to be defined, and training is an absolute necessity to support interoperability.

In the frame of this CWA, only the technical dimension is considered.

Several models exist describing the different levels (or layers) of interoperability. Prominent examples are the interoperability frameworks of the *NATO Science and Technology Organization* (see Section 5.1) and the *ESENet Layers of Interoperability Definition* [3]. The alternative approach from ESENet is visualized in Figure A.5. The four lower layers of ESENet are dedicated to ensuring technical interoperability.

The layer of "Physical Interoperability" deals with the availability of some channel to exchange data and is not part of the focus of this CWA. "Protocol Interoperability" and "Data/Objective Model Interoperability" correspond to syntactic interoperability and cover aspects such as the supported information exchange protocols as well as the use of standardized data elements and the availability of self-explaining metadata. "Information Interoperability" focuses on questions such as mapping of procedures and models to represent each other and corresponds also to the semantic layer of the NATO model. The higher layers "Knowledge/Awareness", "Aligned Procedures", "Aligned Operations", "Harmonized Strategies/Doctrines" and "Political Objectives" describe organizational interoperability and do not belong to the scope of this CWA.

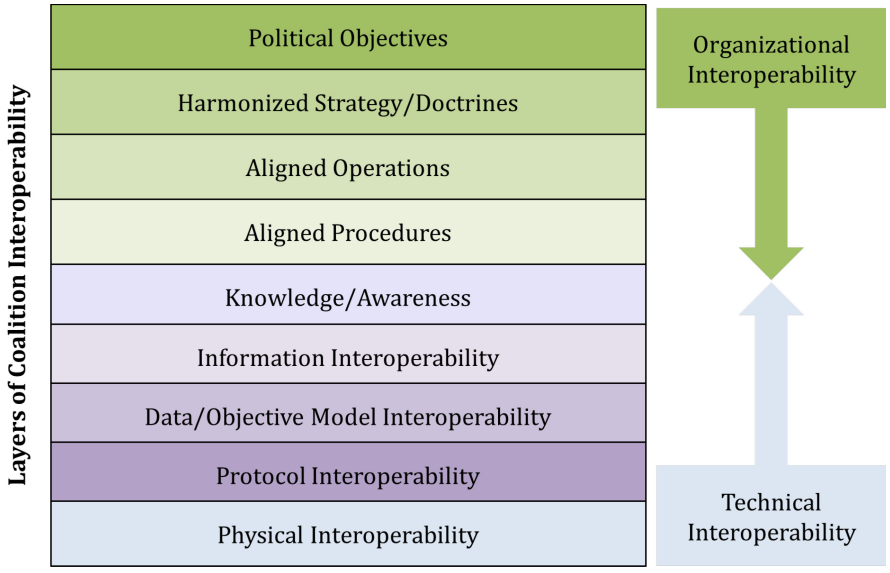

Figure A.5 — ESENet layers of interoperability [3]

A.3 Central idea of a common platform

A major challenge in sharing information between different IT tools used by organizations involved in managing disasters or large scale emergencies is that each organization uses typically a different IT tool that has different interfaces. Direct information exchange between different IT tools is often not feasible. An approach to overcome the problem is to interface each of the solutions with each other solution without the establishment of a common platform. This leads to a large number of requested software interfaces being proportional to the square of the number of interfaced solutions (see Figure A.6).

To overcome this challenge and to omit that all organizations have to buy and learn on how to apply a new common tool enabling them to interact, the concept of a platform called the common information space (CIS) was developed [3][8]. The common information space is set up in a way that organizations intending to be connected to each other do not need to replace their tools, but only provide an interface called adaptor for interconnecting their applied tools to the IT tools of partner organizations via the common information space.

This concept reduces the number of interfaces between the tools considerably. Instead of developing an interface for each new tool, an adaptor needs only to be provided once for each IT tool. This means in case of seven interfaced tools to develop seven adaptors instead of 42 interfaces by interconnecting the seven tools in a bi-lateral way.

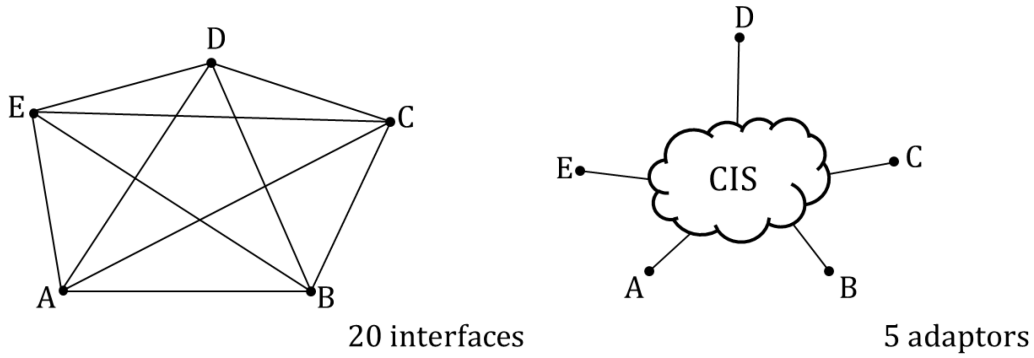

Figure A.6 — Reduction of number of interfaces by application of a common platform

Annex B
(informative)

Topology

This Annex provides additional topologies to the message-based topology shown in Section 5.3, which can be used to implement semantic and syntactic interoperability.

In the context of this CWA topology is defined as the various ways the main elements enabling syntactic and semantic interoperability can be organized. Annex B.1 and B.2 present two alternative topologies dedicated to realize specific types of interoperability:

— replicated database topology; and

— common application topology.

B.1 Replicated database topology

In the replicated database topology (see Figure B.1), each interoperating partner has its own command and control communication system (C2), and a version of a common database, following the reference data model, which is updated by interoperating partners according to mutually agreed procedures. An example of this topology is given by the NATO Multilateral Interoperability Protocol.

In this topology, the common database is replicated. Every change made to the data base is replicated in the other partner's database by a synchronization mechanism. Each interoperating partner has a local version of this database. The local instance of the common database needs to follow the reference data model. Each organization has its own command and control communication system, with its own data model. The mapping happens between the C2 A data model and the reference data model of the common data base. The replication/synchronization mechanism needs to be shared between and implemented by all interoperating partners.

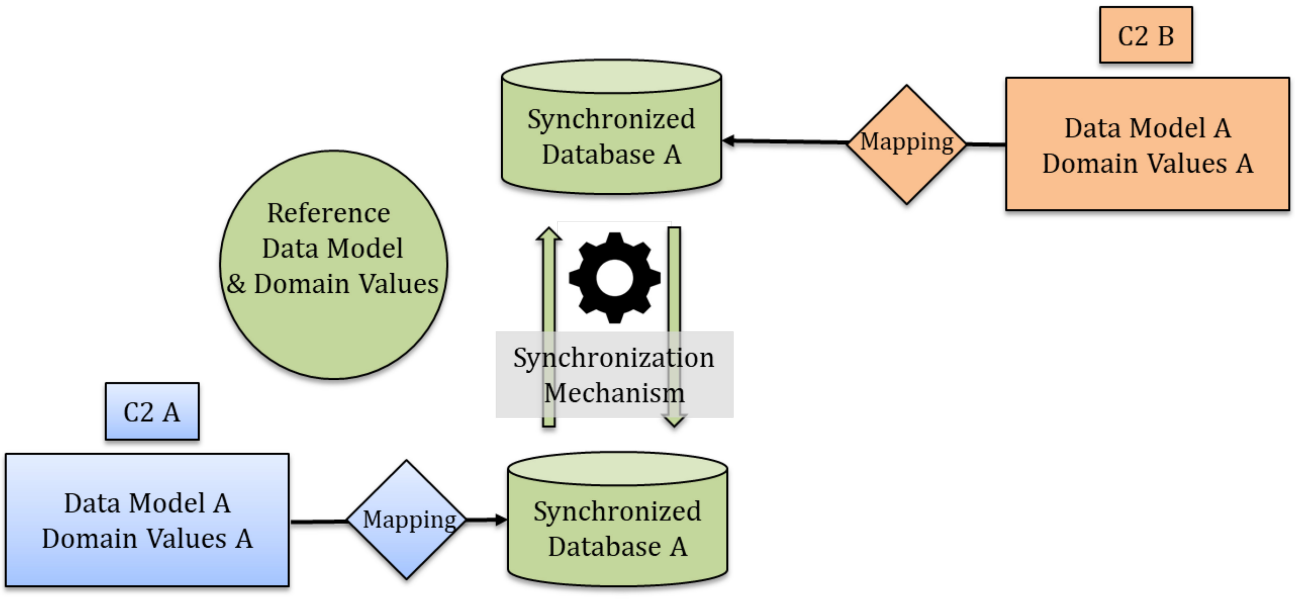

Figure B.1 — Replicated data base topology

Advantage

All interoperating parties are enabled to share exactly the same database and all interoperating parties are in the position to have a completed share of the common operational picture, as long as all relevant information is provided by all partners.

Disadvantage

The realization is hampered because all parties need to agree on a reference data model, and domain values, which can be a long process, even if this reference model can start small. Furthermore, the synchronization of all common databases is demanding in terms of the network bandwidth.

B.2 Common application topology

In the common application topology (see Figure B.2), all interoperating organizations are updating the same single web-based command and control communication system application, which is based on a reference data model.

The updating of the common application by each interoperation can be made fully manually by an information manager. It can also be more or less automatized, following a select and map process similar to the one used in the replicated data base topology.

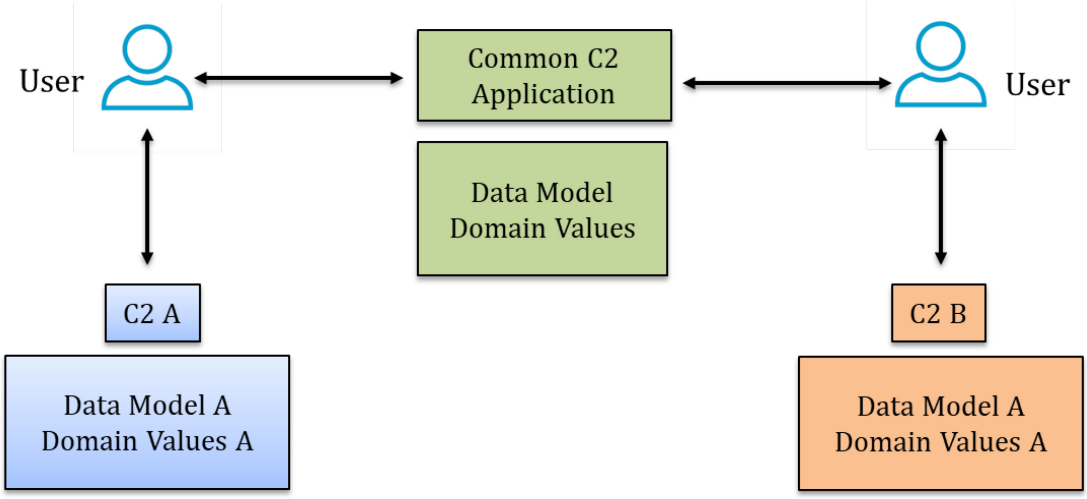

Figure B.2 — Common application topology

Advantage

The common application topology is from a technical point of view easy to implement.

Disadvantage

The topology requires interoperating partners to agree on the usage of the common application.

B.3 Specific aspects of the civil protection environment

Considering that the world of civil protection is heterogeneous, that there are many interoperating partners and little standardization is currently available regarding the data model, it seems difficult for the considered partners to either agree on a reference data model as in replicated database topology, or adopt a common application as in the common application topology.

Annex C
(informative)

Syntactic technical context

The central asset of a platform ensuring syntactic interoperability is that proprietary data formats of a solution connected to the platform are transformed to messages using established standards and protocols that can be received by the interfaces of any other solution connected to the platform. Syntactic interoperability ensures exchange of data in a way that allows automatic processing by another solution. This can be realized by data exchange standards such as EDXL or CAP.

C.1 Connector specifications

The use of standards is imperative to achieve interoperability in crisis and disaster management systems (see also Section 5.4). The main factors preventing interoperability between tools currently used by organizations in the crisis and disaster management domain are the following:

— Tools are often closed, with missing software interfaces for communicating with external systems.

— Tools are often used internally with proprietary data formats, therefore preventing an easy extraction and interpretation of the generated information, by other systems such as common platforms.

The implementation of a application programming interface (API) enabling the use of technologies such as web-services and REST, is necessary to address the need of interconnecting different, legacy or new systems and, therefore the basis of a service-oriented architecture.

The main functionality of a connector is to act as a gateway by providing a connection between a platform and a tool to be connected to the platform. That way, it drives communication to external channels. A central feature of the connector is to convert the tools protocol to the platform standard. An additional feature can be the filtering and validation of messages.

The connector's purpose is to manage the communication at the side of the tool. Typically, the connector needs to be assembled and configured by the tool owner or the manufacturer of the tool in order to transfer proprietary data model of a specific IT tool to the standard data model of the platform (e.g. CAP). For this purpose, a template may be set up, encompassing the below functions.

— Network connector module receives/sends messages from/to the tool according to the used network protocol. Templates for REST, SOAP and RSS connections need to be prepared. The tool owner has to maintain network configuration tables with the addresses of the tool services to be connected.

— Data format converter transfers proprietary data formats of the message to/from the standard messages exchanged in the platform.

— Standard convertor replaces proprietary key values and enumerations by standardized ones and vice versa, based on conversion tables to be provided by the tool owner. This applies only for code value sets mandatorily listed in the standard definition (e.g. CAP status, msgType, category) in order to form a correct standard message.

— EDXL DE generator (or an alternative generator) assembles the parameters for the EDXL distribution element that envelops all messages distributed in a platform. The template has to provide a minimum set of default values that might be extended. For example, security related parameters can be added depending on the message content.

— Filtering of received messages based on EDXL DE parameters. Filters might be extended also based on the message content.

C.2 Data format converter to standardized protocols/data models

The selection of standardized protocols depends on the area of application. The interoperability between different tools has to be based on a common reference data model. Messages will mostly be composed of a message header containing metadata like routing information and the actual message content. For the message content, there are several standards available which specify data models for various use cases. The table below shows examples of standards for some of the use cases in the crisis and disaster management domain.

Table C.1 — Standards to realize interoperability on the syntactic layer

Area of application	Standards (data models)	Information on context
Emergency Management	NATO Multilateral Interoperability Protocol Information Model	Interoperability between military C2 systems
	Emergency management – Message structure for exchange of information (EMSI)	ISO/TR 22351:2015
	Emergency Data Exchange Language Situation Reporting (EDXL-SitRep)	OASIS standards
Alerting	Common Alerting Protocol (CAP)	OASIS standard; national profiles available (e.g. Australia, Canada, Germany, Italy, United States)
Dispatch Center Information	Dispatch Center Interface (DCI)	German/Austrian local standard for exchange of emergency incident data between local emergency management agencies (developed by an EU funded project)
	NG9-1-1 Emergency Incident Data Document (EIDD)	American standard by ANSI (American National Standards Institute)

Hospital Availability Exchange	Emergency Data Exchange Language (EDXL) Hospital Availability Exchange (HAVE)	OASIS standards
Resource Information	Emergency Data Exchange Language Resource Messaging (EDXL-RM)	OASIS standards
Tracking of Emergency Patients	Emergency Data Exchange Language (EDXL) Tracking of Emergency Patients (TEP)	OASIS standards

Converting of the proprietary data formats of the different tools into a reference data model is an approach for interoperability, but it should be decided depending on the use case which standard data format is the most applicable.

A standardized format for the message distribution envelope is defined by OASIS standard Emergency Data Exchange Language (EDXL) Distribution Element (DE), which specifies the metadata for message routing and contains the actual message in element "contentObject", which can be XML or non XML content.

C.3 Message validation

In a message-based topology, a central communication infrastructure has to be established to transfer messages between different tools. Due to the composition of messages of a header and content, validation covers therefore the validation of the message envelope and the validation of the message content. Validation of the message envelope has to be provided by the communication infrastructure as soon as a message arrives. Metadata like information about the message's sender, the desired receivers, and any data necessary for a reliable dispatch of the message to the addressees have to be correct and consistent.

The validation of the message content can be executed at the client side when the message has been mapped to the reference data model or at the edge of the communication system after or as part of validation of the message envelope (see Figure C.1). In principle, it is not necessary for the communication infrastructure to be aware of the syntax and semantics of the message content. This is part of the converting functions placed at the client tools' side. But there may be reasons like the need for central control or for efficiency where it will be better to perform the complete message validation in the communication system. For this, information about the format of the message content can be given to the communication system either as part of the message envelope or as a fixed setting if the interoperability system is assigned to a single message format.

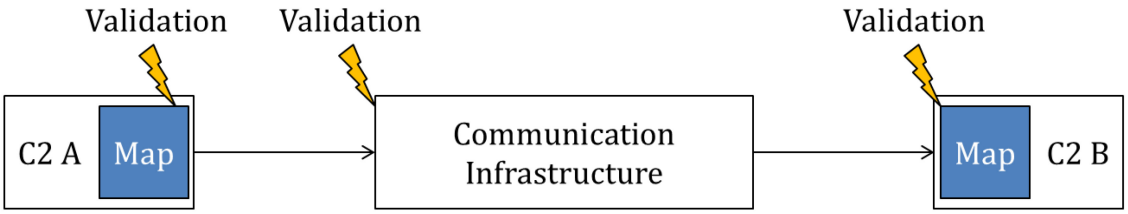

Figure C.1 — Message validation

The syntax validation of any messages can be based on technologies like XML or JSON which provide validation against a predefined schema definition. Semantic validation of messages is more complex, especially if the message format contains free text values. Some standards try therefore to avoid free text as far as possible. In the civil emergency management context, EMSI provides – besides the data model – an open codes dictionary which can be extended when needed and has to be used for the message items' values.

C.4 Security features

Message exchange in emergency situations can contain sensitive or personal data, hence, information security and data protection have to be ensured. The involved data categories should be classified and protected with security measures. Access to information should be restricted to entities that require the information to fulfil their tasks (following the need-to-know principle). The system should be flexible enough to support regional (topological, geographical) data sharing. This provides control over the data and enables usage scenarios in countries with federated organization as well as in inter-country scenarios.

Confidential data should be encrypted, both, in transit and at rest. The communication between distributed tools can be secured using standard transport layer encryption mechanisms, such as HTTPS or VPN. Message content and metadata can further be protected, potentially supporting fine grained encryption of sensitive message content and properties. Secure creation and handling of encryption keys has to be considered and supported by additional devices (e.g. hardware security modules or tokens). Multi-factor authentication (MFA) should be considered when possible (in particular for high-privileged users such as administrators).

Access control mechanisms should restrict access to all functions in the crisis and disaster management system. Revoking access rights when they are no longer needed is another important principle.

While availability is the main requirement in emergency situations, message integrity, as well as confidentiality has to be protected. Manipulated or spoofed messages can interfere or delay disaster response and coordination (e.g. false rejection of an authorized user or blocked communications due to a failure of the public key infrastructure (PKI)). Hence, security measures, their reliability and potential consequences in emergency situations should be carefully analyzed beforehand. Security measures should not restrict availability in the event of an emergency, crisis or disaster [4].

The following set of security properties can be considered:

— Compliance: Relevant laws and regulations (e.g. GDPR)

— Confidentiality: Encryption, authentication, authorization

— Integrity: Input validation, canonicalization, digital certificates

— Availability: Replication, parallelization, backups, recovery

— Non-repudiation: Logging and monitoring (e.g. utilizing a corresponding security information and event management)

— Multi-layer security (defense in depth): Intrusion detection/prevention, security information, event management

When developing software systems, various security practices should be considered:

- Protect source code
  - Protect source code from unauthorized access and tampering
  - Provide mechanisms for verifying software release integrity
  - Backups
- Secured software
  - Take security requirements into account during software design and review it
  - Encrypt confidential data both, in transit and at rest
  - Session management: Logout, time-based, non-predictable, etc.
  - Authentication and authorization (passwords should be protected (appropriate cryptographic functions), brute-force protection, policies, least privileges, etc.)
  - Verify third-party software components (scan for vulnerabilities, review, update, etc.)
  - Cryptography: Reuse well-established libraries and algorithms, keys have to follow current recommendations including high entropy and randomness
  - User input: Validate input, limits, memory management, encoding
  - Avoid unsafe functions and calls
  - Error handling
  - Logging and monitoring
  - Conduct code reviews (manual and automated)
  - Test executable code to identify vulnerabilities (vulnerability testing, fuzz testing, penetration testing, etc.)
  - Secure configurations: Security hardening, disable unnecessary features, test configurations, access control, secure defaults

C.5 Distribution services

The distribution services provide addressing and routing mechanisms that cover the most essential crisis and disaster management needs. The following two communication scenarios are to be supported.

1) Group-based or tag-based communication: Closed or open groups allow the exchange of information around a common or agreed on topic. Groups may be hierarchically (groups) or dynamically organized (topic tags; open participation).

2) Direct addressing with a logical addressing scheme (e.g. OID-based addressing scheme) allowing one-to-one and one-to-many messages outside of groups (e.g. for regular exchanges between neighboring districts or ad-hoc messages without group).

C.6 Resilience

Crisis and disaster management solutions are also being used in situations where infrastructure or organizations may be severely affected. Interoperability solutions take a critical role in the information flow between organizations and their systems, thus a resilient architecture is of high importance. A resilient architecture may be realized by a network of multiple common information spaces.

A resilient interoperability architecture should have the following architectural qualities.

— Geo-distribution: Data and functionality is geo-distributed, such that limited dependence on a single location exists.

— Data replication: Data such as critical information exchanged in one common information space or technical data that is required for exchanging information (e.g. addresses, topologies, access rights) is replicated at critical points (e.g. in a functional node or in a database) within this common information space or adjacent common information space, such that the loss of a single infrastructure component cannot interrupt the information flow.

— Partitioning: Whenever the network connectivity or system reachability is severely affected, the interoperability system can communicate in network or system partitions, such that regional (topological or geographical) communication is still possible in a failover mode.

— Separation of control: In continuation to the partitioning, the control over regional (topological or geographical) communications can be regionally organized such that under severe conditions functionality, control and organization can be maintained at least on a regional level.

— Resilience via distribution: This approach offers more than one point of entry to the system, as well as a redundant distribution of the core system. This proposed solution would catch any failures of a given entry point, as well as any failure of any given core.

Annex D
(informative)

Semantic service technical context

D.1 Resources for semantic interoperability

Resources for semantic interoperability can be structured in different categories:

— standardized (e.g. CEN, ISO);

— de-facto (industrial) standardized; and

— non-standardized.

Examples of different types of terminologies requested to ensure semantic interoperability are:

— dictionaries;

— vocabularies;

— taxonomies; and

— ontologies.

Within this document we focus on hierarchical taxonomies providing classifications from general to specific elements. Other types of taxonomies are faceted (multidimensional classifications) or can be combinations of hierarchies and facets.

A hierarchical taxonomy is composed of a certain number of concepts representing specific objects or set of objects. Each concept has a label, typically a term ("term" is a synonym for "name"). Between the different concepts, generic/specific (i.e. "is-a") relationships exist. For instance, a wildfire is subsumed by natural disaster or police man by first responders. It is important that the different concepts of a taxonomy on the same hierarchical level are independent from each other. This means that these concepts represent groups of objects that have no common elements.

D.2 Building the resources

In order to build a semantic resource (in the context of this document a taxonomy covering a specified universe of discourse in the domain crisis and disaster management), there are several options.

1) The use of existing resources for semantic interoperability or documents, such as an international standard (e.g. ISO 22300:2018).

2) The combined use of existing resources for semantic interoperability or documents, such as the vocabulary from the United Nations Office for Disaster Risk Reduction (UNSDR) and ISO 22300: 2018.

3) The combination of concepts from existing standards (similar to approach two, but excluding concepts not relevant for the specific universe of discourse).

4) Development of a taxonomy by identifying the relevant concepts for the universe of discourse of interest, labelling all concepts (provision of terms) and description of objects/set of objects (provision of definitions).

5) A combination of approach three and four.

EXAMPLE The fifth approach was applied in the DRIVER+ project. A specific project terminology was developed to ensure harmonized understanding in the frame of the project executions. The project coordination team identified key terms and a specific terminological task force checked available definitions in existing resources for semantic interoperability or documents. In case no suitable definitions were identified in available resources, the project team established their own definitions.

A selection of established terminologies applied in the domain of crisis and disaster management can be found in CWA 17335:2018 *Terminologies in crisis and disaster management*.

D.3 Specific aspects of the civil protection environment

Any semantic structure such as taxonomy applied in the domain of civil protection can fulfil several roles that can be summarized as follows:

— The semantic structure is the basis for interpretation and mutual understanding of information exchanged by practitioners and other stakeholders mainly, but not only in the disaster response phase.

— The semantic structure ensures situational awareness during the disaster response phase in an arranged and classified way.

— The semantic structure improves retrieval and mutual understanding of information by means of information exchange platforms such as a common simulation space.

It has to be taken into account that the vocabularies (or other semantic resources) applied nowadays in crisis and disaster management vary considerably according to the context of the involved organizations, as well as the cultural and national background and finally the specific subdomain of crisis and disaster management, e.g. infrastructure protection, CBRNE, or management of natural disasters. It seems not to be realistic to expect that (at least in the close future) all European or worldwide actors are going to agree to use a single, harmonized taxonomy.

It is therefore a suitable approach to allow all actors to continue to use their vocabularies, but to define context based central terminologies and to map the vocabularies of the different interacting actors.

D.4 Semantic mapping and matching

A possible approach to realize semantic interoperability is to provide a semantic web-service offering exchange of messages with semantically annotated terms among the organizations participating at an information exchange platform.

Semantic annotations are terms of concepts commonly used by participants who receive messages and they are semantically related to concepts' terms written by participants who send messages. The service is designed around two main processes:

— semantic mapping; and

— semantic matching.

A prerequisite for the service is that participants at an information exchange platform, prior to the service request, enter their concepts' definitions, terms and their semantic relations to a central terminology such as a taxonomy in a semantic repository. This process is called semantic mapping. On request, the service queries the semantic repository for semantically related concepts of the platform participants via their relations to the central terminology's concepts (semantic matching). The number of semantically annotated terms depends on how comprehensive the content of the semantic repository is.

One can distinguish between exact mapping, meaning that two concepts of different terminologies have exact the same meaning (the same definitions) as the according concept of the central system taxonomy. In case concepts from different vocabularies are related but not the same, typically they can be mapped to the closest concept on a higher level of the central terminology (e.g. "hydraulic pump" is subsumed by "pump"). In case of message exchange in the response phase of a disaster, semantically mapped terms can be matched. In case the correspond is one-to-one to each other and the central term of the central taxonomy, an exact match is provided. In case of non-exact mapping a broader match of terms is taking place. Figure D.1 illustrates the process of semantic annotation.

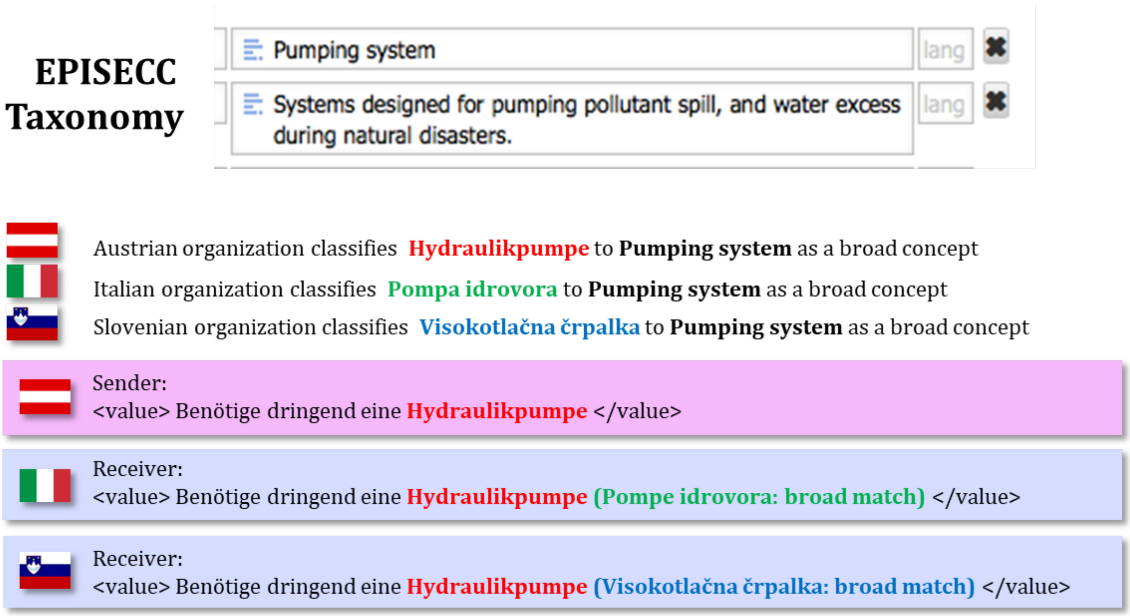

Figure D.1 — Process of semantic annotation

Annex E
(informative)

EPISECC use case for semantic services

An approach on how to realize semantic interoperability was demonstrated within the EPISECC research project in Palmanova, Italy. This Annex includes the description of this approach.

Semantic repository and queries

The *EPISECC Semantic Repository* hosted sets of concepts, predominantly organized as taxonomies, dictionaries, etc. The challenge of semantic annotation consists in associating the concepts of one set with their respective matches (corresponding concepts) in other sets.

For the EPISECC project, partners agreed to create a central taxonomy (named *EPISECC Taxonomy*) relying on concepts represented by terms in English language to bridge all sets of concepts together. Indeed, each term representing users' concepts are associated to the *EPISECC Taxonomy* through a mapping process. It allows the *EPISECC Semantic Repository* to provide the best available mapping concept on every request.

Implementation

To fill and access the *EPISECC Semantic Repository*, the project partners relied on two main tools: Protégé and Apache JENA.

— Protégé: In this free tool developed by Stanford University, concepts were added one by one and linked together (provided the existence of a predicate between them); afterward they were associated to the closest *EPISECC Taxonomy* concepts following the central taxonomy schema. This operation was done manually for the EPISECC demonstration.

  When the concepts are manually linked additional relations can still be generated automatically, thanks to the commutability and transitivity nature of the triples. For this purpose, EPISECC relied on Protégé's reasoner to search and create any inferred link between concepts. The created links were then added to the triple store storage solution – Apache JENA.

  The result were three sets of concepts combining more than 300 of the most recurrent concepts used for crisis and disaster communication between responders from Italy and Slovenia, as well as the *EPISECC Taxonomy* as the third set.

— Apache JENA: JENA is a free and open source framework used to link and build linked data applications and semantic web. It embeds a triple data store database (TDB) that can be queried from a REST-based SPARQL query server (Fuseki). In the frame of EPISECC, due to the micro-service architecture, the effort was organized around the SPARQL REST interface to build dynamic queries to retrieve most suitable data.

Semantic web-services

The semantic web-service was used for enabling semantic interoperability. In a typical interoperability scenario, it provides the application programming interface (API), used by the demanding software components to ask the runtime semantic matching (and related semantic annotations) between

concepts of senders and receivers of messages. Upon reception of a semantic matching request, the semantic web-services:

— select from the message received in input, the information that needs to be semantically annotated, and prepare a JSON structure with the same information inside. Such JSON structure represents the so-called S*emantic Annotation Request Object.*

— send the S*emantic Annotation Request Object* to the downstream component (the semantic service built using Apache Jena and the Fuseki SPARQL query server), in charge of building and executing the query to the underlying *EPISECC Semantic Repository*.

— receive back the original information together with the corresponding semantic annotations (a JSON structure which represents the so called *Semantic Annotation Response Object*), to enclose them in the original message, or to directly deliver them to the calling component (the common information space connector core on the receiver side, in case of realization of the EPISECC demonstrator).

The semantic web-service is implemented as a SOAP web-service.

For a proper and reliable functioning of the semantic interoperability between different organizations cooperating in disaster management, the *EPISECC Semantic Repository* was populated with the *EPISECC Taxonomy* concepts, as well as with proprietary (end users' organizations) taxonomies and schemas, and the mapping between proprietary concepts and EPISECC semantic concepts can be performed beforehand (see Figure E.1).

Figure E.1 shows the integration of the semantic web-service in a typical communication scenario, targeted at realizing both syntactic and semantic interoperability:

1) On the common information space core on the sender side, a message is prepared containing semantic concepts from organization A (sending organization).

2) The message is distributed by the organization A distributor to the distributor on the receivers' side (organizations B, C, etc.).

3) The message is then forwarded to the common information space core on the receiving side.

4) The common information space core receives the message and creates a semantic matching request for the semantic web-service, which is delivered using the provide SOAP interface.

5) The *Semantic Annotation Object Request* structure is created and delivered to the downstream component based on Apache Jena and Fuseki server.

6) The *Semantic Annotation Object Request* is provided back to the semantic web-service.

7) The original together with the annotated concepts are provided back to the calling common information space core component.

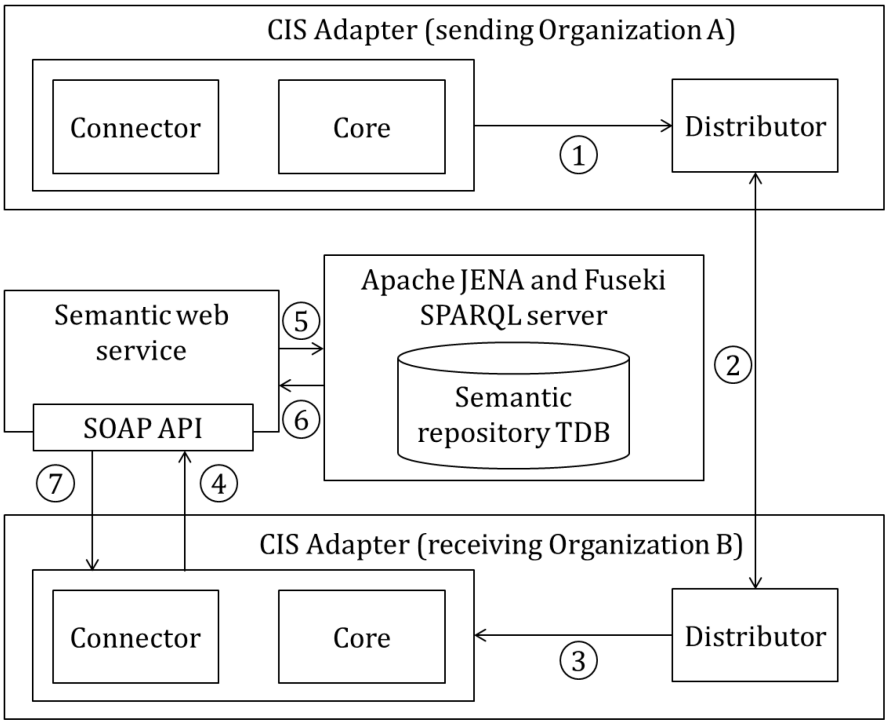

Figure E.1 — Semantic web-service and its integration in a typical communication scenario

Semantic mapping and matching

The semantic interoperability was validated through message exchange processes of two organizations coming from different countries: Mountain Rescue Slovenia and Fire Fighters Gorizia. The Protezione Civile Regione Autonoma Friuli Venezia Giulia (PCRFVG) which acts as LEMA (Local Emergency Management Agency) uses terms and concepts from *EPISECC Taxonomy*. Therefore, three different languages were represented in the CAP messages: Italian, Slovenian and English. Since the process of identifying concepts is time-consuming, a set of relevant concepts for each organization was selected. The selected concepts are closely related to the demonstration scenarios. Such an approach ensured that the exchanged messages have common concepts from both organizations and include semantic annotations.

The concepts were stored in the *EPISECC Semantic Repository*, together with *EPISECC Taxonomy* and are mapped to the *EPISECC Taxonomy*. The mapping procedure sets the relationships (properties) between end users' concepts and *EPISECC Taxonomy's* concepts. It resulted in all possible situations, like exact and broad situations and creation of several compound terms, which makes the validation close to the real situation.

The matching was performed using queries and resulted with semantic annotations. It happens when one organization, in the proof of concept case either the Italian Fire Brigade or the Slovenian Mountain Rescue or Civil Protection Authority, sends CAP messages. The semantic service sends a request for querying over the *EPISECC Semantic Repository* and finds the matching concepts in other organizations. The annotations were inserted in parts of the CAP messages where end users may enter free text. Matching retrieved the concepts' terms and inserted them into the message next to the original term. The process also added two different marks next to the receiver's concept: one if the concepts from both organizations were mapped as "exact" to the connecting concept in the *EPISECC Taxonomy*, and one if there is at least one concept mapped as broad.

Annex F
(informative)

Examples of existing implementations of CIS concepts

F.1 Introduction and elements of a CIS

In cross-border crisis and disaster management situations stakeholders use ad-hoc cooperation, even if this does not correspond to their daily routine. They have to be able to rely on a smooth communication. To archive smooth communication the common information space (CIS) concept uses software modules like the one's shown in Figure F.1. This Annex describes possible implementations by means of two examples: DRIVER+ and EPISECC.

The list of examples is not complete; there are more projects and implementations regarding a common information space. The examples here were chosen because they show good practices of how such a common information space supports the exchange of understandable information between agencies, as well as cross-border in a crisis situation.

Within a common information space, different processes are running (see Figure F.1). The focus is exclusively on cooperation. Therefore, processes such as a time service are not depicted.

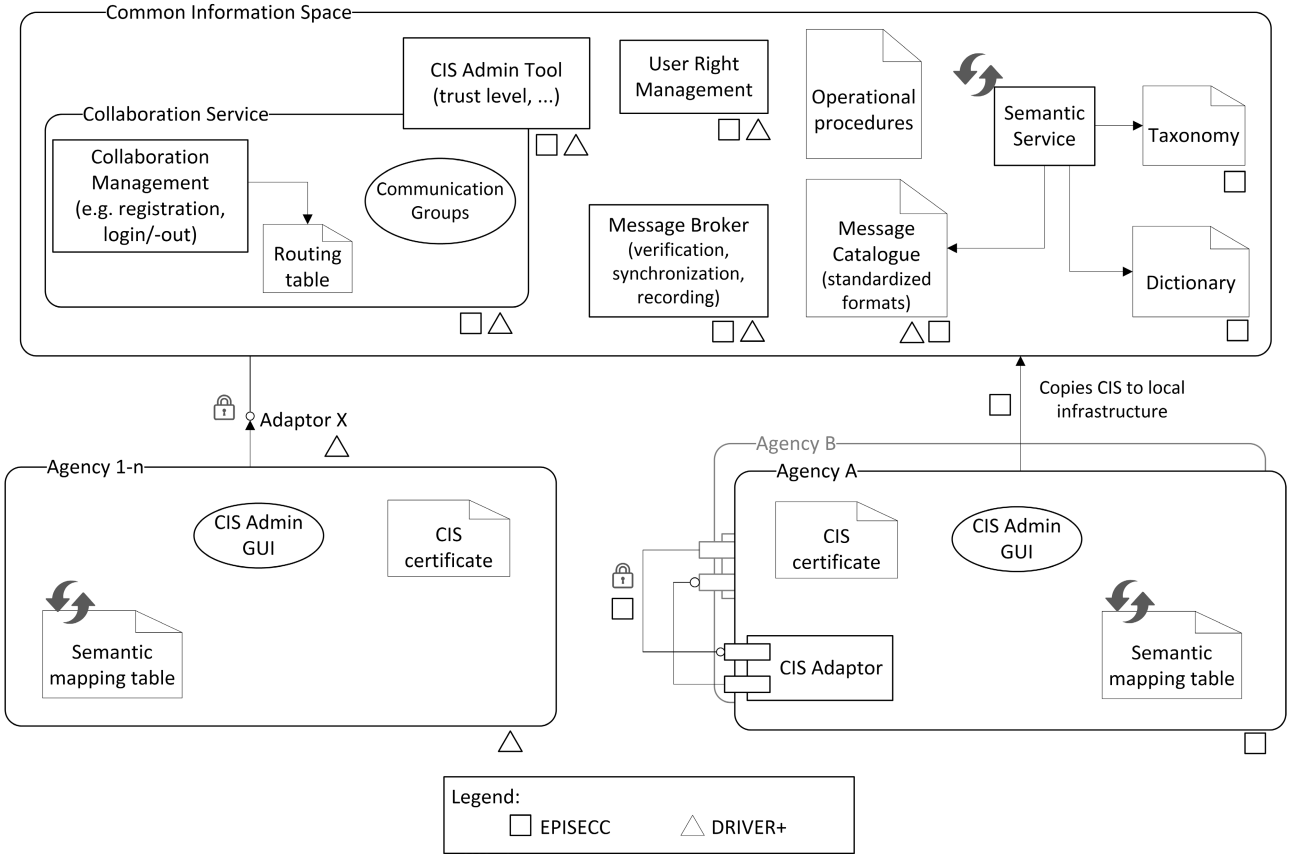

Figure F.1 — Overview of elements of a CIS supporting interoperability

The elements in Figure F.1 fulfil the following tasks:

— CIS Admin Tool: Controls the processes of the CIS. Can be configured via the CIS Admin GUI.

— CIS Admin GUI: Graphical user interface to configure the CIS. With this program, the connections of the CIS adaptor can be controlled, requests for access to external data can be made, and the current configuration can be shown.

— CIS certificate: Digital certificate needed to secure the connection to a centralized CIS or partner network.

— CIS Adaptor: Maps local to external formats and vice versa taking into account semantic services. Takes care of the connection to CIS. Figure F.1 shows two approaches how a connection can be implemented: 1) from one organization to the centralized CIS or 2) directly between two or more organizations. For data transfer the adaptor uses the specified exchange protocols (see Section 5.4). For local implementation a template is mostly provided. Each partner needs to implement only one adapter to connect to the common data format of the CIS.

— Message Broker: Evaluation of messages according to the syntax/formats, synchronizes messages between agencies e.g. if an agency connects later it will get the current information automatically, optional recording capabilities.

— Collaboration Service: Includes everything to enable collaboration between stakeholders, e.g. a user gets information about organizations that can connect or gets information about existing groups in which to communicate (see CGOR concept in next Section), and for CIS Adaptor network information are available to establish connections (routing table).

— Operational Procedures: Descriptions of work processes, preconditions, contact persons, etc. Allow mapping of work processes between different agencies.

— Semantic Service: Ensures semantic mapping and matching of vocabulary. Therefore, different databases are required e.g. a dictionary for different languages, the taxonomy for matching terms and the message catalogue including different (standardized) formats. Another element could be a symbology.

— Semantic mapping table: Global and local mapping tables coexist. The global table contains basic terms, supplemented by a local table to add and easily modify the mapping for tasks. Correct terms in a local mapping table should be migrated to the global database.

F.2 EPISECC and DRIVER+

EPISECC

Within the project EPISECC data and communication flows were analyzed to establish requirements for the common information space architecture. The EPISECC common information space prioritizes the distribution of software modules to the individual partner systems to avoid a single point of failure or a central attack point [3].

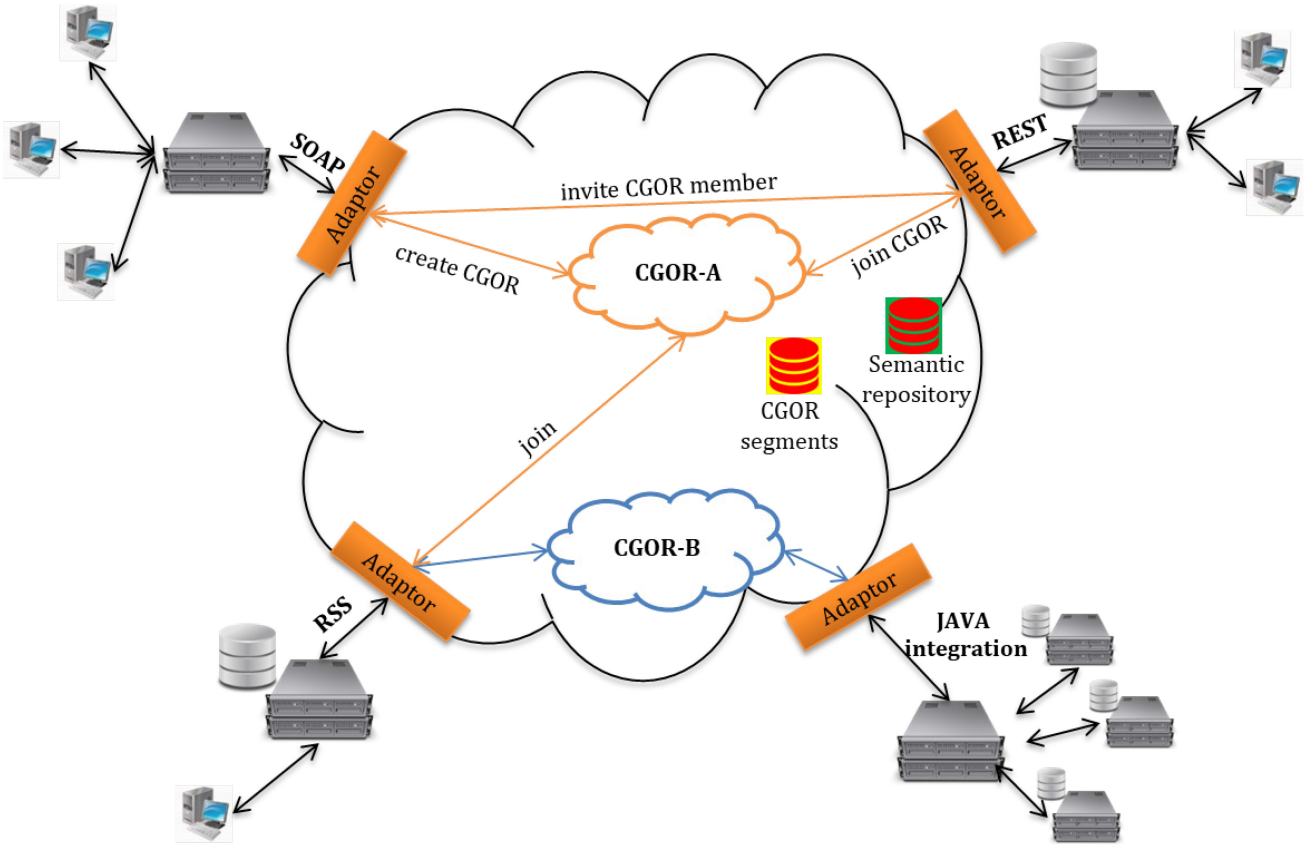

Figure F.2 — Overview of the EPISECC CIS

Standardized data formats are used internally. Therefore, the XML formats EDXL DE, CAP, EMSI and MLP (Mobile Location Protocol) are used. External or proprietary data formats are transferred to the internal formats using (CIS) adaptors. Templates of adaptors support partners in writing their own adapters. Messages are parsed for keywords defined in the *EPISECC Taxonomy*/data model (including closes meaning) to transfer between internal and external formats. The definition of the mapping from an external format to the internal format is defined by each partner and provided to the CIS [5]. Further, the data model includes details for receiving tools to interpret the information, to support semantic interoperability (see Annex D for more details). Besides the key value mapping a conceptual mapping from organization to/from EPISECC concept is generated and stored in the common information space (semantic matching). Both the original and standard key values are received by end users. According to [6] the implementation should follow the related OWASP cheat list.

Software modules are connected via a Secure Sockets Layer (SSL) VPN connection peer-to-peer (from partner-to-partner). Two ways to get an SSL certificate are described: First a public-key-infrastructure (PKI) and second authorized employees who are mutually able to authenticate each other. In a PKI a certificate is issued by a certificate authority. A tool owner or organization needs to request a certificate and register themselves. The PKI is a centralized service and certificates should be provided by a public trust center following the European directive 199/93/EC [7]. Beside the certificate for the connection, the functionality of an adaptor needs to be tested and certified too.

Information is exchanged using communication groups. These are configured via an admin tool by the end user. New groups can be added or a request to join an existing group can be sent. This dynamic and easy to use structure also ensures, that messages are only transferred to partners authorized and wanted to get the information. To realize this, the CGOR (cooperation group online room) concept has been implemented in EPISECC.

Cooperation group online room (CGOR): A CGOR is a dedicated channel to be used for communication between one and one or more organizations connected by adapters to the common information space. For global information exchange e.g. weather information, global CGORs are available by default, and every tool that is registered for participation in the common information space becomes automatically a member of the global CGOR. Specific CGORs can be created by an administrator of any common information space member. Intended participants are invited by the CGOR owner and have to confirm/reject the participation, meaning that any information sent to the CGOR is shared with all other members of the cooperation group. The tools sending information to the common information space have to classify the sent information in a way that the CIS adaptor is able to determine the appropriate CGOR in an unambiguous way. The underlying rules are implemented specifically for the common information space member/tool in the respective adaptor. Otherwise, only the global CGOR can be used for sending public information. Nevertheless, receiving information in a CGOR is always possible. Additionally, data wrapping and encryption ensures that the information is only accessible by CGOR members.

DRIVER+

DRIVER+ focused on the evaluation of new and possibly innovative solutions (programs). Implemented software and its documentation are open source and available on GitHub:

— https://github.com/DRIVER-EU; and

— https://driver-eu.github.io/test-bed-design/.

A database of taxonomy and a dictionary for providing semantic services are not part of DRIVER+ software. In DRIVER+ simulators are connected to a common simulation space and solutions to a common information space. Common simulation and common information space exchange messages via gateways that translate the different formatted messages back and forth. Together with an Admin Tool these three components build the communication unit of the DRIVER+ test-bed. The connection to this unit is secured using SSL/TLS and X.509 standard certificates. SSL client (adaptor) certificates are approved by a system administrator via the Admin Tool. Certificates are issued by a certificate authority. It is also possible to activate topic authorization by using these certificates (realizing communication groups).

Message sending, receiving and logging is based on Apache Kafka (message broker). The advantages of Kafka are that commercial organizations are already using it and Kafkas performance of sending messages is also high. DRIVER+ provides different templates of adaptors to connect to the test-bed in different programming languages (Java, C#, Python) and scripting language (TypeScript, JavaScript). One of two Java adaptors uses the programming paradigm REST. Messages are well structured by using Apache AVRO (a data serialization system). The data schema, syntax of a message, is defined in JSON. Used standard formats are e.g. CAP, EMSI, MLP (Mobile Location Protocol) and GeoJSON (see https://github.com/DRIVER-EU/avro-schemas). All available AVRO schemas are listed in the schema registry.

Group communication realized in DRIVER+: The CGOR concept from EPISECC was in a modified way implemented in the DRIVER+ common information space. Group communication channels (topics) are only permitted to be created by the admin-service. Adapters (organizations) that need a dedicated channel from communication have to send a creation request to the admin service with all necessary information (also the connected organizations need to be specified). The admin-service creates the topic and grants the access according the given information. After the successful creation, the adapters get the information that a topic was created, and they are permitted to connect for sending and receiving.

Annex G
(informative)

Guide on how to reach interoperability – practitioner perspective

The capability to support inter-agency information sharing can be based on appropriate procedures and context-based information-sharing schemes. The language barrier is notably problematic in daybook for automatic translation. There is a general tendency to use liaison officers between organizations to address this gap. The willingness to collaborate is a basic prerequisite (political considerations, confidentiality, competition, human behavior, lack of financing, etc.). The importance of the non-technical aspects of the gap (willingness to share information, organizational and procedural dimensions) ought to be underlined. This gap is all the more significant for large crisis and disasters at a regional to national level, less in the case of smaller crisis and disasters at a more local level.

Four guiding principles are given below:

1) Consider interoperability in all its dimensions (legal, organizational, procedural, semantic or technical).

2) Avoid undermining the importance of political will and cultural blockages.

3) Integrate all potentially concerned actors in the reflection process (not only first responders and law enforcement agencies, but also network operators for instance).

4) Importance of exercising with all concerned actors to confront the concept/system to practical difficulties and misunderstandings.

Bibliography

[1] Bacchelli, F., Boury-Brisset, A., Isenor, A., Kuehne, S., Martinez, R. B., Miles, J., & Wunder, M. (2010). Final Report of Task Group IST-075 Semantic Interoperability.

[2] Neubauer, G., Preinerstorfer, A., Schirnhofer, S., Humer, H., Lichtenegger, G., Vorraber, W., & Knezic, S. (2016). Validation of the Management of past Crisis and Disasters. IDIMT 2016–24th Interdisciplinary Information and Management Talks.

[3] Tolk, A. (2003). Beyond technical interoperability-introducing a reference model for measures of merit for coalition interoperability. Old Dominion Univ Norfolk VA.

[4] Dodson, D., Souppaya, M., & Scarfone, K. (2019). Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)(Draft) (pp. 23-23). National Institute of Standards and Technology.

[5] EPISECC. D4.3 (2016) – Data model.
Last retrieved: 26.03.2020. https://www.episecc.eu/results.

[6] EPISECC. D5.4 (2017) – Architecture of the Common Information Space.
Last retrieved: 26.03.2020. https://www.episecc.eu/results.

[7] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[8] Neubauer, G., Preinerstorfer, A., Lichtenegger, G., Humer, H., Linke, H., Zuba, G., & Dalaff, C. (2017, December). Common information space as enabler for collaboration in disaster management: demonstration of the validity of the EPISECC CIS concept. In 2017 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM) (pp. 1-8). IEEE.