Establish Pan-European Information Space to Enhance seCurity of Citizens

D5.4. – Architecture of the Common Information Space

Grant agreement number:	**607078**	**Date of deliverable:**	**2017-09-30**
Date of project start:	**2014-06-01**	**Date of submission:**	**2017-10-02**
Duration of project:	**41 months**	**Deliverable approved by:**	**G. Lichtenegger, AIT** **G. Tusa, IES**
Lead Beneficiary:	**FRQ**		
Contributing Beneficiaries:	**AIT, AIRBUS, DLR, HITEC, HWC**		

Executive Summary

This document *D5.4. – Architecture of the Common Information Space* is the sole public deliverable of EPISECC WP5. So, it summarizes the results of the tasks 5.1 *Protocol & network interoperability*, 5.2 *Information interoperability,* and 5.3 *Operational interoperability*. It describes the final architecture and technical concepts for secure automated information sharing of the EPISECC Common Information Space (CIS), which are based on lessons learned from regular discussions with practitioners and from the validation of the final proof of concepts (PoC).

Different types of information are exchanged between tools used by organisations involved in crisis and disaster management (responders, infrastructure providers, authorities, scientific institutes etc.).

The need for fast and reliable exchange of information between autonomous stakeholders which are not collaborating in their day-to-day business but must co-operate during disaster response can be derived from the results of WP2 (analysis of the crisis management approaches) and WP3 (Pan European Inventory of events/disasters). The taxonomy model developed in WP4 together with the terminologies used by CIS participants builds the basis for semantic transformations and annotations that help overcoming language barriers and incompatible encodings in different organisations and tools.

Resilience of Internet connectivity is a pre-condition for computer-based information exchange which is not further investigated within the EPISECC project. We rather focussed our research in Network Interoperability on the connectivity between TETRA networks and the IP based CIS, and the novel trends to define standards for utilisation of LTE networks and mobile devices for PPDR communication.

The basic idea of Information Interoperability in the CIS is to connect tools via adaptors. Proprietary data formats and interfaces of one tool are transformed to messages using established standards and protocols that can be received by the adaptors of any other CIS participant (syntactical interoperability). Information security is key in the CIS architecture; the information sharing follows the need-to-know principle. Cooperation Group Online Rooms (CGOR) are defined for partners collaborating in one event/incident, providing segmentation of all messages circulated in the CIS. Messages assigned to a CGOR are readable only for CGOR members.

Making messages of a foreign sender understandable for the receiving tools and human users is very important. Based on the EPISECC taxonomy, key terms of the messages are interpreted. The information consumer gets the original message together with semantic transformations and annotations reflecting his own terminology (semantic interoperability).

The Operational Interoperability comprises processes for the set-up of a CIS in the preparation phase, for accepting organisations as CIS members and assigning trust to them, and for creating CGORS during the disaster response.

Table of Content

List of Tables

List of Figures

List of Acronyms

Abbreviation	Description
ASSI	TETRA Associated Short Subscriber Identity
AVL	Automatic Vehicle Location
C^2 / C&C	Command and Control (system)
CAP	Common Alerting Protocol (OASIS standard)
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CGOR	Cooperation Group Online Room
CIS	Common Information Space
CM	Crisis Management
CPA	Civil Protection Authority
DA	Directory Agent
DS	Directory Services
EDXL	Emergency Data Exchange Language (family of OASIS standards)
EDXL DE	EDXL Distribution Element (message envelope)
EMSI	Emergency Management Shared Information (ISO/TR 22351:2015)
GIS	Geographic Information System
GUI	Graphical User Interface
ICT	Information and Communication Technology
ISO	International Organization for Standardization
ITSI	Individual TETRA Subscriber Identity
LIP	Location Information Protocol
LTE	Long-Term Evolution (4G mobile telecommunication)
MCC	Mobile Country Code
MLP	Mobile Location Protocol
MNC	Mobile Network Code

MS-ISDN	Mobile Station International ISDN number
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OMA	Open Mobile Alliance
PKI	Public Key Infrastructure
PoC	Proof of Concept
PPDR	Public Protection and Disaster Relief
REST	Representational State Transfer (Web service interface)
SA	Situational Awareness
SensorML	Sensor Model Language
SSI	TETRA Short Subscriber Identity
TETRA	Terrestrial Trunked Radio
W.I.	Wrapped Information
WP#	Work Package #
XML	Extensible Mark-up Language

Architecture of the Common Information Space & Lessons Learned

1. Introduction

1.1. D5.4 in the context of EPISECC

This deliverable D5.4 is the only public document within the EPISECC Work Package 5 *Architecture of Common Information Space*. Therefore, it summarizes and partly even repeats the results of the other deliverables D5.1 [1], D5.2 [2], and D5.3 [3] to publish a comprehensive picture of the CIS architecture. Based on the experience with the implementation of a prototype which was demonstrated and tested during the Proof of Concept (PoC), the final architecture was adjusted and the lessons learned are highlighted in this document.

In WP5, the design of an information sharing platform for crisis and disaster management on all relevant layers is elaborated. Task 5.1 *Protocol & Network Interoperability* highlights the radio and mobile communication and the connection of radio networks with the common information space. Task 5.3 *Operational Interoperability* handles the technical procedures required for establishing interoperability between involved organisations. Task 5.2 *Information Interoperability* specifies the technical platform of the Common Information Space (CIS). It describes the architecture and concepts for secure automated information sharing; different type of information is exchanged between tools used by organisations related to crisis and disaster management (responders, infrastructure providers, authorities, scientific institutes etc.).

This document *D5.4. – Architecture of the Common Information Space* describes the concepts for information sharing between the IT tools of stakeholders involved in disaster response. The tools itself were created by the EPISECC partners outside of the EPISECC project (background development), further evolved and adapted in WP5 to be compatible with the CIS concepts, and during validation activities in WP6. The CIS components were developed as a prototype in WP5, and integrated with the existing tools for the final PoC in WP6. The experience made during the prototype implementation and the feedback of participants and observers gathered during the PoC exercise build the second source of this document.

1.2. Structure of D5.4

The first section provides a summary and overview over the CIS architecture and its concepts. It is intended as an entry point for interested readers who want to understand the basic ideas of EPISECC and how they could promote improvements in joint disaster response.

The second section describes the final architecture and technical concepts of the EPISECC Common Information Space based on the experience made during the prototype development and evaluation.

It is the high-level documentation of the EPISECC CIS prototype including those concepts that are discussed in WP5 but were not implemented in the prototype due to budget and capacity limitations.

The third section of the document summarizes the feedback of all stakeholders (PoC participants and observers, AB members, consortium partners, external tool providers) concerning the CIS architecture. It highlights the success factors of EPISECC CIS but also potential week points and fields of improvements. The document concludes with technical requirements which had to be considered when the EPISECC CIS is going to be exploited as an operative solution for crisis and disaster management in European context.

Promising concepts and architectural approaches that were discussed during the project but were not fully elaborated or implemented in a different way are documented in the last section.

The conclusion finally summarises the achievements of EPISECC concerning the CIS architecture, and the steps that would be required to make the CIS concept an operative part of European disaster management.

2. The Idea of EPISECC Common Information Space

This section gives an overview on the idea of the EPISECC Common Information Space (CIS) and the intended use of the concepts developed during the project. It is intended as an entry point for the interested reader.

2.1. The role of information interoperability in crisis management

Hierarchical management structures have dominated crisis and disaster management in the past. Today, a paradigm change is on the way. Professional responders are pushed into collaborating with an increasing number of organisations and even the citizens (i.e. crowds) operating in a different manner. Crisis and disaster management will be a highly networked and collaborative activity in the near future. Today, the term “networked security” is used for a new way of electronically facilitated collaboration between stakeholders involved in a non-military disaster relief mission. Process data are shared via the information cloud and enhance the effectiveness of well proven processes.

The stakeholders (see **Figure 1**) are on the one hand organizations from the public safety domain where crisis management is part of their core business. On the other hand, also organizations whose core-business has nothing to do with crisis management play an important role (e.g. infrastructure providers, logistics and transportation companies, medical service providers …); they are required to contribute to the crisis management effort in addition to their own business continuity management.

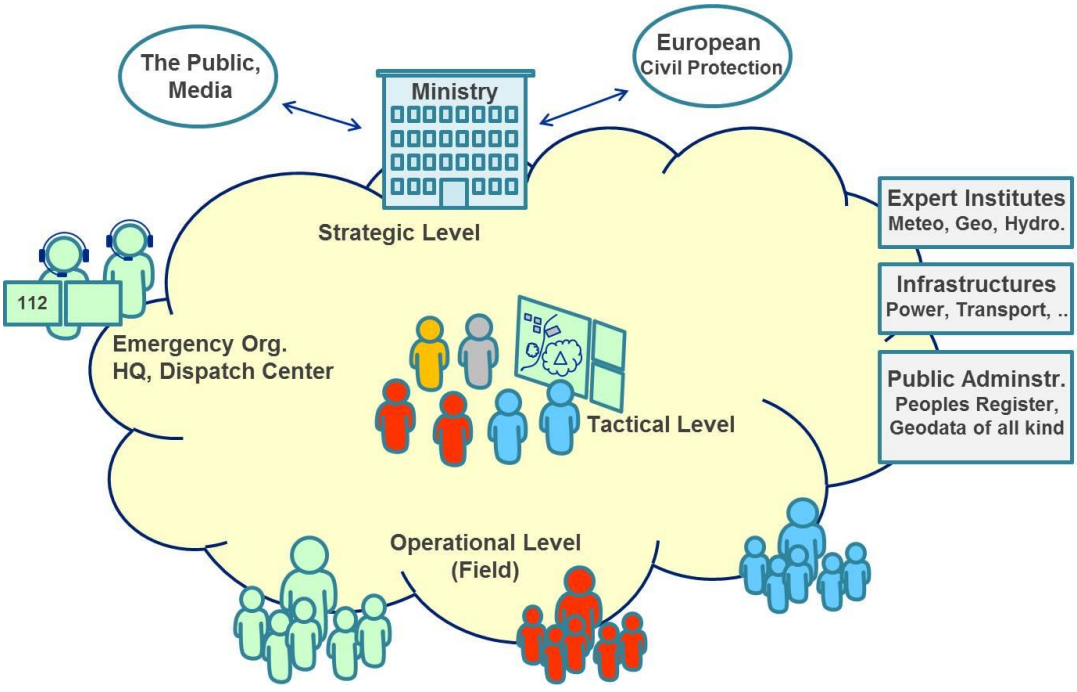

Figure 1: Information interoperability stakeholders

2.1.1. Objectives of information interoperability

Cross-organizational collaboration and sharing of related information today is still mostly based on human interaction like face-to-face meetings, telephone calls, fax transmissions, email messages etc., and on proprietary and closed IT systems of the organisations. Consequently, situation awareness is hampered by a fragmentation of relevant information into pieces held by different stakeholders. Within the highly collaborative scenarios of the non-military crisis management operations this fragmentation causes uncertainty whether the information base for critical decisions is up-to-date, comprehensive and valid.

Decision making based on a comprehensive picture of the situation requires exchange, verification and integration of all the different pieces of information provided by the stakeholders with their specific organizational and cultural background. At the same time a common understanding of the situation is also a basic prerequisite for successful collaboration.

2.1.2. Situation Awareness and Common Operational Picture

One of the most essential challenges in emergency and disaster response operations is to immediately obtain and continuously maintain situational awareness (SA). Major aspects of an organization-specific situational awareness are:

General situation in the affected area

- Weather conditions,
- Special local circumstances,
- Restrictions in infrastructure,
- Restriction in basic supply,
- Public behaviour,
- Other particularities with general effects.

Each of these aspects covers not only the current status, but also possible future developments.

Threats and Damages

- Kind and cause of threats / damages,
- Extent and impact of threats / damages,
- Dangerous / restricted areas
- Who or what is affected by threats / damages,
- Subsequent threats and damages.

Resources and response actions

Status of organization's own resources, and activities and capabilities of the other involved responders:

- Forces and means already deployed,
- Forces and means at further disposal,
- Uncovered needs for response.

The common operational picture (COP) is compiled from data shared between all stakeholders throughout the whole lifecycle of the operation, and combined with already existing (geo-referenced) information on infrastructure, population, vulnerabilities, land coverage etc. Connecting and integrating the various systems for communication, information management and intelligence of all actors in disaster relief, the CIS enables the automated and timely distribution and exchange of situational awareness (SA) information.

Especially the local emergency management authority (LEMA) as the responsible body in disaster management can benefit from preceding and ongoing situational assessments from various sources. On the other hand, the LEMA, when having compiled a COP, can provide a homogeneous, continuously updated overview of an event.

Almost any information that is related to situational awareness has a spatial reference. This leads to the advantageous situation that this information, automatically exchanged via the CIS between the organisations command and control (C^2) and information systems, can immediately be displayed on the organisation's digital situation maps.

2.1.3. Information interoperability use-cases

A detailed specification of use cases to be experimented during the proof of concept is given in deliverable D6.2 [4]. This chapter lists in a generic way use cases for automated information sharing as a reason for the introduction of a common information space in cross-organisational and even cross-border disaster management.

Generic use-case I: Data/information flow from RESPONDERS to LEMA

Since LEMA is dependent on data/information that is received from responding organisations (their organisation specific situational awareness) the establishment of information interoperability in the CIS will be of value.

Generic use-case II: Data/information flow from LEMA to RESPONDERS

LEMA is the entity in need/in charge of the COP. LEMA is responsible for taking the overall tactical decisions for the disaster relief operations. In short, these decisions comprise WHO has to perform WHAT activities WHERE and WHEN (eventually together with WHOM). Such decisions together with accompanying information are usually communicated during briefings of the LEMA with all responding organisations. Covering this in the CIS information elements and mechanisms will be a great contribution to the efficiency and the quality of a collaborative mission execution.

Generic use-case III: Data/information flow from RESPONDERS to RESPONDERS

Everything stated with generic use-case I is true for this as well. A standardised information exchange between responders is currently neither state of play nor established frequently. Nevertheless, a systematic exchange of data/information regarding the *General situation in the affected area* and the *Threats and Damages* would be of a great value for every responding organisation.

Generic use-case IV: Data/information flow from EXTERNAL INFORMATION PROVIDERS to LEMA

Everything stated with generic use-case I is true for this as well. Beyond information from responders, LEMA needs data from external sources as well, e.g. meteorological, hydrographic or seismic data and forecasts, status of critical infrastructure, traffic data. Such external information is available in various formats on different channels and can be linked to the CIS by specific adaptors. So, this information can contribute immediately to a comprehensive COP.

Generic use-case V: Data/information flow from LEMA to INFRASTRUCTURE PROVIDERS

Continuity of critical infrastructure is crucial for successful disaster management. Including critical infrastructure providers in a specific information channel and alerting chain might help optimizing the maintenance of critical infrastructure.

2.2. The EPISECC Common Information Space solution

The focus of the Common Information Space is to facilitate and support multi-organizational collaboration during the response phase of a crisis and disaster management effort, e.g. in case of flooding, forest fires, or earthquakes.

The analyses of EPISECC WP2 and WP3 confirm the evident need for fast and reliable exchange of information between autonomous stakeholders which rarely collaborate in their day-to-day business but have to co-operate during disaster response. Therefore, the IT tools of the organisations should be enabled to exchange information automatically, that means to be able to send selected own data and to receive and interpret data from other tools in a way that the users can understand the meaning. These concepts and requirements realise the Common Information Space (CIS) architecture of EPISECC.

One basic requirement is at the one hand that the existing legacy tools need not to be modified or even replaced, at the other hand that the connection of a tool to the CIS can be established fast and easily without interfering with the existing solution or the other tools in the CIS. This was proven by the integration of the tool SARONTAR[1] from TeleConsult Austria[2] in the final proof of concept prototype (see 4.1.1). SARONTAR is deployed and in use at the Austrian Mountain Rescue Services in the province Styria.

The EPISECC approach is using adaptors which connect existing export/import interfaces of tools to the CIS and transform proprietary data formats into standardised messages that are exchanged within CIS (syntactical interoperability). So, the number of interfaces is reduced significantly in case of many CIS participants (see Figure 2 and Table 1), and the provided data is mapped to standardised information types and data structures.

[1] Situational Awareness and Command & Control of Rescue Forces in Alpine Regions (SARONTAR)

[2] http://www.teleconsult-austria.at/

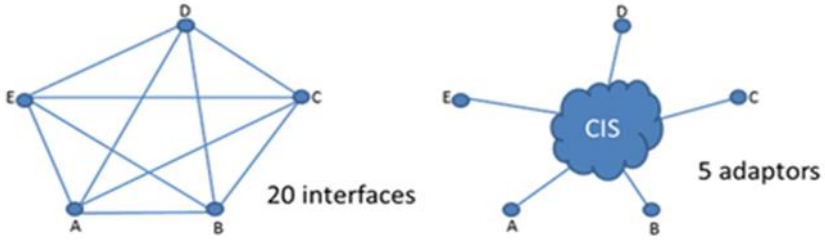

Figure 2 : Adaptors reduce number and complexity of interfaces

If every partner exchanges one type of data with every other CIS participant, the number of adaptors is equal to the number of participants (n), while the number of individual interfaces increases to the second power of the number of partners: n*(n-1).

participants	2	3	4	5	6	7	8	9	10
adaptors	2	3	4	5	6	7	8	9	10
interfaces	2	6	12	20	30	42	56	72	90

Table 1: Number of adaptors vs. number of individual interfaces

The sole transformation of data formats doesn't make a message understandable if the semantic of terms and acronyms is different for sender and receiver. The EPISECC taxonomy/data model (see D4.2 [5] and D4.3 [7]) is used for mapping the taxonomies of CIS participants (during CIS preparation), and for automated matching of terms during the information exchange. That means that matched keywords can be interpreted by the receiving tool, and semantic annotations to text messages explain the meaning of terms to the users (semantical interoperability).

The information security concept of the CIS architecture makes the message transfer safe and enables the CIS participants to decide dynamically which information goes to which group of recipients (data ownership, need-to-know principle).

2.2.1. General CIS architecture – adaptors

The adaptors are the basic idea of CIS. The CIS adaptors link the participating tools to the Common Information Space. For every tool interface, a specific adaptor must be implemented and installed. Adaptor templates are provided by the project team to enable the tool providers writing their adaptors in an easy and fast way.

The adapters stay in the responsibility and run within the secured network environment of the tool owner. Every access to the data hosted by the adapter is monitored by the authorisation check implemented in the adaptors and is recorded for audit and tracing purposes.

Every adaptor consists of three parts:

CIS Connector: manages the communication with the tool interface and translates proprietary protocols to standards, and back. The Connector is written by the tool provider based on the EPISECC Connector template.

CIS Core: manages central functions in a uniform way. The application of security policy and the semantic matching is controlled by the Core (Security and Semantic boxes).
Value added services can be integrated in the Core (available for the whole system).

CIS Distributor: manages the connections inside the CIS and the data exchange with the other Adaptors in the CIS.

In addition to the adaptors there are some central components (services) managing the access rights and the semantic interoperability.

The **Discovery Agent Service** manages the CIS participants (organisations and their tools) and the parameters needed to address information to them. Every tool and adaptor joining a CIS must be approved and authenticated before becoming part of the CIS.

The **Partition Service** segments the CIS participants in groups of organisations, collaborating in a mission (Collaboration Group Online Room, CGOR). That allows sharing of specific information only with defined subsets of CIS participants.

The **Admin Web GUI** is a user interface to the adaptor Core for administration of the Partition Service during operations. Every CIS participant can create a new CGOR or join a CGOR he is invited to.

The **Semantic Web Service** is used for enabling Semantic Interoperability. It provides the software interfaces, used by the calling software components (CIS adaptor Core) to ask the runtime semantic matching (and related semantic annotations) between concepts of senders and receivers of messages.

The **Semantic Repository** contains all available taxonomies of organisations with their mapping to the EPISECC taxonomy. It is queried by the semantic Web service.

2.2.2. Syntactical interoperability: joint formats and standards

Definition of Syntactic Interoperability [8]: "*If two or more systems are capable of communicating with each other, they exhibit syntactic interoperability when using specified data formats and communication protocols*".

The adaptor architecture is an abstraction layer that hides the individual data formats and protocols of the tool interfaces and transforms the provided information into the protocols and standard data formats adopted in CIS. The information is shared between the adaptors by sending standard messages to the intended recipients. The data formats proposed in the project are existing XML standards that were developed in the domain of emergency and disaster management (see 3.1).

These standards are propagated and published by the OASIS open standards consortium [10], OMA Open Mobile Alliance [15], and ISO [14].

The participating organisations, their tools and the services which they are providing/consuming, and the current configuration is stored in the Directory Agent by the CIS administrator. The adaptors access this information for the message routing (peer-to-peer communication).

The syntactical interoperability architecture is depicted in Figure 3.

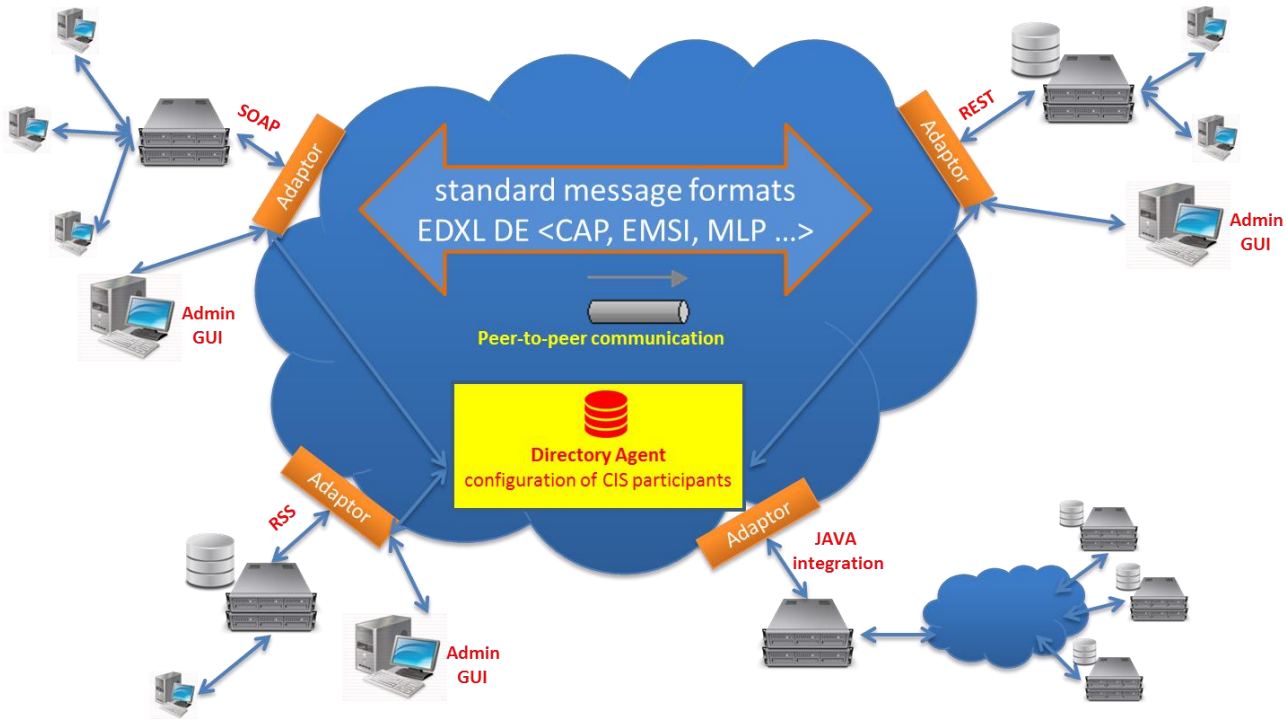

Figure 3 : Syntactical interoperability via Common Information Space

Using published standards instead of developing own data formats provides many benefits concerning effort, reliability, completeness, and usability of the message formats. Tools that already handle these standards can be integrated seamless in the CIS. Tools with very specific proprietary data formats might encounter issues with information mapping, or even lose some specific information that cannot be mapped to the standards.

That can be mitigated by defining CIS profiles: conventions about the interpretation of the standard definitions and usage of freedom given in the standard. *Example: a CAP message (see chapter 323.1) that lists device IDs in the field Addresses is directly forwarded as a short text message to TETRA terminals and mobile devices by the adaptors of MDG and SARONTAR.*

2.2.3. Semantical interoperability: understandable information

Challenge: understandable information

In general terms, semantic interoperability is defined as the ability of computer systems to exchange data with unambiguous, shared meaning. Differently from Syntactical interoperability, Semantic interoperability is not concerned with the formatting or packaging of the data, but with the simultaneous transmission of the data together with its meaning (semantic), by linking proprietary data elements (key terms and concepts) to a common vocabulary of terms and concepts.

The need of using a shared vocabulary for ensuring a common understanding of the exchanged information, is highlighted in the simple scenario depicted in Figure 4 below. Different end users' tools for disaster management, from Italian Fire Brigades, Greek Fire Brigades, Greek Police, and German Red Cross in the considered example, might be able to seamlessly exchange data, provided each of their systems are connected through suitable software interfaces/Adaptors and the involved organisations have agreed on common protocols for the shared data (*syntactical interoperability*). Still, the proper, mutual understanding of the information may be compromised by the fact that each organisation represents relevant terms and concepts (e.g. incident codes, resource codes) using a proprietary encoding or vocabulary. Tools for *semantic interoperability* are therefore needed to map proprietary terms and concepts in the corresponding common ones (EPISECC Taxonomy) during the set-up and configuration of the CIS system. So, the matching (conversion) between relevant terms and concepts insade the shared messages can be provided at runtime during operations.

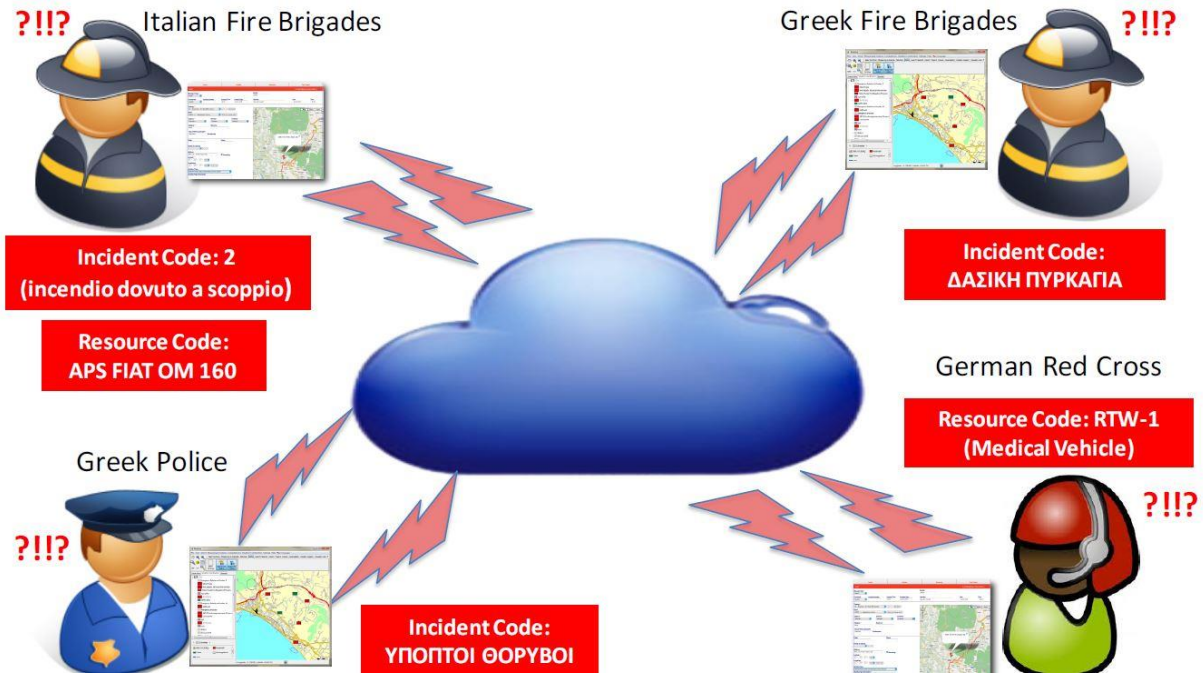

Figure 4: Challenge of sharing commonly understandable information

Semantic Box

It has been described in WP4 (see deliverable D4.3 [7]) how the Semantic Interoperability in EPISECC will involve the following steps:

1. EPISECC Taxonomy building: population of the EPISECC Taxonomy, including all relevant terms, concepts and codes used in disaster management, and insertion of the common EPISECC taxonomy into the Semantic Repository.
2. Further population of the Semantic Repository: Semantic Repository needs to be populated with existing structures containing concepts, like e.g. CAP, EMSI, and other common dictionaries, terminologies or taxonomies and cooperating organisations' concepts.
3. Semantic mapping: at configuration time, there is the need to perform the mapping between terms and cooperating organisations' concepts from existing structures and the EPISECC taxonomy, and store this mapping into the Semantic Repository.
4. Semantic matching: at runtime, i.e. during information sharing through the CIS and in order to be sure that the most relevant information can be understood by everyone involved in the communication, there is the need to match key concepts, previously stored in the Semantic Repository and selected from the shared information, with the EPISECC taxonomy, and further with the concepts of other organisations involved in the CIS. Semantic matching uses relationships between concepts established in the previous step.

In the actual EPISECC and CIS concept, the EPISECC taxonomy is a live, dynamic structure that will be constantly updated with new terminologies and with new end users' concepts, together with their mapping.

2.2.4. Information ownership and data security

Confidentiality and integrity of the data exchanged on the CIS is of crucial importance. Every CIS participant must be sure that the submitted data are safe (can't be accessed unless by the intended addressees) and the received data are reliable (can't be faked or modified). The following procedures and design principles shall ensure the information security.

Registration and authentication of CIS participants

Trust should be established between all components and users of the CIS architecture. These can be divided into three layers of interoperability

- Information Layer, which includes organisations and individual users
- Automation layer, which includes CIS Software components
- Communication and hardware layer, which includes communication network and devices

Trust from the Emergency Organisation perspective is rooted, when an authorised employee – possibly administrator – of the organisation obtains and installs an official CIS-Software Package (CIS-SW). An official CIS-SW package should be signed and certified of its integrity and would provide assurance that it does what it is supposed to do. The official CIS-SW includes all the necessary CIS

software components, which are needed by an Organisation to connect its external tools to the CIS and exchange information and services with tools connected to the CIS.

The CIS-Connector which is programmed individually based on the provided Template has to be tested and certified before it is allowed to connect the CIS, in order to guarantee that the sent data are valid and compliant with the applied CIS policy and don't disturb the flow of information in the CIS.

Trust between emergency organisations and authentication of the organisations and users can be established either by using accredited certificates or by having an authorised employee from each organisation who mutually authenticate each other. Trust between CIS-SW components is established by allowing only signed CIS-SW to interact with each other. A secure connection SSL-VPN based solution should be established between CIS-distributors to protect information in transit. Furthermore, implementation procedures should ensure that related OWASP cheat lists are followed (https://www.owasp.org/index.php/REST_Security_Cheat_Sheet)

CGOR – Cooperation Group Online Room

Not every information is intended to be shared with all participants in the Common Information Space for several reasons. Personal data are liable to the European and national data protection directives, requiring the "need to know" principle. Confidential and sensitive data must be restricted to a dedicated list of recipients and must be protected by design.

While the responsibility for the processing, classification and release of data always stays with the user of the owning organisation, the Common Information Space provides technical concepts fulfilling the data protection requirements. The basic idea is the segmentation of CIS participants in groups that currently need to cooperate in a mission and to share information. The virtual online room for sharing data between all members of a cooperation group is called CGOR. It is comparable to a mailing list in a secured e-mail system, containing a list of recipients, and enables group-specific data encryption.

A global CGOR for sharing public information is available by default, and every tool that is registered for participation in CIS becomes automatically a member of the global CGOR. Specific CGORs can be created by an administrator of any CIS member in a simple Web GUI. Intended participants are invited by the CGOR owner and can confirm the participation, meaning that any information sent to the CGOR is shared with all other members of the Cooperation Group (see Figure 5). The routing of the messages and CGOR specific data encryption ensures that the information is only accessible by CGOR members.

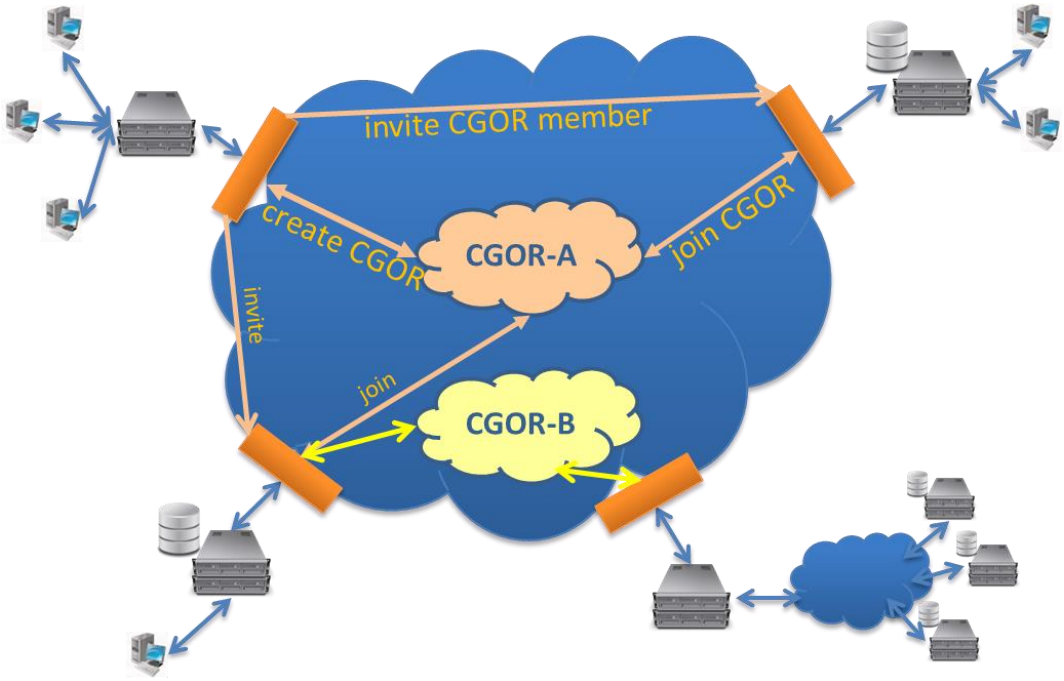

Figure 5: Information segmentation – CGOR

The tool sending information to the CIS has to classify the sent information in a way that the CIS Connector is able to determine the appropriate CGOR in an unambiguous way. The underlying rules are implemented specifically for the CIS 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.

Examples (see also chapter 5.4):

- *Location info of police units must be limited to security forces only. A corresponding CGOR is established with the determining parameter "POLICE". The Connector checks the availability and sends MLP messages only to this CGOR; otherwise the information sharing is denied.*
- *A railway company joins the CIS, providing public traffic information (location and status of trains by EMSI resource messages), and information on incidents (alerts by CAP) that shall only be shared with police and fire brigades. The connector allocates EMSI messages to the Global CGOR but CAP messages only to the corresponding CGOR.*
- *In case of a large incident, several relief organisations have to cooperate for a limited period of time. A CGOR is created for that incident. The Connectors of every organisation are configured accordingly, and every message with the incident ID is posted in the CGOR. After the response phase, the CGOR is closed. There must be a default rule for sharing information related to an incident without corresponding CGOR.*

An administration tool will be provided by the CIS supplier. The administrators of the participating organisations can set-up new CGORs, invite other organisations, and confirm invitations by others,

based on trust and cooperation agreements. When the need for cooperation has ended, every organisation can abandon the CGOR membership, and the owner can close the CGOR.

A more advanced approach might comprise the automated generation of CGORs based on tool functions and defined rules.

Example:

- *The COP tool of the Civil Protection Authority (CPA) automatically generates a CGOR if an incident is created in the tool, and invites all organisations assigned to the incident. The tools (Connectors) of the addressed organisations automatically accept invitations from CPA. When the CPA closes the incident, the corresponding CGOR is also closed automatically.*

This approach requires that the participating tools are prepared for this way of working. At least the leading CPA COP must support the functions triggering the CGOR management, and the tools of participating organisations must be able to assign automatically their shared information to the generated CGORs.

2.3. The network – basis of information exchange

The following part details the EPISECC architecture and its benefits for first responders to ensure protocol and network interoperability during a large incident. This is the basis to provide operational communications for first responders and their needed command and control as well as information delivery.

2.3.1. Internet, public mobile network, TETRA

Today, interoperability between governmental radio systems for public protection and disaster relief (PPDR) e.g. TETRA, TETRAPOL and proprietary systems is limited. They are typically isolated within one country and even within one organization system and very often without interoperability with other countries and/or organizations.

Cellular 4G/LTE systems are widely available in European countries with good coverage. However, in disaster situations cellular networks are usually out of operation (power failures) or congested as too many civil users are trying to access the service.

Satellite services are available during disasters but as those services and terminals are not in use in normal communications due to their limitations and cost, those terminals are not in place in incidents. Services are not initially configured to be available and first responders are not necessarily trained to use them.

Hence incidents need special preparedness to handle availability of networks and planning for their connectivity and interoperability.

One EPISECC project effort has been focused on ensuring protocol and network interoperability during a large incident. This is the basis to provide operational communications for first responders

and their needed command and control as well as information delivery. As such this document describes:

- the architecture of underlying communication networks including:
  - Interconnection of legacy PPDR networks via dedicated gateways and the CIS
  - Network re-configuration and redundancy
- data traffic optimization
- the security and privacy solutions at both protocol and network level.

The 3GPP standardization for inclusion of critical communications into cellular networks was also studied and taken into account.

The architecture depicted in Figure 6 is proposed for the underlying fixed radio networks.

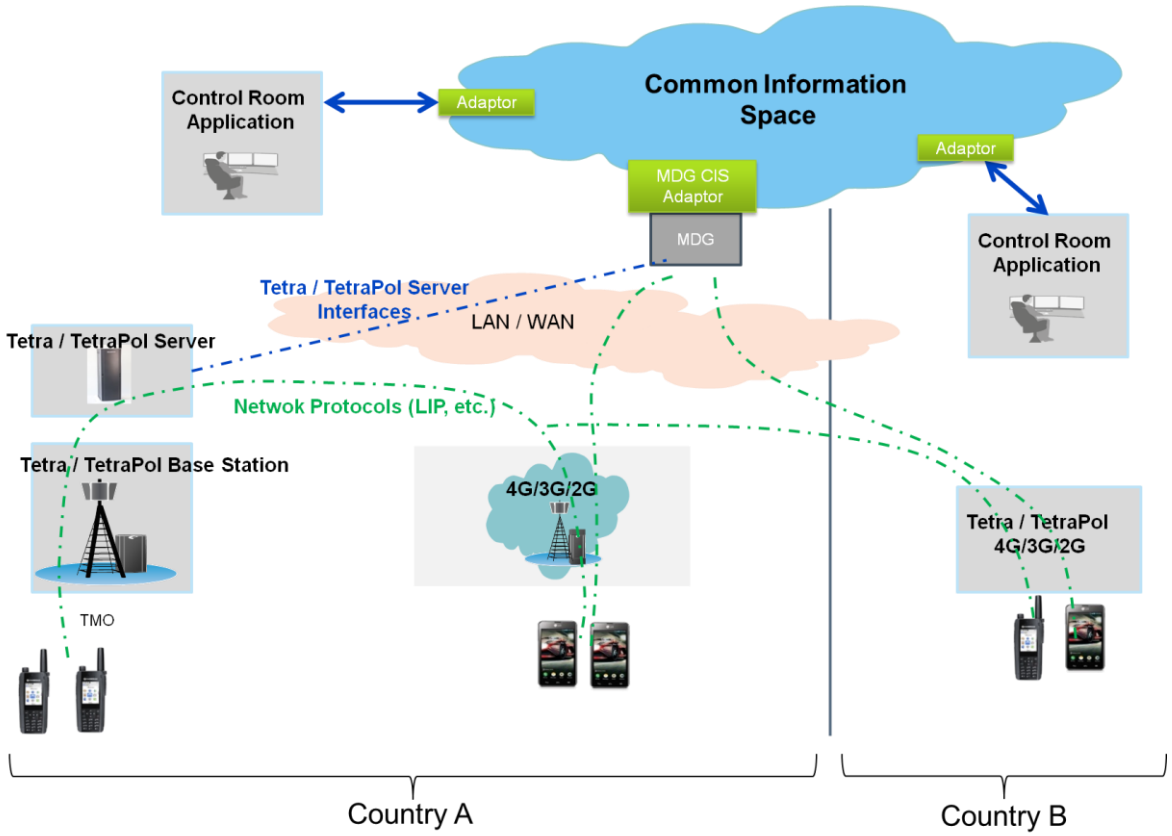

Figure 6: Linking network information to CIS

2.3.2. Linking TETRA to the Common Information Space

EPISECC CIS architecture proposes a decentralized concept to interconnect various (Legacy) PPDR data/situation awareness systems together. Airbus AVL server (Mobile Data Gateway, MDG) is aimed to be connected to the CIS common core via the adapter, as defined in the architecture. As the mapping application provides service (independent of CIS interface) to the TETRA mobile users and

dispatchers (OM100), it behaves as a location server for other CIS interconnected systems to get real-time positioning and status information of field units.

The adaptor performs the following functions for the CIS connector related part (Figure 7):

- Identification of AVL service to CIS connected systems (service discovery)
- Protocol conversion from MDG API (location and status) to the CIS selected protocol MLP
- Protocol conversion from the CIS CAP protocol to the MDG API (short message)

Optionally

- subscribing to Location / Status / Availability services provided by other applications connected to CIS, including also back-to back AVL service interoperability of two TETRA light AVL services, connected via CIS (e.g. Light AVL client adapter).

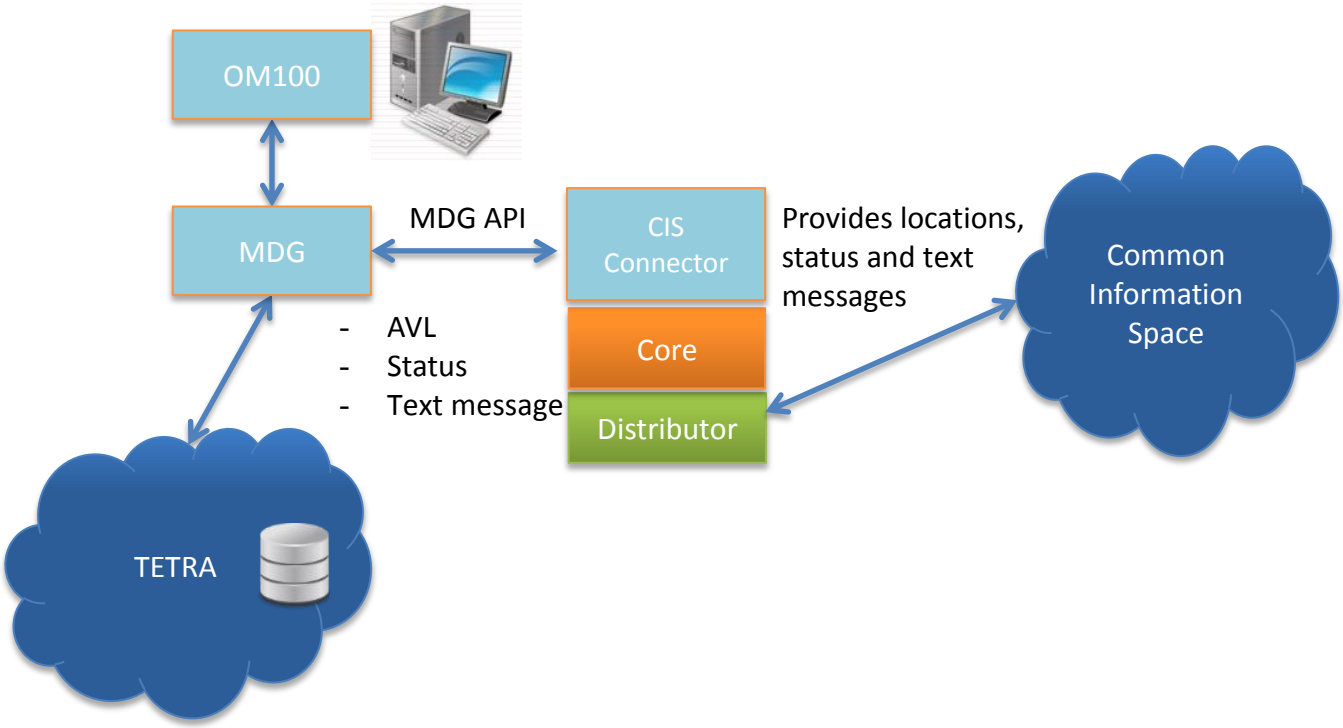

Figure 7: AVL service connection to CIS

For the EPISECC project and for the best reliability, the MDG was improved to be deployable in a portable way. This configuration is called wireless MDG. The purpose of this architecture is to guarantee that the MDG is still available even if the TETRA IP backbone is damaged during the disaster. Indeed, if the MDG is connected to the TETRA network through a “standard” fixed IP backbone, if this backbone is seriously damaged, the MDG would offer a degraded service and potentially no service. To avoid this use case, the wireless MDG was designed to be quickly deployable in the TETRA network.

The wireless MDG is seen as a TETRA terminal for the TETRA infrastructure (potentially in fall back mode). To ensure the integrity and the confidentiality of the data exchange in the Common Information space, the wireless MDG implements the TETRA security features.

2.4. Procedures for collaboration in a CIS

The following section describes recommended procedures for the set-up of a CIS and the application of CIS membership. It was discussed and agreed upon with the EPISECC advisory board, but it is not a mandatory requirement from technical point of view. It was not subject of the final Proof of Concept.

The preparation of a Common Information Space and the tools to be linked should be started in the preparation phase before the critical situation. Every participating organisation must get authorised and must create the connectors for the tools they are running. After the installation, registration and parameterization of the adaptor software, the organisation is ready to participate in the CIS.

It is the goal of the EPISECC project to have only one CIS in each disaster situation where every involved organization can exchange information.

There may be several separate CIS setups which don't overlap concerning the missions they are covering. For example

- a CIS used by Italian, Slovenian rescue services
- a CIS for local usage in Scandinavia

To be able to use a CIS during a disaster, several steps must be executed before the disaster starts:

- A CIS must be created by one organisation (CIS service provider)
- Other organisations have to become members of this CIS

These two steps take time and cannot be executed ad-hoc. So, they must be executed in the preparation phase. In the next chapters, we will explain these steps in more detail.

2.4.1. Stakeholders

To establish a CIS the following stakeholders are needed:

- CIS product owner
- CIS service provider
- CIS member

2.4.1.1. CIS Product OWNER:

The CIS product owner sells the CIS components, maintains the components and supports the CIS service provider during the setup of the CIS and the maintenance**.**

The CIS product owner has the following responsibilities:

- Maintenance of CIS Software and components
- Provide a Website with the following functions
    - Register organizations for CIS usage
    - Check if service provider is allowed to participate in CIS
    - Provide access to CIS Software
    - Provide a list of installed CIS and who is the CIS administrator

- Provide a help desk for CIS usage
- Owns a certification process for Adaptors

2.4.1.2. CIS service provider

The CIS service provider is an organisation that wants to setup and maintain a CIS for himself or other organisations, e.g. a civil protection organisation or a governmental organisation.

The CIS service provider:

- Creates, operates and manages a CIS for several organizations
- Organizes and operates his CIS
  - invites organizations to participate to the CIS
  - checks requests of organizations who want to participate
  - removes organizations from the participants list if necessary
  - provides the CIS administrator

2.4.1.3. CIS member (user)

A CIS member is an entity that was invited by the CIS service provider to participate in the CIS. The CIS member needs to have a tool that can share information and that should be connected to the CIS. Therefore, a CIS member:

- is one organization that wants to exchange information via the CIS
- is one organization that uses a tool to connect with the CIS
- can create CGORs, participate in CGORs

2.4.2. Creation and setup of a CIS

A group of public safety services / a group of countries wants to share information with each other and install their own CIS. The following describes the requirements to setup the CIS environment.

Prerequisites for implementing a CIS:

- The organisation has to own a secured network infrastructure
- The organisation must have the possibility to configure the network as needed
  - The network includes a DNS server to address future partners by their hostname instead of their IP address
  - The organisation has a digital signature provided by an authorized Trust centre (e.g. A-Trust[3], LuxTrust[4])

[3] https://www.a-trust.at/

[4] https://www.luxtrust.lu/en

When the CIS service provider fulfils the prerequisites, it can install the CIS with following steps:

- Request an EPISECC membership approval certificate that contains a specific identifier issued by the EPISECC CIS service owner
- Download the CIS server libraries with the central EPISECC components (discovery services, the partition service, the semantic repository and semantic services, and the administration tool) from the EPISECC Website

To **implement a new CIS** following steps have to be executed:

1. Setup a certification authority to certify/deliver any certificate that will be used in the CIS (can also be an existing public Trust centre)
2. Install the CIS discovery services and partition server using the installation application from the downloaded CIS server libraries
3. Use the setup administrative UI to setup and configure the CIS
4. Setup a VPN as CIS support network infrastructure

To **setup and to manage the CIS**, different administration UI tools will be provided:

- A Web-Site including all instructions and conditions for new organisations to prepare all steps for joining to the Common Information Space
- A Web-Site for the registration, authorisation and installation steps:
    - To register all information of the participating organisation, including certificates of the new organisations, the purpose of their participation and the list of contact persons.
    - To check registrations and if valid, add the organization and provide the preconfigured Adaptor software to be downloaded
    - This server acts also as a portal for logging and system recovery. A failing member can reconstruct its node by a new download
    - This server provides the possibility for extending the vocabulary of the semantic repository by the member specific taxonomy and for mapping them to the EPISECC Taxonomy.
- A Web hosted tool for the configuration needs of each member during the CIS operations:
    - To Manage the creation and modification of CGORs
    - To invite members to the CGOR
    - To configure the CIS adapter to influence the behaviour, which CGOR should be used for communication
    - To monitor the message transfer without the need of access to the partners' tools and message content.

2.4.3. How to become member of a CIS?

CIS membership enables a partner to publish or access data to/from CIS. The following sections describe the proposed process for enabling an organisation and their tool to be a CIS member.

2.4.3.1. Prerequisites

Organisations who want to participate in the CIS should provide an electronic certificate from a public Trust Centre following the European Directive 1999/93/EC. This prerequisite avoids the need for the CIS service provider and CIS administrator to check the identity of an organization and the person requesting the participation in a CIS.

Participation in the CIS requires that the organisation looking to request a CIS membership should agree to the terms and conditions covering usage of the CIS to send and receive information, as well as terms and conditions covering information to be sent and information to be received. This should cover: data quality that the emergency organisation is expected to provide, its liabilities regarding choosing the recipients, the CIS responsibilities to deliver information in secure manner to intended recipients, the organisation responsibilities towards received information including processing, storing, usage, etc. This may be done by a qualified person such as an organisation legal representative/department, or in case of governmental organisation, the ministry that governs the organisation.

To join the CIS, an organization must be acknowledged as a public or private authority that participates in civilian protection and security or providing relevant and reliable information that is needed in disaster response. They must also have an information system or a legacy tool with a certified CIS adapter to interact with CIS. Legacy tools that can be connected to the CIS must comply with following prerequisites:

- Must be able to exchange information
- A CIS adaptor must be developed for this tool, based on the provided templates and components.
  It is the responsibility of the organization to provide this adaptor; the CIS product owner supplies the CIS software components and may provide support with implementation and integration.
- The adaptor must have a certificate ensuring that it is compliant with the CIS services and the CIS rules, issued by the CIS product owner after testing.

If an organisation wants to translate its local semantic into foreign semantics and vice versa, it is responsible for selecting relevant semantic concepts (data dictionaries, vocabularies, terminologies, etc.) and mapping procedures (i.e. classification of the selected concepts against the EPISECC Taxonomy).

2.4.3.2. Steps to be executed

To request participation in a CIS, the applicant must fill an online form referring its legal registration as civilian protection organization.

The application of organisations to become a CIS member is submitted to a CIS operator by an authorised representative of the organisation. The application may be submitted electronically to the CIS operator official web-site. For this operation to be completed successfully the following is done

1. The Emergency Organisation should have an electronic-Id issued by a certified trust centre. This will provide an electronic authentication of the emergency organisation identity. The electronic-ID should also name individuals who are authorised to represent the emergency organisation to carry the application process.
2. The CIS operator should have a valid certificate (signed by a trusted third party) installed on its official web-site. The certificate is used to provide a secure https connectivity during the application process
3. An Emergency_Organisation_authorised_representative fills an Organisation application form on the CIS-operator official web-site. He provides the Emergency Organisation electronic-ID during the application process.
4. When a form is completed and submitted, it is subjected to an automatic check first. A human verification may also be required to decide on the acceptance of the emergency application. A decision is made based on both the applicant eligibility to join, and the correct application procedures are satisfied. This Organisation is now a member of the Common Information Space.
5. Once an application is approved. The next step is to connect the organisation to the CIS. A certificate is issued to the organisation and an authentication mechanism - such as username and password- is provided to the Emergency_Application_Employee to access the CIS-Member-Administrator-portal (This is a portal that allows an authenticated authorised_Emergency_Organisation_Admin to connect to the Directory Agent, and Directory Structure, create a local copy of the CIS-software, connect his legacy tools, configure the CIS local directories, test connectivity of the tools to the CIS-through ping tests-, run tests to ascertain that his tool Connector is valid and approved). Note that at this stage the portal can only be used for viewing the directory agent and directory structure, and create a local copy of them. However, to carry on the rest of the portal functions such as; connecting the tool, run tests, linking the local-DA and local-DS to the CIS-operator's DA and DS, the CIS software package need to be downloaded first as described in the next step.
6. The Emergency Organisation employee obtains the CIS-Connector-SW suitable for its tool. He installs it and connects it to his tool.
7. To enable the CIS-key feature; Semantic Annotation, the Emergency Organisation Employee needs to obtain and install the necessary semantic repository.
8. At this stage, the emergency Organisation tool is connected to other tools via the CIS.
9. First Connection tests are run, such that the tool is able to receive and display information sent on the CIS-default CGOR. A testing CGOR is used in this stage to test connectivity, sending and receiving, information annotation and all features of the CIS. At the end of this stage, the CIS connection is ready for operational stage.

10. Through the Administrative UI of the CIS-Adapter, the Emergency Organisation employee can see all the CGORs that his organisation tool is connected to. He can start receiving and/or sending information by ticking the CGOR access control list.

3. The architecture of EPISECC Common Information Space

This section specifies the technical CIS architecture. It describes the design concepts and functional components that are building the CIS platform.

3.1. Interoperability standardisation in Crisis Management

Standards are the basis for syntactical interoperability in CIS. The project EPISECC uses the following standards in the prototype and proof of concept, but it does not restrict the CIS to exactly these formats and protocols. The CIS architecture can handle any formats that the concerned adaptors have implemented.

Every message content is packed in an **EDXL DE** [11] envelope that provides all parameters needed for the message routing, including data protection rules. The message content can be either a valid XML file or any mime type object (picture, text document, spreadsheet …) that the implemented adaptors can handle.

The EPISECC CIS prototype adopted the following standards.

- Common Alerting Protocol **CAP** [12]: "CAP is a simple but general format for exchanging all-hazard emergency alerts and public warnings. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. … And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience." The CAP standard definition allows to amend the defined data structure by individual parameters and to define customized CAP profiles.
- Mobile Location Protocol **MLP** is an application-level protocol for receiving the position of Mobile Stations (mobile phones, tablets, radio devices, etc.) independent of underlying network technology. In context of EPISECC CIS, MLP is used for reporting the location and the status of mobile devices of the responders in the field, and so for tracking of resources.
- Emergency Management Shared Information **EMSI** [14] is used to transfer the situational view of an emergency as seen by an observer at a particular time to another observer, thus contributing to the situational awareness of the various parties regarding a given disaster or crisis event. The EMSI message follows an XML structure based on an object model whose main entities are:
  - events, understood as something that takes place which an agency should respond to (e.g. a natural or man-made disaster),
  - resources available to support or help in the response to the events, and
  - missions aimed at handling the events and thus reducing their impact.

  The objective of the EMSI specification is to ensure that the semantics of an individual message are unambiguous. A taxonomy of terms and hierarchical encoding to be used in the EMSI message is defined in the comprehensive EMSI data dictionary.

This list can be extended if the concerned tools are able processing the corresponding information, e.g. by adding sensor data (SensorML. SOS) [17], or information on missed persons (PFIF) [19].

3.2. CIS adaptors architecture

The CIS adaptors link the participating tools to the Common Information Space. For every tool a specific adaptor must be implemented. Adaptor templates will be provided by the CIS product owner, enabling the tool providers to write their adaptors in an easy and fast way.

The adaptors stay in the responsibility and run within the secured network environment of the tool owner (CIS member).

Every adaptor consists of three parts (see Figure 8):

- **CIS Connector**: manages the communication with the tool and translates proprietary protocols to standards, and back. The Connector is written by the tool provider based on the EPISECC Connector template.
- **CIS Core**: manages central functions in a uniform way. The application of security policy and the semantic matching is controlled by the Core (Security and Semantic Services)
  Value added services can be integrated in the Core (available for the whole system).
- **CIS Distributor**: manages the connections inside the CIS and the data exchange with the other Adaptors in the CIS.

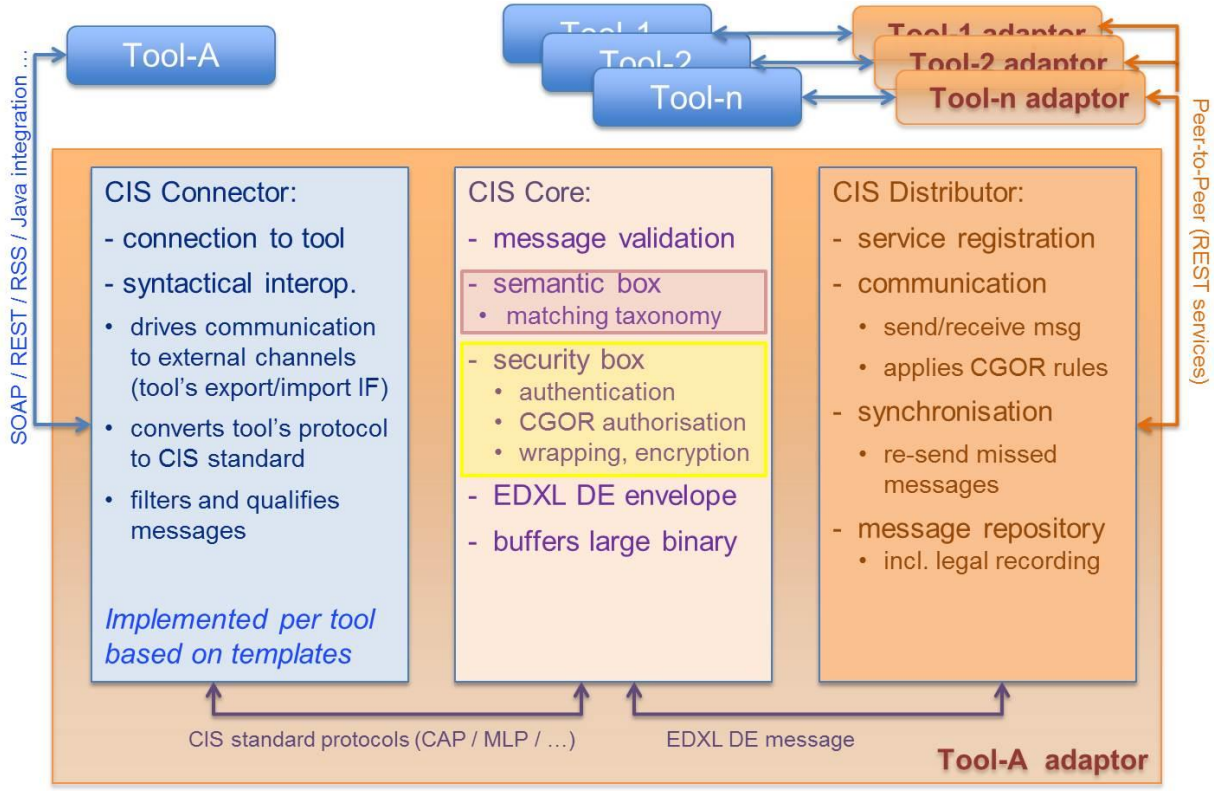

Figure 8 : CIS Adaptor architecture

3.2.1. CIS Connector

The CIS Connector handles the communication on the side of the tool – that means it covers all tool specific protocol and data handling implementations. Therefore, it has to be programmed and configured by the tool owner or manufacturer based on the adaptor template.

The template consists of components providing the following functions:

- Network connectivity module receives/sends messages from/to the tool according the used network protocol.
  Templates for REST, SOAP and RSS connections are 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 CIS (this step may be bypassed if the tool already uses the appropriate standard).
- Standard translator replaces proprietary key values and enumerations by standardized ones and vice versa, based on translation 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 …) to form a correct standard message.
  (Do not confuse with the semantic annotations provided by the Semantic Box which are based on mapped taxonomies.)
- EDXL DE generator assembles the parameters for the EDXL Distribution Element that envelops all messages distributed in CIS. The template will provide a minimum set of default values that might be extended by the developer of the CIS connector. I.e. security related parameters can be added dependent on the message content.
- Filtering of received messages based on EDXL DE parameters.
  Filters might be extended by the developer of the CIS connector also based on the message content.
- Logging, for debugging purposes only.

3.2.2. CIS Core

The CIS Core is provided by the CIS Product Owner and can't be modified by the CIS members. It manages central CIS features, partly based on the EDXL DE parameters transferred:

- Authentication assures that incoming messages originate from a trusted partner application, according to the service registration.
- Authorization services control the flow of information and protect sensitive data from unauthorized access. Appropriate encryption mechanisms are defined and implemented in the CGOR concept (see sections 2.2.4 and 3.5).
- Validation of the transferred messages assures the formal correctness and application of standards. Improperly formatted messages will be rejected.

- EDXL DE Wrapper packs the information into an EDXL Distribution Element (envelope) that adds meta-information to the payload message.

Additional Core functions which were not implemented in the prototype could be:

- Object Buffer function stores large binary objects (message attachments) in an accessible store (e.g. FTP server) and replaces them by the URI in the message.
- Value Added Services (optional plug-ins) may make use of the transferred information e.g. for message logging, auditing, reporting or statistics.

3.2.3. CIS Distributor

In the proof of concept, the distribution mechanism implementation matches the peer-to-peer communication architecture described in D5.2 [2]. Therefore, it has following features:

- There are 2 REST interfaces: one that sends message, another that receives them.
- It can send a message either to one or several members of the same CGOR at a time
- The sender's distributor accepts an EDXL-DE-wrapped message from its CIS Core and addresses it individually to any recipient distributor provided it is part of the same current CGOR.
- The message sending is made asynchronous so the sender does not expect immediate response. Yet, a timeout exception triggers itself if a receiving distributor does not acknowledge reception within the 5 minutes following the message dispatch.
- The receiving distributor acknowledges the reception of EDXL-DE message regardless of their ability to process the content of the message as the sender does not care if the recipient fails to process the message once it is delivered.
- Each sent and/or received message is stored in a document database handled at distribution level only. This message storage database was implemented in case a synchronization mechanism will be added for previously lost messages (e.g., because a connected receiving tool was offline) (see 5.1).

3.2.4. Semantic Box

The Semantic Box implementation in the PoC prototype matches the description made in deliverable D4.4 [8]. Its role consists in translating concepts (words) between sender's and recipient's taxonomy (official set of words used by responders). The link between 2 concepts from distinct taxonomies is called a semantic relation. Therefore, it is composed of 3 main components:

The Semantic Matching Web Service is a SOAP Web Service which exposes methods to:

- receive standard messages (e.g. CAP) and then:
  - validate them against the specifications
  - identify relevant semantic concepts within the messages structure, or hashtag-annotated semantic concepts from free text (e.g. #Fire) inside the messages
- group the identified semantic concepts in a "mapping set" (JSON object), and forward them to the semantic translation service

The Semantic Box must be extended in case of additional standards to be supported in CIS message content.

The Semantic Repository Wrapper Service is a micro service that welcomes as input a JSON-formatted mapping set from Semantic Matching Web Service, builds a SPARQL query form these concepts and submit the query to the semantic repository hosted by the JENA server. From the JENA server response, the Semantic Repository Wrapper Service returns to the Semantic Matching Web Service a new mapping set containing all the initial concepts, their equivalence(s) in recipient taxonomies along with their semantic relation.

The Semantic Repository is the storage part of the semantic functionality. It contains all established mappings (i.e. semantic relations) between concepts from different taxonomies represented as triples *(concept) - [semantic relation]-> (concept equivalence)*. These triples were assembled and formatted in an ontology file on the Desktop Protégé software. The resulting ontology file was afterward uploaded on an Apache JENA server where it can be consulted using SPARQL queries.

The preparatory steps (population of the EPISECC Taxonomy, further population of the Semantic Repository with common taxonomies and cooperating organisations' terminologies, and Semantic mapping between cooperating organisations' concepts and the EPISECC taxonomy) are realised by the EPISECC technical team using Protégé Desktop tool [20] for taxonomy schemas creation and population, and for mapping of concepts from different taxonomies. The content in the Protégé tool is then transferred to the Semantic Repository, which is a Triple Store (TDB) realised using the Apache Jena Framework [21].

3.3. Sharing Information

The following sequence diagrams Figure 9 and Figure 10 show flow of information between the CIS Adaptor components.

The interface to the Tool is individual and must be implemented in the Connector. It may be REST, SOAP, Java integration or any other interface technology. The internal connections between all other components are implemented as REST services (details in deliverable D5.2 [2]).

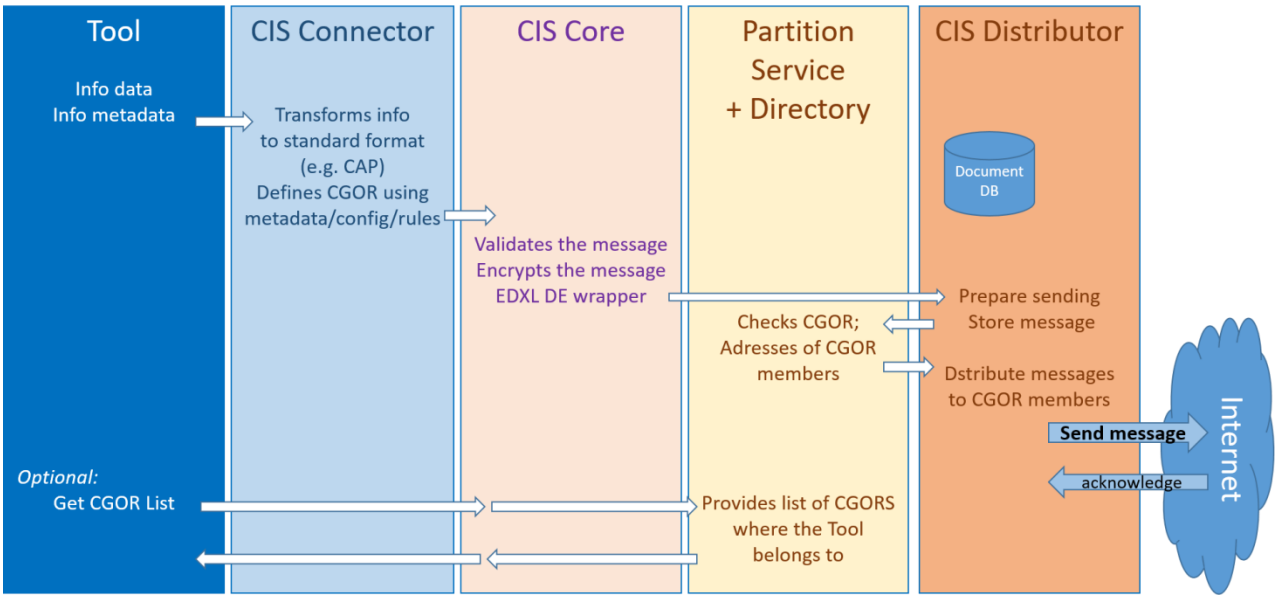

Figure 9: Sending information to CIS

The Core must define the CGOR where the message is addressed to. This can be implemented using static parameters in a configuration file, or dynamically by a rule engine evaluating information metadata or content. In the specific case of tools supporting the CIS distribution feature, the CGOR can also be defined by the Tool user.

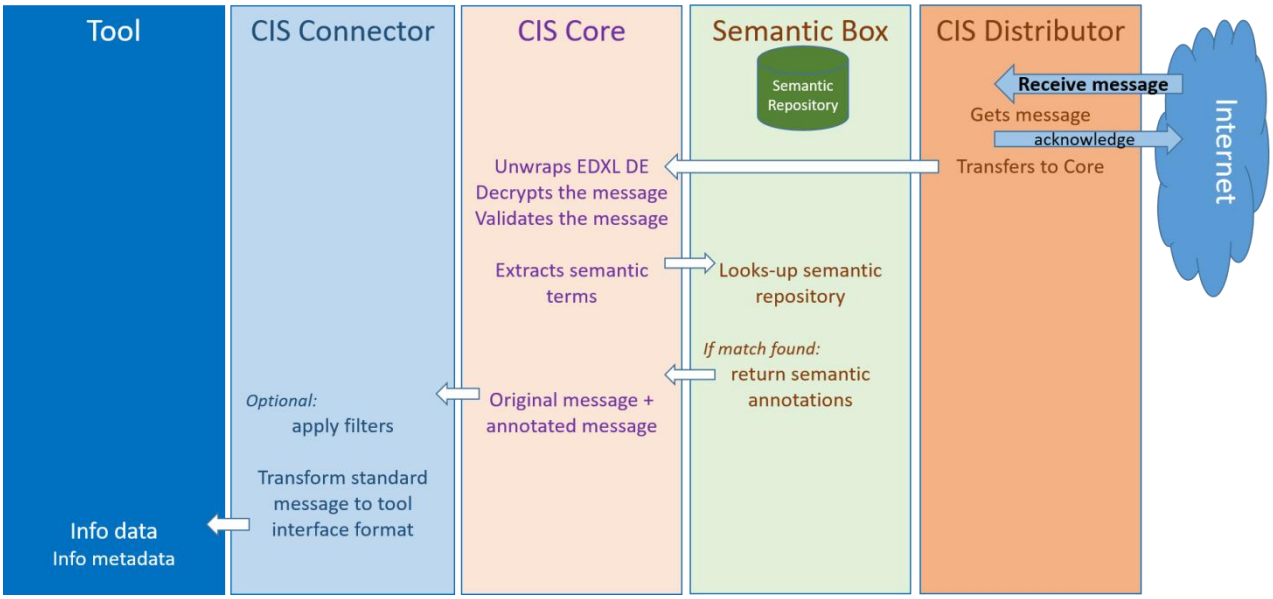

Figure 10: Receiving information from CIS

When a message arrives from CIS, the distributor requests the callback interface of the CIS Core to the partition service. Once the partition service provides callback URL, the EDXL-DE message is forwarded to its associated CIS Core for processing.

The Core queries the Semantic Matching Web Service for requesting semantic interpretation, dependent on the used standard. If semantic annotations are retrieved, the Core transmits both, the original and the annotated message to the Connector.

The Connector must be programmed in a way to handle the transmitted information appropriately so that the Tool can use them. This information handling can also include filtering dependent on message content or EDXL DE parameters set by the sender. Amending the standards used in CIS, message profiles (defined sets or values of standard parameters) may be agreed upon between the CIS participants.

3.4. TETRA terminal/user identification in EPISECC CIS

TETRA addressing is based on the traditional telephony network addressing principles: full ITSI phone numbers, with country (MCC), network (MNI) codes and local number (SSI). TETRA standard does not define any relation of that local number to URL´s or other IP based identifiers. Country and network codes can be converted to country names and network names, publicly known across countries. TETRA local addresses are based on ISSI space: MCC-MNC-SSI number and also optionally on MS-ISDN number with similar structure. There is also an entity of ASSI: Associated identification, related to the ITSI, but used in a terminal instead/in addition to the ITSI ASSI is a phone number as well. In case of TETRA migration (terminal to migrate to another network), it is given a visitor associated identification, V-ASSI: intermediate identification for the migrating visiting TETRA terminal. None of these numbers relate to any IP network addressing/numbering principles or the emergency protocols, considered in EPISECC. Evidently an URL can be created based on the ITSI number and ITSI based URL can be converted back to ITSI number, but it does not provide any further mnemonic information of the identification.

In existing TETRA networks, the ITSI space has been divided to different organisations, differently in different countries and networks. No standard relation of ITSI addresses/address ranges to the organisation name/role or user space is standardised. Each TETRA network allocates the ITSI numbers to different terminals of the user organisations in its own way, as defined by the network administrator.

In TETRA systems, the usual way of indicating the user is the TETRA terminal phone book, that usually associate a mnemonic name to a TETRA terminal ITSI, phone number. Management of the phone books is outside of any standardisation; TETRA user organisations or users update their terminal phone books manually or by programming tools. Across TETRA networks and user organisations, no common agreement of mnemonics exists. Each organisation defines its phone book mnemonics in its own way.

In summary to relate TETRA user identities to EPISECC defined protocols (CAP, EDXL, EMSI), there is no standard, no automatic or any simple way as:

- TETRA standard does not support TETRA user/terminal identification based on semantic names, organisations or resources. Harmonisation of TETRA addresses to semantics is too late, as fragmentation has already taken place and it is not possible to change the address space in use.
- TETRA radio interface signalling is optimised for minimal delay: amount of data over the air: there is no TETRA air interface signalling for alphanumeric or textual identification. Only way is to transfer ASCII characters over the air is to use short messages
- TETRA network gateways may add their own user/terminal identification information, but no standard way to couple with standard TETRA terminal addresses exist
- TETRA phone number could be mapped (by a mapping table) to CAP callout message ID/sender ID, or to EMSI RESOURCE ID/ORG/NAME/TYPE.
- CAP and EMSI have also a number of mandatory fields that are not known TETRA entities. Should some dummy values to be used?

For EPISECC implementation, to identify TETRA users/terminals in CIS, each TETRA to CIS adapter needs to include a conversion table of TETRA standard addresses and/or proprietary GW identifiers to the CIS supported protocol identifiers. This has to be built to each adaptor or GW, that supports standard TETRA terminals.

In case, that the CIS adaptor is integrated as part of a Control Room /dispatcher application, other TETRA terminal/unit associated resource information, if included in the Control Room application, may be then mapped to the CIS supported protocol (CAP, EMSI) RESOURCE related elements (RESOURCE identifiers, organisation identifiers, unit name, type and resource capabilities). In this case, another independent CIS connected application could resolve these unit identity and resources, related to the TETRA terminal associated unit, entering the incident scheme and also identify its associated TETRA ITSI address. In the EPISECC demonstration a TETRA network integrated Control Room system was not used, but a gateway (MDG), that only identifies the TETRA terminal ITSI and converts it to MLP protocol MSID field.

In EPISECC CIS, not supporting MLP or TETRA protocols, MLP identifier MSID (indicating originating/destination TETRA terminal ITSI) is to be mapped to EMSI RESOURCE /ID, (string of max 80 characters, containing the full TETRA ITSI address) or CAP CALLOUT MESSAGE ID. Airbus MDG converts the SDS/LIP message to an MLP supported short/positioning messages, that associates the TETRA identities (TETRA ITSI´s of sending and receiving parties) to MLP identifiers. Based on MLP identifiers, the MDG CIS Adaptor needs to subscribe to TETRA terminal for services which include location reports (based on reporting interval and/or reporting distance), short data (SDS) messages to/from TETRA terminal and status (registration state, emergency state, etc.). Service subscription is in this case made based on the EMSI RESOURCE/ID that is converted to MLP MSID address. MDG is to provide the MLP protocol based AVL and text messages to the CIS adaptor, based on the above subscription. The CIS adaptor is to map the MLP address to the resource identifier of the used CIS protocol (EMSI or CAP). If CIS supports directly MLP protocol, no conversion to CAP or EMSI is needed. A tool specific identifier conversion table from/to every TETRA network or Control Room

application, using TETRA services in each adaptor or GW is to be developed. This is outside of EPISECC scope. Identification of CIS adaptors (adaptor IP addresses), adaptor discovery to find the peer CIS adaptor and management of the CIS connections between the CIS adaptors, are as defined in EPISECC, but not related to above TETRA terminal identities.

3.5. CIS member and CGOR administration

Existing emergency management tools do not include the concept of Communication Groups Online Rooms (CGORs) for dynamic group building, therefore an additional administration service, the "EPISECC Administration Interface" was developed during the EPISECC project, which can be seen in Figure 11. The administration interface is based on a client web application for configuration of the CIS-Adaptors. Its purpose is to establish and manage the CGORs for tools, which have no dedicated feature implemented to manage CGORs themselves.

CGORs are similar to emailing lists. They serve as sub-groups composed of CIS-participants, who exclusively share information between a subgroup of stakeholders involved in crisis- and disaster management. These subgroups are involved in the management of one specific incident or recurring types of emergencies/events. This fact concludes that the organisations have to be in a list of stakeholders of the CIS during the preparation phase, therefore before any emergency event happens. After the event occurs, CIS participants can create CGORs and invite other participants to share information on this specific CGOR (a specific mission or a specific event). When a CGOR is created, a distribution list (like a mailing list) of all the CGOR-members is created and maintained by the CGOR creator, who has the administration rights for this CGOR. This list is updated in case a new member is added or removed. The distributor component of the CIS-adaptor enforces the access rights of the CGOR. For every dedicated CGOR, the Distributor has a list of the CGOR-members and distributes the information only to the list members.

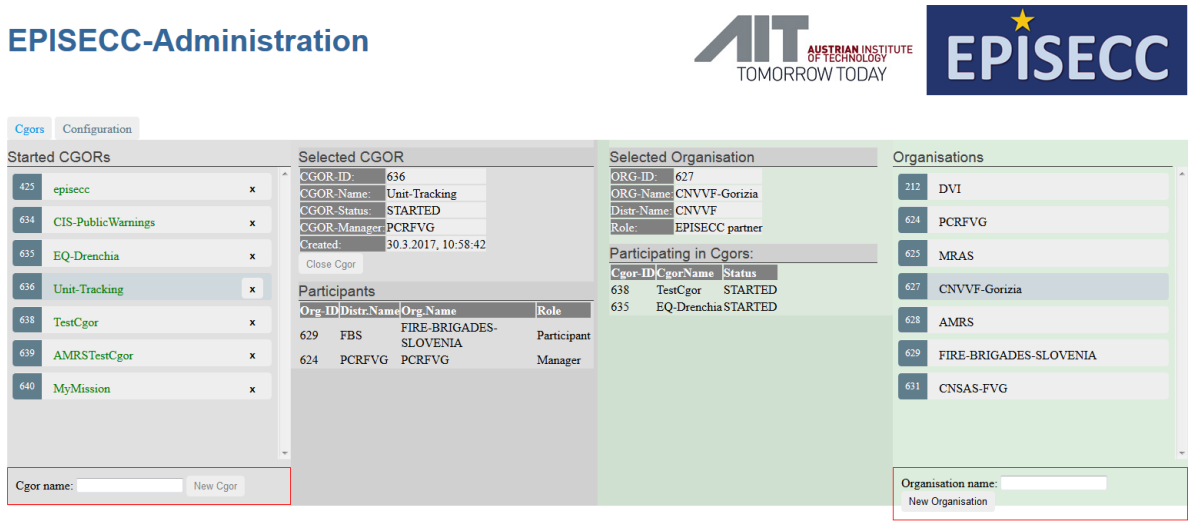

Figure 11: EPISECC Administration Interface

Every specific CGOR has at least one administrative member (creator), whose rights are:

- adding, inviting and removing CIS-members to the CGOR,
- closing the CGOR,
- editing CGOR-member rights.

CGOR-member rights are:

- accepting/rejecting of invitations,
- send information to the CGOR,

  receive information from the CGOR.

The EPISECC Administration Interface has connection to the local CIS Adaptor. The interface can be used to display the list of participating organizations and the list of enabled CGORS. All CGOR operations (creating CGORS, inviting members, accepting invitations, removing participants, closing a CGOR) as described above can be initiated by this tool, this guarantees seamless information exchange of stakeholders in crisis- and disaster management via established connections during specific events.

4. Lessons learnt - CIS architecture and function

4.1. CIS Prototype and Proof of Concept – achievements

4.1.1. Connecting tools to CIS prototype

Developing the CIS components, implementing CIS Adaptors and connecting the tools of EPISECC project partners, defining the message content and profiles with respect to the PoC exercise scenario, adapting some tools for the use of CIS, and compiling the semantic repository was an iterative process that encompassed parts of WP4, WP5 and WP6. A broad spectrum of CIS functionality could be covered with the **tools of EPISECC partners** in the prototype:

LifeX COP (Frequentis): common operational picture tool prototype, collecting all information from CIS and sending alerts and incident information to CIS by adaptors integrated in the LifeX COP backend (Java integration of Connector and Core). A CGOR interface was implemented in the tool which allows the user to send information (CAP messages) to selected CGORs.

DISP (HITEC): mission oriented operational picture (adapted product) that can receive and send alerts (CAP messages) and receive device positions (MLP messages). Every CGOR is related to one mission (event that is displayed for the user). DISP implemented a deep integration of the Segmentation service and mission handling.

Jixel (IES): incident management tool used by the Italian fire brigades CNVVF for cross regional communication of major incidents. Jixel directly shares CAP messages with CIS, the required CAP profile is handled in a Connector component integrated in Jixel itself. CGORs where information has to be sent are selected by the Jixel tool operator during message preparation. Jixel features were also extended with the implementation of an Inbound REST API, in order to be able to receive CAP messages from other CIS participants.

MDG (Airbus): product linking TETRA network to the Internet. Adaptors were developed for sending device positions and receiving CAP messages which are forwarded as text messages to the addressed devices (profile requires the device IDs in the CAP Addressees field).

WI-MoST (HWC): mobile communication tool demonstrating the information wrapping security concept. Wrapped information is only accessible between WI-MoST clients; all other CIS participants get only the unwrapped parts of the information of CAP messages via CIS.

In addition to the EPISECC partners, third party tool providers were invited to join the final PoC exercise. It should be demonstrated that we fulfilled the requirement to easily connect existing tools with limited efforts based on the EPISECC Connector template. The tools Planning&Response from Intergraph and Ruatti Commander from Ruatti Systems were checked and no technical impediments were identified. Nevertheless, Intergraph and Ruatti Systems did not join the EPISECC PoC for non-technical reasons.

Thankworthy, Teleconsult Austria agreed to participate voluntarily with their tool **SARONTAR**. SARONTAR is a map-based mission control tool for mountain rescuers (see Figure 12), deployed and in use at the Austrian Mountain Rescue Services in the province Styria.

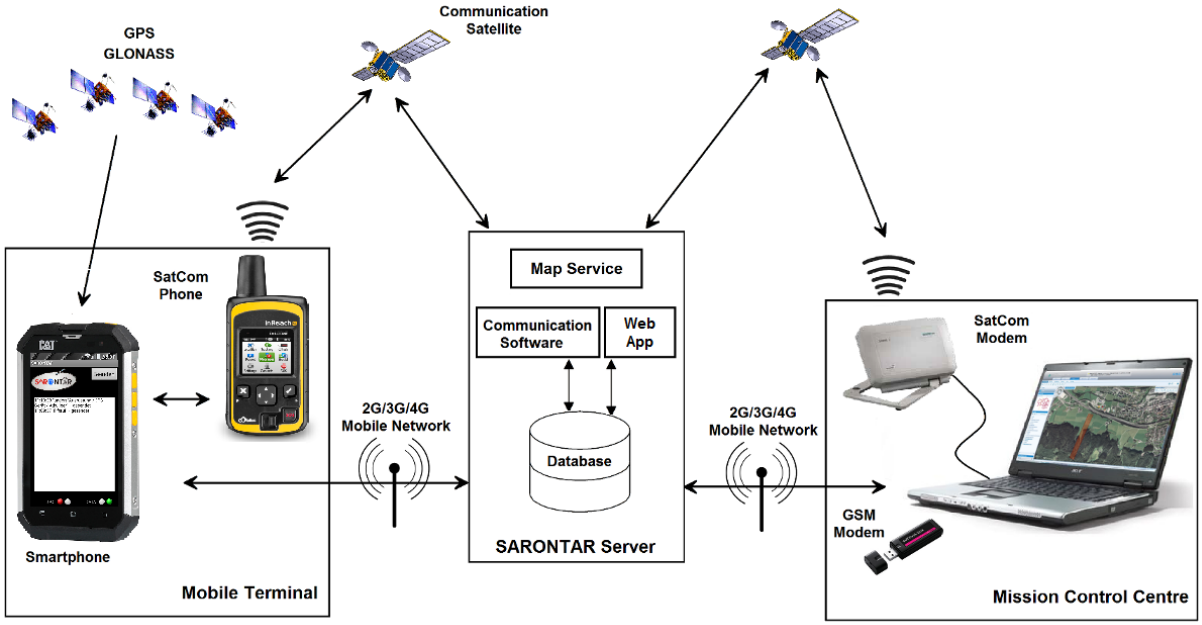

Figure 12: SARONTAR mission control in Alpine regions

Teleconsult set-up a test server and mobile field devices, exposed their interfaces as REST services and installed the CIS components. Frequentis built the Connector to the SARONTAR interface and supported with the deployment and tests. Altogether, it took about 4 days for Teleconsult and one week for Frequentis to integrate SARONTAR in the CIS and make it ready for the PoC. During the PoC, Teleconsult successfully participated with their server and two field devices and was seamlessly integrated into the CIS and the exercise in Palmanova, Italy.

This shows that the CIS concept effectively supports the communication of legacy tools with reasonable efforts that can be spent in the preparation phase of the disaster management life cycle.

4.1.2. Insights during PoC exercise

A detailed description of the proof of concept, the evaluation process and the results is given in deliverable D6.3 [5].

Evaluations usually built up upon qualitative and quantitative data. A qualitative evaluation describes the participant's individual (subjective) feedback and thoughts concerning the effectiveness, advantages/disadvantages etc. of the provided solution whereas a quantitative analysis is based on recorded (objective) data such as processing times to handle different tasks. The results from a quantitative analysis may allow comparing the performance of processing tasks (for instance by using support tools), but requests availability of adequate reference data.

During the PoC, several participants were involved in the evaluation process and their expertise was used as input as shown in Figure 13:

- Evaluators being people that are explicitly assigned to fulfil that role,
- Observers being other visitors or guests that might be asked questions by us or asked to complete a questionnaire (e.g. group of visitors from different emergency services from Slovenia),
- Staff being people from contributing beneficiaries that moderate the feedback sessions, the final discussion round, questionnaire hand out etc.

The aim of the evaluation in the context of the Proof of Concept is to validate the concept as well as the demonstrator of the CIS developed in the frame of the EPISECC project. Apart from proofing technical functionality it is imperative to analyse how the concept of connecting different operative tools already applied in daily routine in the CIS is received by practitioners, operators, end-users or other stakeholders. Since there was no focus on evaluating individual technical functionalities of the different IT tools, a quantitative analysis seemed not appropriate for the given task and turned out to be not practicable due to missing robust reference data from common handling processes. Thus, a qualitative-based assessment composed of 4 steps was chosen for the evaluation: observations, flash feedback, discussion, and questionnaire.

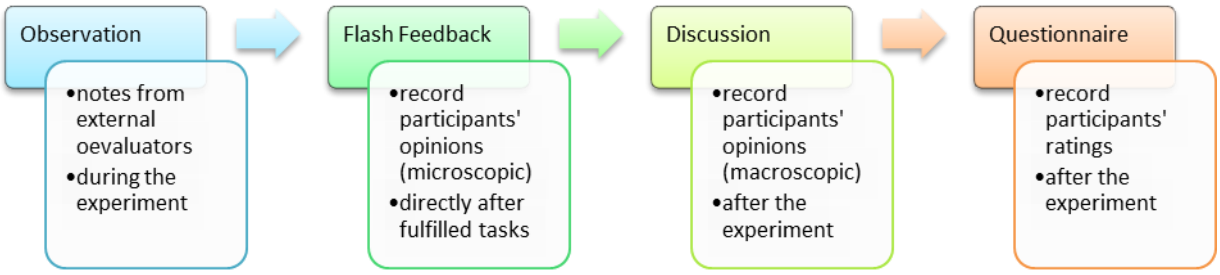

Figure 13: Evaluation methodologies used in the EPISECC Proof of Concept

Figure 13 gives an overview on the assessment technologies used and gives a short description of the metrics and sequence of execution of the methods.

To analyse the evaluation, notes were taken during all four evaluation steps. After analysing the notes for the observation and the flashlight feedbacks, no major issues dedicated to the CIS architecture or other technical issues were made. The feedback given by all evaluators were addressing the overall functional usage of the CIS concept.

Based on the detailed analysis of the complete evaluators' feedback, the results of all four steps the final statements of all evaluators could be summarized as,

- "… very promising approach…",
- "… very successful concept…",
- "… impressive opportunities offered by the CIS…",

- "… I am impressed by the solution for information exchange across borders…" and
- "… we have seen an excellent tool."
- "… excellent software…"

The results from the evaluation process show on the one hand that the evaluators saw the provided solutions as an important support for interoperability with the meaning of cross boarder and cross organisational information exchange in crisis management, and on the other hand that some improvements have to be implemented with regard to technical, organisational, legal and political aspects to guarantee more reliable and feasible implementation in the day-to-day work flow of organizations active in disaster response.

All evaluators liked the provided solution. Within these statements the evaluators commonly agreed that the CIS has demonstrated the potential to improve processes in crisis management.

The suitability and relevance was seen for the solution by all evaluators. This means that every evaluator rated the CIS as good enough for rapid, informed and appropriate decision making as well as useful and helpful. Furthermore, it was stated within the evaluation panel discussion that the usage of CIS offers the opportunity to use additional information sources and to share / exchange information more easily. The elimination of the need for information translation was considered as one of the great advantages of the CIS. The evaluators agreed on the fitting of the CIS in existing processes.

It was common sense amongst the team of evaluators that all of them could imagine to use the CIS in crises and disaster situations. 80% of the evaluators stated that the CIS provided the usage of additional information within the demo. All evaluators believed that this has improved the operational work during the demo.

The efficiency was enquired by the following questions:

- Did the used additional information improve your work?
- Would you say that you could finish the tasks faster with the help of the provided solution?
- Was faster situation awareness possible?

The answers given by the evaluators showed that the additional information used improves the work (see Q7).

Two third of all questionnaires comprised the confirmation, that tasks could be finished faster by using the CIS. Furthermore, nearly all questionnaires stated that faster situation awareness was given.

All in all, the CIS is improving the efficiency in crisis management operations!

Concluding the evaluation process the evaluators highly appreciated the CIS concept and were convinced by the added value CIS is offering for first responders operating in crisis and disaster situations. They recommended to bring the CIS into operational use and to keep the CIS simple and focused on the main functionality a robust interoperability of information exchange. All evaluators commonly endorsed to institute the CIS in the crisis management.

4.2. Decisions made during the prototype implementation

Several architectural decisions were influenced by feedback of Advisory Board members and by the experience made during the prototype implementation. Some decisions concern only restrictions for the PoC prototype and don't give direction for a general CIS architecture.

4.2.1. Standards used in PoC

The CIS concept identified several standards for information interoperability (see section 3.1). The prototype implemented only MLP for sharing device positions and CAP for sharing information about the events.

We skipped the use of EMSI which would provide much more powerful features for automated information processing due to the complexity of the standard and the lack of suitable interfaces exposed by the considered tools. It seems that a comprehensive and complex standardisation of information would require more specific tools to be handled.

The CAP standard however was sufficient for the information sharing in the exercised scenario. The PoC exercise sowed that almost all content was transmitted as human-readable text rather than automatically processed parameters. The introduction of a CAP profile for CIS that offers some additional parameters would help with specific requirements, e.g. addressing CGORs and classification of information.

4.2.2. Information distribution mechanism

Two different ways of message distribution were considered at the beginning of WP5:

- Message Bus or Enterprise Service Bus. There are several open source middleware platforms for secured messaging available, e.g. Open MQ or Apache Kafka. On the one hand, using such middleware would provide important features for secured transactions, scalability and stability. On the other hand, it would require a central messaging server that must be set-up and maintained by some authority and that would be a single point of failure in the CIS architecture.

  The CGOR concept can be implemented by dynamic message queues. Every Collaboration Group Online Room is represented by one message queue where the CGOR members are subscribed.
- Peer-to-peer messaging architecture. The message routing is managed decentralized. Every CIS participants runs a Distributor in his server which communicates with the other participants' Distributors. The central Directory and Partition Service can be replicated to every Distributor; so, the CIS works even in case of partial network interrupt. The transaction mechanism is replaced by mutual synchronisation between the distributors. The CGOR mechanism is implemented by the Segmentation Service and secured by CGOR specific encryption of messages.

The consortium decided to implement the peer-to-peer message transfer for the PoC prototype. The reason was the recommendation from the Advisory board to avoid the need for a central organisation that needs to invest in server infrastructure and maintenance services. Furthermore, a central node where all messages have to pass-by and that would stop the CIS function in case of network interrupt was not recommended.

4.2.3. Distributed architecture and central services

Despite the decentralised peer-to-peer message distribution, there are still some central services necessary: The Directory Agent managing the CIS participants and their organisations, the Segmentation Service for the implementation of CGOR and data ownership concepts, and the Semantic Repository and Semantic Services providing the semantic interoperability. The CIS Service Provider must make available these services to all CIS participants.

All these services in the prototype were implemented as central services, accessed via the internet at runtime. If such central solution shall be avoided, it would also be possible to replicate and synchronize all needed data to every CIS participants' server and to run the services offline in the CIS environment of every participant.

4.2.4. Information ownership and security

Another central service that was skipped in the prototype is the encryption service which provides certificates together with the accepted CGOR invitations. In the prototype, the messages shared in a CGOR were not encrypted. The routing of shared information was implemented only by lists of addressees in a CGOR gained from the Segmentation Service. For the PoC, we decided to provide rather visible features of tools and communication than invisible and hardly to demonstrate information security topics.

The Information Wrapping concept which hides parts of shared information depending on user roles and defined information security policy was implemented only within the WI-MoST tool because it would have been too complex and too specific to define a common policy and to implement the information wrapping as a global method in CIS Core.

4.2.5. CIS deployment

In our concept, we intended to provide a fully distributed system where the adaptation chain (Connector, Core, Distributor + Directory structure and Directory Agent) will be totally hosted in each partner's premises.

During our several test sessions, only the Core and Connectors were hosted on each partner's side. All the distributors, along with the directory structure and directory agent were held in HITEC's premises.

Regarding the distributed aspect of our solution, we finally decided to keep the distributors on HITEC's servers also for the PoC. It relieved each partner of potential network infrastructure

configuration issues and made it possible to monitor the entire communication during the tests and the exercise. Further explanations are provided in the alternative concepts, chapter 5.5.

4.3. Legal and ethical impacts on CIS

Legal compliance is a quality aspect of ICT tools for PPDR organizations. It is reasonable to expect that only tools that were designed to conform to applicable regulatory measures, such as standards and laws, can be adopted by PPDR organizations. Designing data flows within the CIS is important for the legal (sometimes referred to as regulatory) compliance purposes.

4.3.1. Identification of CIS participants

Beyond the technical capability for automated data sharing, trust between the partners and confidence in data security and integrity is key for the acceptance and willingness of organisations to share their information. A context aware and configurable security concept is integrated in the CIS architecture. The trust policy requires the registration and certification of the CIS participants.

Communication Groups and Online Rooms (CGOR) can be established dynamically according to current communication needs, and only the trusted and accepted participants are able to read or publish the information circulated in a CGOR.

For the sake of legal certainty, the CIS Service Provider should only accept qualified electronic signatures and certificates. The regulation (EU) n° 910/2014 [5] distinguishes between different kinds of electronic signatures; qualified signatures being the ones with the highest degree of bot technical and legal certainty. The security requirements imposed on qualified signatures are much higher than the standards that apply to other electronic signatures. Given the sensitivity of the data that could be processed within the CIS, it is wiser to choose for a qualified electronic signature. The annex I of the regulation determines the specific conditions that any qualified signature should fulfil. The Regulation also introduces the concept of 'Electronic Seals' which allows to sign as a legal entity. This might also be of interest to CIS users.

We opt for using the services of a Qualified Trust Service Provider (QTSP) who issues the signatures, rather than an own internal CIS trust procedures. It would be too cumbersome to incorporate the requirements needed to guarantee the identity of the persons joining the CIS within the CIS framework itself.

[5] The Regulation (EU) n° 910/2014 of 23 July 2014 on electronic identification and trust services replaces Directive 1999/93/EC to which is referred in section 2.6 of Deliverable 5.3 on operational interoperability. This final Deliverable was elaborated on the new Regulation.

4.3.2. Data ownership in CIS

A sensitive point is the ownership of data and information to be shared in CIS. To ensure the quality of information it is recommended to clarify the responsibilities of the engaged actors/organizations. The practice shows that better information quality is ensured if actors own the data they generate and create. The attribution of data ownership also may help to answer questions about the control of the information flow, the cost of information, and the value of information.

By design, all business logic and the ownership of information stay with the CIS member organisations and their tools participating in information sharing. The common information space itself does not create, own or process the data. It is not a central data repository, but just an information broker that distributes information that was released for sharing with defined partners.

EPISECC CIS is based on distributed processing implementation by peer to peer architecture. This means that there are no dedicated servers and clients, instead all processing responsibilities are allocated among all the machines that that are considered to be peers. To become a peer an entity needs to register as a CIS member. This architecture ensures that there is no centralised data storage or information gateway which could become a single point of failure or a target of cyber-attacks, leaking sensitive or protected data. In fact, the information to be shared stays in the domain of the data owner and the implemented authorization and data protection concept guarantees that every piece of information is only accessible by authorised participants.

Nevertheless, there are critical aspect of potential tampering of the meaning of information during the transformation of the tool interface data to standard messages and the amendment of received messages with semantic annotations (functions of the CIS adaptors). Therefore, we strongly recommend running detailed tests when linking new tools to a CIS, and to validate carefully any new taxonomy used for semantic transformations.

4.3.3. Audit trail of information flow

Wikipedia [9]: "*An audit trail (also called audit log) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. Audit records typically result from activities such as financial transactions, scientific research and health care data transactions, or communications by individual people, systems, accounts, or other entities.*"

Chronological logging of the information flow in CIS was suggested by end users and in the 2nd project review. It is very useful for the analysis of the progress of a critical situation and the evaluation of the collaboration of responders. Furthermore, it may be relevant as an evidence in case of political debates or juridical interventions after a disaster.

As there is no central CIS data store, and CIS has no means to access any data that were not sent as a message by the owner, there is no reason for auditing more than the message traffic in CIS.

The decentralized architecture of CIS is a big advantage with respect of data ownership and confidentiality but prohibits a single comprehensive auditing of all messages. There is no single point where all messages would pass by and so no central message logging is possible.

But the adaptors of every tool keep record of all sent and received messages in a local database within the Distributor. This database is situated in the protected network of the CIS member and cannot be accessed from outside due to information security reasons. That means that it would be very easy to show the own message log for every organisation and to create reports on the message transfer by organisation. Such reports can be requested from the organisation providing the picture from the organisation's point of view. Combining all logging reports would give the complete picture of the information flow in CIS.

5. Alternative and not implemented concepts

During work package WP5, some features and concepts were discussed and elaborated by the project partners which could not designed in detail or implemented and evaluated in the PoC prototype due to time and effort limitations. These features are not needed for the scenario played in the PoC exercise and for the given tools but they are considered as helpful and even necessary in different situations for an operative CIS implementation.

This chapter summarizes these ideas, explaining the expected benefits. It shall save the efforts made for developing the solution concepts and give an outlook to additional features and properties which might be beneficial in the future.

5.1. Information synchronisation, re-sending and queries

A synchronization mechanism could allow CGOR members to recover for lost messages following network interruption or permit newcomers in the mission to catch up with the whole course of events.

For this purpose, such functionality might be implement at partition and distribution level. In fact, the distributor is designed to save any incoming or outgoing message in a document database.

For performance issues, we assumed that CIS participants would like to request by themselves only the missing part they are interested in instead of retrieving large sets of messages which may cause information duplication or loss. This implies the possibility to negotiate content retrieval between two partners, one labelled as a “supplier” while the other being a “supplicant”.

To track whether the message is received or not, we associated the distributor’s acknowledgement to a proof of delivery. Thus, any unacknowledged message is flagged “NOT DISTRIBUTED” by the sender’s distributor. Therefore, implementing a synchronization service consisted in scanning all undistributed messages that were to be sent to partners in the network, expose them to potential “supplicants” and only resend those requested.

Yet, during the implementation phase, several questions arose:

- Since this feature is on demand, how can we give control to tool’s user?
- Moreover, how can we ensure that all the partners are able to receive old messages sometimes with past expiration dates? Indeed, the message flow shall remain unchanged, which implies that the retrieved messages still flow from supplicant distributor to its core, and finally reach his tool. For example, HITEC’s DISP tool back then was rejecting messages whom sent date was past for over 10 minutes using the classic EDXL-DE support. If other tools had this issue, was it worth to remove such logic constraints and risk the spread of past information?
- Besides, how to model the exchanges between supplicants and suppliers having only EDXL-DE messages formats? Basically, how to represent the need of specific messages based on a sequence number or time slots from partner tool?

Although we found viable solutions for some of these questions, we preferred to shift our priorities to focus on message consistency between senders and receiver in CIS.

5.2. Service registry and exploration

5.2.1. Service registry to discover internal services

As the CIS implementation unfolded, we aimed to communicate in a more dynamic fashion. Indeed, CIS components like distributors, core or connectors all had fixed addresses when the remote testing phase started between the partners. These fixed URL addresses were first hard-coded in the application before being moved to configuration file. Since all the CIS components were developed as microservices, it was more natural to use load balancing frameworks to keep the services going in case one service falls. This principle was explained in deliverable D5.2 unterhalb[2] chapter 5.2.2. Therefore, adding a service registry allows to navigate between the CIS services without never worrying about neither their addresses nor their names, even when they are load-balanced.

The service registry was implemented at distribution level only. This implies that a distributor relies only on the name of a service (Core, partition or recipient distributor) to address it.

5.2.2. Service discovery at partner level

Beside the internal service discovery, it was also intended to expose business services to partners through a service registry. For example, if a partner had a service capable to predict an earthquake in a specific area, and propose close shelters or escape routes, the wanted to offer the possibility to open such service to other CIS partners.

This part was abandoned because it requires too much adaptation for each partners' tool.

5.3. Information wrapping and security policy propagation

Wrapped information is defined as a containment of information set and its context-dependent management policy. The policy may include functional capabilities and its main functionality is to provide access controls for the information set.

The information wrapping concept and its application in the CIS was discussed. The EPISECC prototype however implemented one example of wrapped information sharing with the tool provided by HWC. Wrapped information as instantiated in the EPISECC project, uses the attribute based access control concept to control access to the information. It provides a layer of security that is separate of the layer provided by the CGOR.

The benefits of the wrapped information are that it can be used to offer end-to-end encryption, since the information is "wrapped" – encrypted – instead of point-to-point. It offers more flexibility and extra layer of control, as will be described in this section.

5.3.1. Applying wrapped information scenario in CIS

A “Disaster Victim Identification” team personnel is involved in disaster response operation. The team has the task of identifying victims of the disaster. They need to exchange information in between team members as well as with other parties such as LEMA. Messages that contain victim identifying information must be kept strictly confidential and not to be shared or ‘leaked’ with non-authorised individuals. In this scenario, the DVI team members is issued personalised portable devices (Smart phones/tablets). Each device has set of attributes installed on the device proving that

1. An attribute proving membership of the DVI team
2. An attribute corresponding to rank of the person issued the device

During a disaster, the DVI team shares information in the form of CAP-messages with other organisations on the same CGOR. When a DVI team member sends a CAP message that includes identifying information of the victims, he/she can select to wrap these specific information- i.e encrypt the selected information- such that the wrapped information can only be decrypted on connected devices with the authorising attribute (i.e. being member of the DVI team in this example). The decryption key is available only to the DVI team devices since they have the attribute of DVI team membership. Devices connected to the DVI team CGOR but without this attribute installed, would receive shared messages but would not be able to decrypt the attribute-encrypted part of the message.

The benefit in this scenario is that an extra layer of access control is given back to the DVI team members, with the added flexibility in to select information elements to encrypt, while achieving an end-to-end protection in the process.

5.3.2. Attributes types

There are three types of attributes can largely be categorised into

1. Subject Attributes: subject is the individual (human or process) who/which is accessing the shared information. Subject attributes may be the subject role, job title, clearance, training, etc.
2. Contextual Attributes: These describe the environment which can include the time, location, device used for access. For example, access may be allowed only within a Geo-fence (On field, control room, etc.), within defined time, or from only customized devices.
3. Resource attribute: The resource in CIS is so far the shared information. Resource attributes may include the type of information (medical record, personal identifiable information), the classification or sensitivity

The type of attribute sometimes may affect how the attributes can be managed- i.e. created, obtained and revoked. In the EPISECC project, the attributes that are used can be regarded as a combination of both subject and contextual.

5.3.3. Integrating Wrapped information with CIS

Wrapping and unwrapping of information is done using a Wrapping-tool that can is inserted as a proxy either on the device level or at the CIS-core component. When the wrapping-tool is used on a device level -as in the case described in the above scenario-, the information is protected from device to device (end-to-end). However, such deployment is separate from the CIS and will require customization for the devices running the external tools. If the wrapping-tool is installed in the CIS-core, information is protected only to the CIS-core and any connected tool to the CIS-Core will be able to access the information unfettered.

During the project demonstration, the wrapping tool is inserted on the device level, to show case end-to-end security.

An important requirement is that tools and CIS-core should be able to receive wrapped information as well as access the unwrapped parts of the information without having to have a wrapping tool installed. This is achieved by inserting the encrypted 'original' message as a payload in another plaintext 'carrier' CAP message. The carrier CAP message contains the following

- Information elements from the 'original' CAP that the sender did not wrap
- Information elements that describe that payload is encrypted
- An encrypted payload

All tools without the Wrapping-tool will be able to view the 'carrier' CAP message, but will not be able to decrypt the 'payload'. Devices with the Wrapping-tool installed AND have the authorizing attribute will be able to decrypt the payload and see the full contents of the original message.

5.4. CGOR properties and attribute based message routing

The CGOR concept (see 2.2.4) allows the segmentation of the common information space. That means that a message can be sent only to a restricted group of recipients (members of a specific CGOR). In this concept, it is crucial to define the appropriate CGOR for every sent message. That must be implemented in the Connector, specific for every tool and dependent on operational requirements of the organisation owning the information.

Two mechanisms are implemented in the CIS prototype, a third one is outlined on conceptual level.

- Fixed CGOR configuration: The default CGOR can be configured for each tool in the Config file that is processed during start-up of the Connector. In the same way, additional CGORs can be configured for specific purposes of the tool. The Connector addresses the messages accordingly (sets the CGOR name into the EDXL DE parameter in the REST call to the Distributor).
  The disadvantage of this simple solution is that the potential CGOR names must be predefined before the tool is connected to the CIS and the communication is started.
- CGOR-aware tools: The Partition Service provides – via the Core – a function that lists all CGORS where the organisation has joined-in (see 3.5). Tools can create a user interface to this list, and the tool user can select the appropriate CGOR for the information to be shared.
- Automatic rule based message routing (not implemented in the prototype, see section 5.4)

- When accepting a CGOR invitation, the Admin tool shall enable the participant to define CGOR properties which can be used for rule based selection of target CGOR for messages. The properties are specific for every participant, according to his needs and conventions.

  The Connector can implement a rules engine that uses the CGOR properties together with defined parts of the message to find the right CGOR, e.g. or classified messages:
  if SCOPE=RESTRICTED than select CGOR with PROPERTY1="Confident"

5.5. System administration simplification

Due to the distributed nature of our solution, we packaged the CIS Distributor, directory agent and the directory structure (partition) in containers that could be portable and launchable form partner premises instead of concentrating all the distributor on HITEC's servers (the previous testing configuration). The Docker containers were packaged with security certificates to allow partners to join a private ad hoc network that could be mounted on a private mobile hardware like HITEC's NOSACO(R).

Due to the lack of visual administration tool, along with the problems of synchronizing tools through their distributors, this packaging solution required thorough networks skills to set up, along with basic knowledge of containers management. This set up was not deemed ergonomic for partners, especially in case a network issue occurs and no IT-qualified partner is available to solve the problem. We decided not to use it to avoid adding complexity and failure points to our proof of concept.

Anyway, a handy package solution should be created in a productive rollout scenario.

6. Conclusion

Starting from the vague idea of information sharing in an heterogenous environment and based on the results of the WP3 – Pan-European inventory of disasters, we analysed the requirements of decision makers and stakeholders in European disaster management. We concluded that we have to design an architecture enabling easy and cost-efficient data sharing between legacy tools and existing data sources. The information shall be understood and interpreted by tools and personnel of different domains and languages, and information security, confidentiality and integrity must be granted.

The technical WP5 partners AIT, FRQ, HITEC, HWC, IES started an iterative design process and defined step by step a SW architecture which is able to fulfil the requirements and which also includes the results of WP4 – Taxonomy building. The iterations were presented to the consortium, the advisory board, the reviewers and on international symposia (see WP8). The feedback we gained from the stakeholders triggered and influenced the further iterations and gave us direction to usable and valuable solutions.

In parallel to the architectural design, the technical partners started the prototype implementation (task T6.2). This gave us confidence that our theoretical draft can be converted into concrete software solutions and be tested in a realistic scenario. Vice versa, the experience with the SW implementation were beneficial to the architectural design and helpful for finding solutions that can be deployed.

Although not all architectural concepts had been implemented in the prototype due to time and effort constraints, the CIS installed and exercised in the final PoC fulfilled the requirements bearing from the scenario. It provided meaningful information exchange between the different tools and responder organisations during the exercise, and was assessed in a very positive way by the practitioners acting as evaluators and the involved first responders.

The ideas, concepts, designs and components developed during the EPISECC project and lined-out in this deliverable build a solid basis for the deployment of a common information space that will be able supporting European disaster management on cross-regional, national or even European level.

Potential business cases for putting the concepts into operations are elaborated in WP9 – Exploitation. Anyway, the request for proposal and the order placement must come from interested parties in charge of crisis prevention and disaster management.

Bibliography

[1] EPISECC deliverable D5.1 – Protocol and Network Interoperability, 2016

[2] EPISECC deliverable D5.2 – Information Interoperability, 2016

[3] EPISECC deliverable D5.3 – Operational Interoperability, 2016

[4] EPISECC deliverable D6.2 – Proof of Concept Implementation

[5] EPISECC deliverable D6.3 – Validation by End Users

[6] EPISECC deliverable D4.2 – Taxonomy model, 2016

[7] EPISECC deliverable D4.3 – Data model, 2016

[8] EPISECC deliverable D4.4 – Ontology model for the EPISECC use case, 2017

[9] Wikipedia
https://en.wikipedia.org/wiki/
[accessed July 2017]

[10] OASIS open standards consortium
https://www.oasis-open.org/
[accessed 8 Sept. 2016]

[11] OASIS Emergency Management TC, EDXL DE V 2.0 standard draft, 2012
http://docs.oasis-open.org/emergency/edxl-de/v2.0/csprd02/edxl-de-v2.0-csprd02.odt

[12] OASIS Standard, Common Alerting Protocol Version 1.2, 2010
http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.doc
[accessed 8 Sept. 2016]

[13] CEN, "CEN Workshop agreement CWA 15931, Disaster and emergency management – Shared Situation Awareness", 2009.

[14] ISO, TR 22351 Technical Report: Societal security - Emergency management - Message structure for exchange of information
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57384
[accessed 8 Sept. 2016]

[15] OMA (Open Mobile Alliance)
http://openmobilealliance.org/
[accessed July, 2017]

[16] OGC (Open Geospatial Consortium)
http://www.opengeospatial.org
[accessed 8 Sept. 2016]

[17]OGC, Sensor Model Language (SensorML)
http://www.opengeospatial.org/standards/sensorml
[accessed July, 2017]

[18] Open Source Geospatial Foundation, GeoServer software server
http://geoserver.org/
[accessed 8 Sept. 2016]

[19] Ka-Ping Yee, PFIF 1.4 Specification, 2012,
http://zesty.ca/pfif/1.4
[accessed 8 Sept. 2016]

[20] Protégé free, open-source platform
http://protege.stanford.edu/products.php
[accessed 8 Sept. 2016]

[21] Apache Jena open source Java framework
https://jena.apache.org
[accessed 8 Sept. 2016]