Establish Pan-European Information Space to Enhance seCurity of Citizens

D6.2. – Proof of Concept Implementation

Grant agreement number:	**607078**	**Date of deliverable:**	**M27**
Date of project start:	**2014-06-01**	**Date of submission:**	**2017-05-23**
Duration of project:	**2017-10-31**	**Deliverable approved by:**	**TCCA, TUG**
Lead Beneficiary:	**FRQ**		
Contributing Beneficiaries:	**Airbus, AIT, HITEC, HWC, IES, KULeuven, UNIST**		

Executive Summary

According to the Description of Work, the Proof of Concept (PoC) seeks to validate and prove that the results achieved in WP 4 (Taxonomy and Ontology model) as well as WP 5 (Architecture of common information space) give a helpful answer to the persisting problems related to interoperability. The suggested taxonomy and common information space (CIS) architecture should be demonstrated to be self-consistent and should build the base for further improvements in cooperation of Civil Protection authorities, first responders, and other involved stakeholders.

The consortium jointly developed a software prototype, implementing the concepts and architecture provided by WP4 and WP5. Tools of EPISECC partners and of external parties, which are actually used by responder organisations, are sharing information, using the CIS adaptors. Semantic services enable the mutual understanding of information exchanged cross language and culture barriers between the organisations involved in disaster response. The data protection concept allows to establish sub-groups of CIS participants (Cooperation Group Online Room CGOR) who exclusively share information between the stakeholders involved in one incident (need to know principle).

This CIS prototype together with the connected tools will be tested in the final PoC exercise with representatives of civil protection authorities and responder organisations, in order to evaluate the concepts developed within the project, including also procedures for the set-up and administration of a CIS in case of a cross-border disaster. A scenario was designed that shows different levels of interoperability and information sharing between crisis managers and responder organisations from several European countries.

Before going into the final PoC exercise with end-users and practitioners, several tests and validations were performed internally – a Dry Run of the prototype and a fruitful discussion of the EPISECC concepts in the Advisory Board in Vienna, several online test sessions between the SW developing partners, and a dry run of the final prototype and the scenario steps on-site in Palmanova.

Based on these experiences the plot and the evaluation grid for the final PoC exercise were elaborated.

Table of Content

List of Tables

List of Figures

List of Acronyms

Abbreviation	Description
AB	Advisory Board
AMRS	Austrian Mountain Rescue Service
CAP	Common Alerting Protocol (OASIS standard)
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CGOR	Cooperation Group Online Room
CIS	Common Information Space
CIS DA	CIS Directory Agent
CM	Crisis Management
CMCS	Civil-Military Coordination Section
CNSAS	Mountain Rescue Italy (Corpo Nazionale Soccorso Alpino e Apeleologico)
CNVVF	Italian fire brigades' association (Corpo Nazionale dei Vigili del Fuoco)
COP	Common Operating Picture
DISP	Disaster Information Sharing Platform
DVI	Disaster Victim Identification Team Italy (fictive unit)
EDXL	Emergency Data Exchange Language (family of OASIS standards)
EDXL DE	EDXL Distribution Element (message envelope)
ELSI	Ethical, Legal, and Social Implications
EMSI	Emergency Management Shared Information (ISO/TR 22351:2015)
EUCP	European Civil Protection mechanism
FFAS	Fire Fighters Association Slovenia
GIS	Geographic Information System
JSON	JavaScript Object Notation
ICT	Information and Communication Technology
LEMA	Local Emergency Management Authority
MDG	Mobile Data Gateway

MLP	Mobile Location Protocol
MRAS	Mountain Rescue Association Slovenia
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
PCRFVG	Protezione Civile da Regione Autonoma Friule Venezia Giula
PKI	Public Key Infrastructure
PoC	Proof of Concept
PPDR	Public Protection and Disaster Relief
REST	Representational State Transfer (Web service interface)
SA	Situational Awareness
SOAP	Simple Object Access Protocol
UN-OCHA	United Nations Office for the Coordination of Humanitarian Affairs
USB	Universal Serial Bus
WI-MoST	Wrapped Information Mobile Sharing Tool
wMDG	wireless Mobile Data Gateway
XML	Extensible Mark-up Language

Introduction

This Deliverable D6.2 describes how the EPISECC Proof of Concept (PoC) is implemented and organized. It is based on the PoC design given in D6.1 [1] and the results of WP4 taxonomy building and WP5 architecture of Common Information space (CIS). It documents the results of Task 6.2:

- the planning and set-up for the final PoC exercise and the evaluation of the results;
- the implemented software prototype to be used in the PoC exercise;
- the utilization of the developed software, concerning Ethical Legal and Social Implications, operational interoperability, and testing.

This document does not repeat the CIS architecture, semantic models, operational concepts, and general PoC design but rather documents the actual implementation of the prototype and its intended use in the PoC exercise.

Section 1 *Proof of concept planning and execution,* describes the preparatory tasks, the scenario design, the evaluation process and the set-up of the PoC exercise. It represents the planning base for the final Proof of Concept event in Palmanova on May 10-11, 2017. It specifies how the prototype shall be used during the PoC scenario in order to evaluate the CIS concept and operational interoperability during the set-up and execution of a CIS-based disaster response. Several verification tests and validation steps taken during the course of the project are documented in section 2.

Section 3 *CIS prototype implementation* focusses on the proof of the CIS, based on the CIS architecture specification given in D5.2 [2]. The prototype was designed in order to enable the tests of the main CIS concepts during an exercise with disaster management practitioners. It comprises the CIS central components, the CIS adaptors and the tools of the participating organisations which are integrated to the Common Information Space. Furthermore, it consists of the Semantic Repository with the taxonomies of the involved organisations and the mapping to the EPISECC taxonomy, and the Directory agent with the meta-data of the CIS participants. The Admin tool enables to administrate the security and data ownership concept of Collaboration Group Online Rooms (CGOR). Protocol & network interoperability is demonstrated by the interactive integration of mobile and simulated fixed TETRA infrastructure, and the seamless integration of tools with mobile device (tablet, smart phone) clients.

The implementation of legal and ethical requirements is outlined in chapter 4, based on the future General Data Protection Regulation and a concept of Controller-processor agreements and informed consent.

Finally, chapter 5 summarizes in brief the steps that organisations have to take to enable their participation in a common information space and to join a collaboration group in case of a disaster.

1. Proof of concept planning and execution

1.1. Goals

This chapter includes an overview on the multiple targets of Task 6.2 of EPISECC. Basically, the main focus is to show that all results and assumptions achieved in the preceding deliverables from the work packages 2, 3, 4, 5 and 7 of EPISECC are consistent and complete. Moreover, it has to be shown that the existing IT solutions such as the information processing systems Mobile Data Gateway, LifeX COP, DISP, WI-MoST and JIXEL provided by the EPISECC partners Airbus, Frequentis, HITEC, HWC and IES are integrated to the EPISECC Common Information Space. In addition, it will be shown that the IT solution SARONTAR from an external contributor can be integrated, too.

Based on the first stage description of the PoC of EPISECC which is documented in Deliverable D6.1 [1], the final description of the PoC planning and execution is provided in this report. It is the aim of the validation phase to proof the developed concepts in a functional exercise and to verify the main hypothesis about the impact of the EPISECC projects (see also Chapter 5.1 of Deliverable D6.1):

"The developed system will improve inter organisational collaboration by facilitating information exchange and assessment across organisational borders."

Specifically, it is the intention to show that syntactic and semantic connection of the above mentioned C2 and other systems can be accomplished. However, also physical interoperability aspects are covered.

The first stage exercise set up was described in chapter 7.2 of Deliverable D6.1. The plot of the unexecuted FVG40^{exe} exercise served as basis for the EPISECC set-up. It is a substantial target of this report to show the final PoC Set-Up. Compared to the first stage set-up, several revisions were made due to recommendations of members of the Advisory Board and also because of technical and organisational developments that took place since the submission of Deliverable D6.1. As a consequence of these recommendations and developments, the former EPISECC episodes of D6.1 were also adapted, the description of the revised scenarios is therefore a fundamental part of this report.

Chapter 5 of Deliverable D5.3 [4] includes key indicators for interoperability. These indicators are integrated in the concept of the evaluation process for the Proof of Concept. It is the intention to develop methodologies and criteria on how to evaluate the performance of the EPISECC demonstrator.

The final PoC is the last step of several consecutive validation steps for the concept of the Common Information Space that started in 2016. These preceding tests will be described both from a technical perspective as well as from the perspective of end users provided predominantly by members of the EPISECC advisory board.

1.2. Set-up of the event

1.2.1. Venue

The PoC will take place in Palmanova in Italy (Figure 1) at the regional operations centre of the civil protection authority of Friuli Venezia Giulia (PCRFVG, see Figure 2). PCRFVG, as a member of the Advisory Board of the EPISECC project, is highly interested in the CIS and the related interoperability concepts developed by the EPISECC consortium and therefore offered its facilities for the PoC event.

Figure 1: Location of Palmanova

Figure 2: Centro Operativo Regionale PCRAFVG

The structure of the PoC event and the various tasks that will be performed by different groups of participants present challenges with respect to the assignment of rooms at the PoC venue. Since the PoC will be segmented (see section 1.2.2) in different sections the participants of the PoC will be situated according to their designated roles in different locations and relocate in the course of the event. PCRAFVG has made a set of rooms available within the centre to meet the following specific demands of the event:

- Introductions to the EPISECC project and the PoC event
- Briefings of participants and observers
- Realistic command and control environment for playing a disaster scenario
- Separation of national and international responder organisations
- Remote observation possibilities for the scenario play
- Break out rooms for evaluators and observers
- Panel discussions

The rooms and their allocation in the operations centre are shown below in Figure 3, Figure 4, Figure 5 and Figure 6.

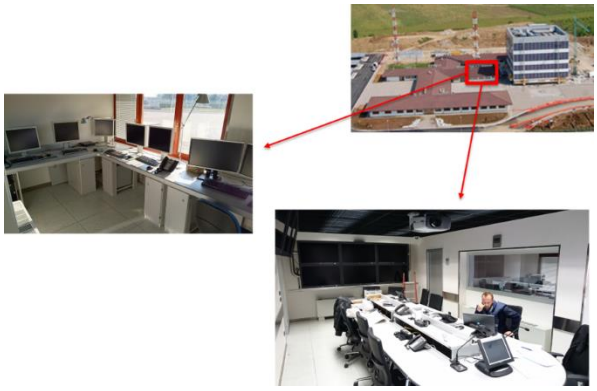


Figure 3: Operations room (small)

Figure 4: Operations room (large)

Figure 5: Conference room

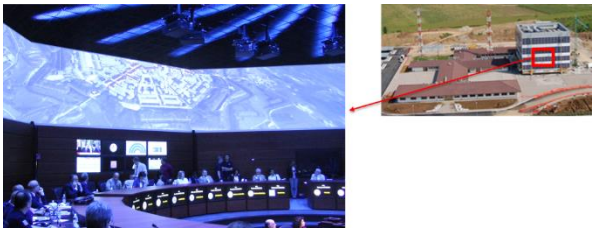


Figure 6: Conference and situation room

1.2.1. Participants

It is anticipated that the PoC event will involve approximately 100 persons in total. These persons can be segmented in the following groups:

- EPISECC consortium members
- Scenario players
- Evaluators
- Observers/Guests
- Other staff

EPISECC consortium

The consortium will be present at the PoC event en bloc with approximately 25 persons. Dependent on their role in the consortium these persons are

- Promoting the concepts and aims of the EPISECC project
- Playing an active part in the scenario (e.g. operators of information management tools)
- Directing the scenario play and the related activities
- Facilitating the evaluation process
- Guiding observers and guests
- Facilitating the event logistics

Scenario players

The scenario (see section 1.3) will be played and facilitated by the following organisations:

Table 1: Scenario players in the PoC event

Acronym	Full name	Role	Supporter (tool)
PCRAFVG	Protezione Civile Regione Autonoma Friuli Venezia Giulia	Local emergency management authority (LEMA)	FREQUENTIS (LifeX COP)
CNVVF	Corpo Nazionale dei Vigili del Fuoco – Fire Fighters Italy	Responder	IES Solutions (JIXEL)
CNSAS	Corpo Nazionale Soccorso Alpino e Apeleologico – Mountain Rescue Italy	Responder	HITEC LUXEMBOURG (DISP)
AMRS	Austrian Mountain Rescue Service	Responder	TeleConsult AUSTRIA (SARONTAR)
MRAS	Mountain Rescue Association Slovenia	Responder	HITEC LUXEMBOURG (DISP)
FFAS	Fire Fighters Association Slovenia	Responder	AIRBUS DEFENCE & SPACE (MDG - TETRA)
DVI	*Disaster Victim Identification Team Italy (fictive unit)*	*Responder*	HWCommunications Cyber Security and Resilience (WI-MoST)

The participating authority and the responder organisations will be supported by the technical partners of the EPISECC consortium that are going to provide their information management systems as tools to be used. In addition to that AIT provides an administration tool for the common information space that can be accessed and used buy every organisation participating in the PoC event.

With Teleconsult Austria an external software provider will show the interoperability of its information management system SARONTAR which is used by the Austrian Mountain Recue Service.

To address and show the aspects of information security in the course of the PoC scenario play in general it was decided to introduce an artificial responder with special requirements in that field – the disaster victim identification unit. Its information exchange will be treated with special

information security protocols by the Wrapped Information Mobile Sharing Tool (WI-MoST) provided by HWCommunications.

Evaluators

To ensure a proper and qualified evaluation of the presented concept and the related impact on the operations of the organisations involved in the PoC scenario a team of external evaluators has been nominated. Some organisations that have a seat on the Advisory Board of the EPISECC project have appointed experts from their organisation (different to the person sent to the advisory board) to act as neutral evaluators. In addition, international experts in the field of crisis and disaster management (CRDM) have been invited to join the team of evaluators.

Table 2: External evaluators

Name	Organisation	Professional background
Katja Banovec Juroš	Administration of the Republic of Slovenia for Civil Protection and Disaster Relief	Department for Informatics and Communications
Ingrid Nordström-Ho	United Nations Office for the Coordination of Humanitarian Affairs (UN-OCHA)	Head of the Guidance and Norms Unit, Civil-Military Coordination Section (CMCS), Emergency Services Branch (ESB)
Gudrun Van Pottelbergh	Europe Conflict and Security Consulting	Humanitarian Affairs Officer at UN-OCHA (ret.); Operational Support Officer at OSCE (ret.);
Franz Petter	City of Hamburg - Authority for the Internal and Sports	Fire service operations department
Helmut Aschbacher	Austrian Red Cross	IT services and staff work; Expert for civil-military cooperation in the Joint Forces Command of the Austrian Armed Forces; Expert within the EUCP mechanism;
Johannes Vallant	Austrian Fire Brigade Association	Disaster management branch, expert in communication and warning systems; Expert within the EUCP mechanism;

Günter Hohenberger	Provincial Government of Styria	Head of the provincial warning center Expert within the EUCP mechanism;

To promote the EPISECC project and its contents as widely as possible the PoC event is arranged in a way that enables further professionals from the crisis and disaster management domain to join and follow the scenario executed by the participating organisations. Approximately 50 persons are expected to follow the PoC event on the main day as additional observers/guests.

1.2.2. Agenda

The entire PoC event is planned to last from May 9th to May 12th in 2017. The first and the last day are reserved for internal project procedures such as preparatory activities, internal feedback and consortium meeting. The timetable of the PoC event is as follows:

Table 3: Timetable May 9th

Time	Topic	[E][1]	[P]	[X]	[O]
09:00 – 20:00	• Preparing the location in Palmanova (IT) • Set-up of the equipment in Palmanova (IT) • Preparing the location in Nova Gorica (SLO) • Set-up of the equipment in Nova Gorica (SLO) • Testing				

Table 4: Timetable May 10th

Time	Topic	[E]	[P]	[X]	[O]
09:00 – 12:30	• Arrival of scenario players • Final preparation • Final testing				
12:30 – 14:00	• Lunch • Arrival of evaluators				
14:00 – 18:00	• Introduction to EPISECC				

[1] [E] EPISECC consortium, [P] scenario players, [X] evaluators, [O] observers/guests

	• Introduction to the PoC event • Introduction to the scenario • Briefing of scenario players and evaluators				
19:30	• Social event – dinner in Palmanova				

Table 5: Timetable May 11th

Time	Topic	[E]	[P]	[X]	[O]
08:30 – 09:30	• Registration				
09:30 – 10:00	• Welcome speeches • Official group photo				
10:00 – 12:00	• Proof of concept scenario play				
12:30 – 14:00	• Lunch in Palmanova				
14:00 – 15:30	• Evaluation panels with scenario players and evaluators				
15:30 – 17:00	• Exhibition of the participating information management tools by the technology partners • Exhibition of the main EPISECC concepts by the consortium members (open space and parallel sessions)				
17:00 – 18:00	• Forum discussion on future aspects and application of the EPISECC common information space and the related concepts				
19:30	• Social event – dinner in the vicinity of Palmanova				

1.3. Scenario

1.3.1. Starting situation

The original scenario formulated in the DOW in combination with the plot of the (unexecuted) FVG40^{exe} exercise in 2016[2] served as basis for the development of the scenario for the EPISECC PoC. The starting situation for the EPISECC scenario is defined as follows:

> *On May 11th 2017 at 09:59 local time an earthquake is happening in the province of Udine in the region Friuli-Venezia Giulia.*
>
> *The epicentre is located in the municipality of Drenchia at the coordinates 46°10'16.1"N 13°37'32.5"E.*
>
> *The earthquake has a magnitude of 6.2 at a depth of 10.54 km.*

This earthquake has fatal impact on the whole region including Italy, Slovenia and Austria. The main operational area for the operations performed by the responders within the EPISECC scenario is the border region between Italy and Slovenia at the cities of Gorizia and Nova Gorica. The cascading effects relevant for the EPISECC scenario in this area are:

- Collapsed buildings
- Rock falls
- Obstructed roads
- Fire in commercial areas
- People trapped under the rubble
- Injured people
- Fatalities

1.3.2. Operating sites

In Goriza (IT) three different operating sites will be involved:

- Fortress of Gorizia
- University Centre of Gorizia
- Commercial area in Gorizia

In Nova Gorica (SLO) one operating site will be played:

- Commercial area in Nova Gorica

The operating sites (see Figure 7) have been chosen based on the requirements arising from the uses cases (section 1.3.3), the storyboard and the 2 hours time frame for the scenario play:

- Cross-border scenario with engagement of international responders
- Integration of field equipment such as radios and smart devices
- Real time tracking of field resources

[2] EPISECC deliverable D6.1 - Proof of Concept design – Final version, section 7.2.2

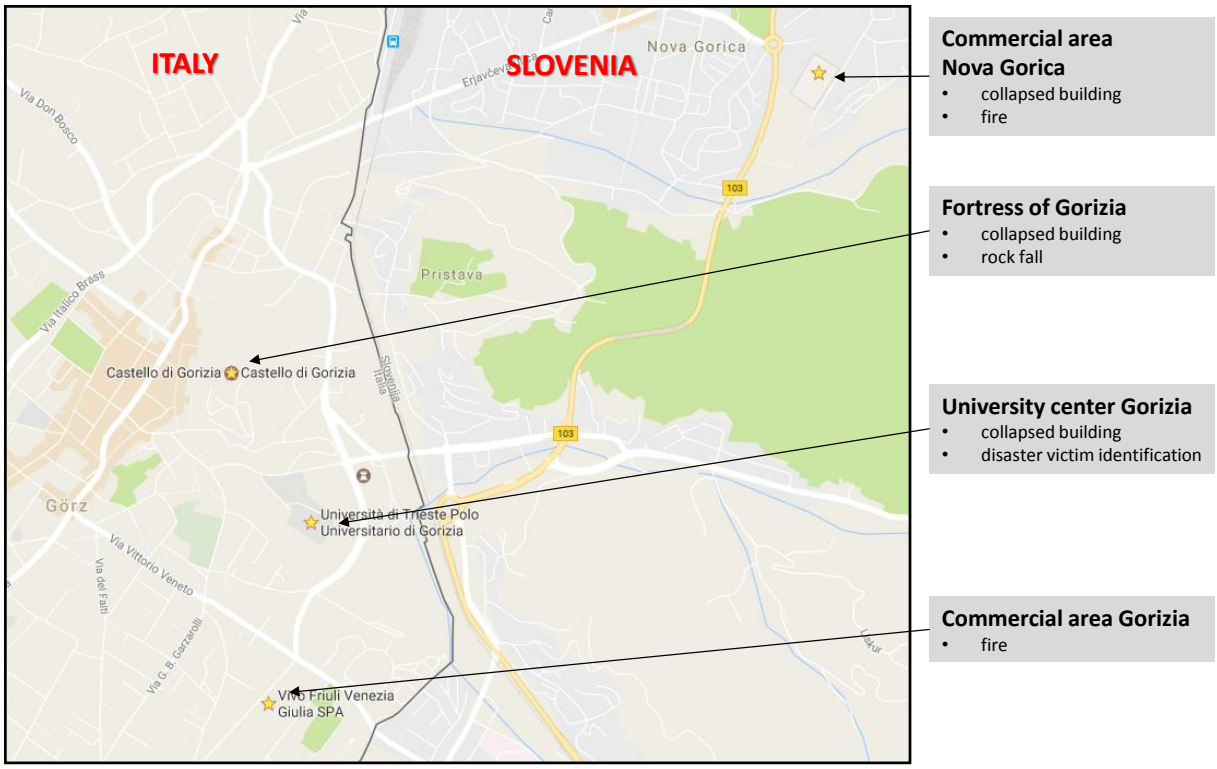


Figure 7: PoC operating sites

1.3.3. Use cases

Use case no. 1

>> PCRAFVG as the local emergency management authority receives early warnings, disaster related data as well as situation assessment information from national responders and prepares a first common operating picture <<

Scenario players in this episode:

- PCRAFVG (Civil Protection FVG)
- CNVVF (Fire Fighters Italy – Gorizia)
- CNSAS (Mountain Rescue Italy)

ICT[3]-tools used in this episode:

- LifeX COP
- JIXEL
- DISP
- CIS administration tool

[3] Information and communication technology (ICT)

The basic course of this use case will be:

1. *PCRAFVG receives earthquake notification from a national alerting system via the common information space (CIS)*
2. *PCRAFVG gets into contact with the local responder organisation in the area (CNVVF)*
3. *CNVVF operations centre Gorizia joins the earthquake related CIS session established by PCRAFVG*
4. *PCRAFVG distributes earthquake related information to CNVVF via CIS*
5. *PCRAFVG issues certain basic request for information to CNVVF via CIS*
6. *CNVVF reports on own operations in the city of Gorizia via CIS*
7. *CNSAS joins the earthquake related CIS session established by PCRAFVG*
8. *PCRAFVG receives real time CNSAS unit positions from smart devices via the CIS*
9. *CNVVF gives a situation update on own operations in the city of Gorizia via CIS*
10. *PCRAFVG shows a first common operating picture on the earthquake operations in Gorizia*

CIS related aspects shown in this episode:

- Administration of the common information space (CIS)
- Interoperability between ICT tools of a different kind
- Semantic treatment of exchanged information provided by the CIS services
- Real time tracking of field units via the CIS
- Common operating picture

Use case no. 2

>> PCRAFVG as the local emergency management authority triggers help from neighbouring countries Austria and Slovenia <<

Scenario players in this episode:

- PCRAFVG (Civil Protection FVG)
- AMRS (Austrian Mountain Rescue Service)
- MRAS (Mountain Rescue Association Slovenia)

ICT-tools used in this episode:

- LifeX COP
- SARONTAR
- DISP
- CIS administration tool

The basic course of this use case will be:

1. *PCRAFVG approaches Austrian and Slovenian authorities for assistance in the earthquake operations*
2. *AMRS joins the earthquake related CIS session established by PCRAFVG*
3. *MRAS joins the earthquake related CIS session established by PCRAFVG*
4. *PCRAFVG distributes earthquake related information to AMRS and MRAS via CIS*
5. *PCRAFVG distributes information about the operations of national responders in the area of Gorizia to AMRS and MRAS*
6. *PCRAFVG assigns AMRS to an ongoing operation in the city of Gorizia*
7. *PCRAFVG assigns MRAS to an ongoing operation in the city of Gorizia*

CIS related aspects shown in this episode:

- Administration of the common information space (CIS)
- Interoperability between ICT tools of a different kind
- Semantic treatment of exchanged information provided by the CIS services

Use case no. 3

>> First responders collaborate in on-site response <<

Scenario players in this episode:

- PCRAFVG (Civil Protection FVG)
- CNVVF (Fire Fighters Italy – Gorizia)
- CNSAS (Mountain Rescue Italy)
- AMRS (Austrian Mountain Rescue Service)
- MRAS (Mountain Rescue Association Slovenia)
- FFAS (Fire Fighters Association Slovenia)
- DVI (Disaster Victim Identification Team Italy; fictive unit)

ICT-tools used in this episode:

- LifeX COP
- JIXEL
- DISP
- SARONTAR
- MDG – TETRA
- WI-MoST
- CIS administration tool

The basic course of this use case will be:

1. *PCRAFVG receives real time AMRS unit positions from smart devices via the CIS*
2. *PCRAFVG receives real time MRAS unit positions from smart devices via the CIS*
3. *PCRAFVG receives real time CNSAS unit positions from smart devices via the CIS*
4. *PCRAFVG includes FFAS in the earthquake related CIS session*
5. *PCRAFVG receives real time FFAS unit positions from TETRA radios in Nova Gorica (SLO) via the CIS*
6. *PCRAFVG updates the common operating picture on the earthquake operations in the border region Gorizia / Nova Gorica*
7. *CNVVF, AMRS and MRAS compile their own operating pictures*
8. *CNVVF reports on own operations in the city of Gorizia via CIS*
9. *MRAS reports on new operations in the city of Nova Gorica via CIS*
10. *CNSAS move to Nova Gorica to support MRAS operations*
11. *PCRAFVG updates the common operating picture on the earthquake operations in the border region Gorizia / Nova Gorica*
12. *CNVVF, AMRS and MRAS update their own operating pictures*
13. *PCRAFVG includes DVI in the earthquake related CIS session*
14. *PCRAFVG assigns DVI to an operation in Gorizia*
15. *PCRAFVG receives real time DVI unit positions from smart device via the CIS*
16. *DVI reports on own operation in Gorizia via CIS (with information security protocol applied)*
17. *PCRAFVG distributes a general warning via the CIS (push message to all CIS members)*

CIS related aspects shown in this episode:

- Administration of the common information space (CIS)
- Interoperability between ICT tools of a different kind
- Semantic treatment of exchanged information provided by the CIS services
- Real time tracking of field units via the CIS
- Common operating picture
- Information security concept

1.4. Evaluation

Validation and evaluation are often used as synonyms neglecting essential differences concerning the assessment level:

- **Validation** is the process of checking whether or not a certain (possibly partial) design is appropriate for its purpose, meets all constraints and will perform as expected. Therefore, it is determining whether the process as (technically) implemented can yield an output that meets the expected requirements / meets specifications with acceptable capability. For validation the process must be challenged using calibrated gauges / verified measurement systems.
- **Evaluation** is the process of computing quantitative information of some key characteristics of certain (possibly partial) design. It is determining whether the process in its entirety can yield an output that meets the desired requirements.

In scope of the present PoC, (technical) validations related to the different tools being part of the overall CIS are assumed as prerequisite due to the fact that these tools are already implemented instruments in day-to-day-business and therefore, must be already validated during their development. Thus, only the evaluation of the entire CIS solution was considered as element of the PoC.

1.4.1. Methodology

Typically, evaluations are built up upon both 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 identifying and comparing the performance of processing tasks by the help of respectively no help of support tools, but therefore presume adequate reference data.

The aim of the evaluation in context of the Proof of Concept is to assess the overall solution developed in scope of EPISECC project and to give a tendency of how the concept of connecting different already existing tools by an overarching architecture is received by practitioners, operators, end-users etc. Since there is no focus on the evaluation of individual technical functionalities of the different 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:

1. Observations
2. Flash Feedback
3. Discussion
4. Questionnaire

Observations are continuous evaluation activities running parallel to the operator's activities. They are meant to monitor the attendee's behaviours, handling issues etc. from an external perspective

during the experiment. The **Flash Feedback** records the participant's opinions at selective times of the experiment. It provides a snapshot of the current thoughts and feelings concerning the solution handling, individual issues or even ideas of what might be improvements of the provided solutions directly after a fulfilled use case during the experiment. The advantage is that a Flash Feedback gives a very personal and direct feedback not distorted from third parties' opinions. On the contrary, the **Discussion** is an open panel where all participants have the opportunity to discuss their individual as well as collective experiences, opinions, questions and so on afterwards. Thus, the discussion provides a more macroscopic or consensus like feedback concerning the overall appearance of the solution from all involved parties. The **Questionnaire** is a paper-and-pencil instrument which collects a conclusive feedback guided by concrete questions on detailed characteristics of the provided solution. It is usually laid out in a semi-structured manner and therefore, enables some kind of statistical analysis by the help of Likert scales and closed questions (i.e. allowed answers are only "yes" or "no"). However, the structured questions will be complemented by open questions with a text box for additional individual feedback from each participant. The questionnaire is handed-out after the experiment.

Figure 8 sums up the used assessment technologies and gives a short description of the metrics and time when each method is executed during the experiment.

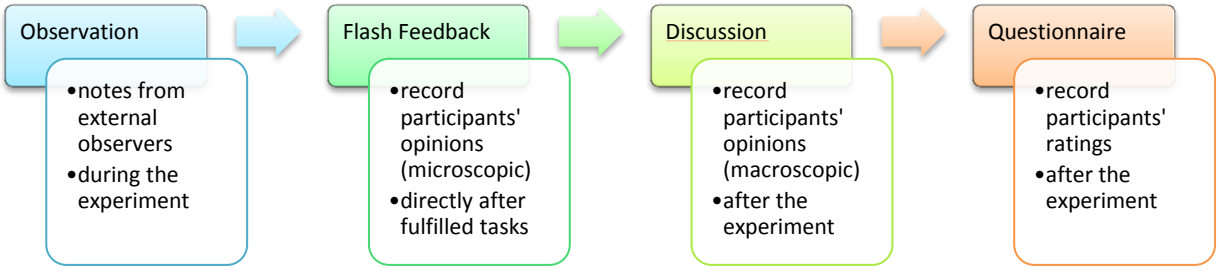


Figure 8: Evaluation methodologies used in the Proof of Concept

For the present Proof of Concept, the temporal sequence of the mentioned evaluation methodologies is scheduled as outlined in Table 6.

Table 6: Evaluation schedule

Time	Topic	Evaluation Methodology
10:00 – 11:45	Proof of Concept: Use Case 1	Observation
		Flash Feedback
	Proof of Concept: Use Case 2	Observation
		Flash Feedback
	Proof of Concept: Use Case 3	Observation
		Flash Feedback
11:45 – 12:00	Evaluation Panel	Questionnaire

14:00 – 15:30	Evaluation Panel	Discussion

1.4.2. Criteria

The evaluation concept is based on a set of predefined success criteria which are adapted to the specified uses cases during the experiment:

- Use Case: Event takes place and solution (CIS) is booted.
  - Reduced time need for set-up of communication
  - Reduced complexity
  - Reduced number of sub processes
- Use Case: Transnational help is activated.
  - Reduced response time
  - Reduced complexity
  - Reduced number of sub processes
  - Increased interoperability
  - Multiplied information channels
  - Supported multilingualism
- Use Case: First responders are supported by CIS information distribution.
  - Enhanced situational awareness
  - Quality of information exchange: timeliness, completeness, comprehensibleness
  - Reduced response time
  - Increased interoperability
  - Improved coordination
  - Supported multilingualism

Since detailed queries are neither scope of the flash feedback/discussion nor the observations, the semi-structured questionnaire addresses those criteria by the following question bunches:

1. Assessment of Use Case and PoC set up
2. Assessment of the interoperability
3. Assessment of the benefits
4. Assessment of semantical perspective
5. Assessment of international perspective

1.4.3. Participants

During the PoC, several participants are involved in the evaluation process:

- **Tool Handlers** being acting people that are assigned to use the tools during the experiment,
- **Evaluators** being people that are explicitly assigned to fulfil that role (cf. Table 2)
- **Observers** being other visitors or guests that might be asked questions by us or asked to complete a questionnaire (e.g. the visitors group from Slovenia),
- **Staff** being people from contributing beneficiaries that moderate the feedback sessions, the final discussion round, questionnaire hand out etc.

1.4.4. Level of representativeness

Given the scope and design of the uses cases with only a small sample size, the results from the evaluation will lack in statistical power and therefore, are not robust in order to generate a general statement. Since a lot of functions as well as the user interface are still at prototype level, the results from the debriefing questionnaire for example will, however, give a tendency of how the concept of connecting different already existing tools by an overarching architecture is received by practitioners, operators, end-users etc. The limitations of this experiment are limitations generally found in comparable V2 maturity level experiments (EUROCONTROL 2010) and also related to any in-field / table-top experiment. In general, the maturity assessment dictates the nature of validation and evaluation and therefore, the level of representativeness and limitations of the experiment's results. In this experiment, the following limitations are identified:

- The results of the experiment are representative for similar tasks under test on the Level of a simulated crisis. Implications are limited to overall conditions, (real-time) traffic conditions and events similar to this evaluation experiment.
- Within the experiment scenario only a small number of possible use cases can be considered. Different application cases are conceivable.
- Due to limited time budget, the experiment scenario will be executed for just one time. Multiple executions will increase significance of the results.
- The limit number of participating professional responders in the evaluation may influence the weight and generalizability of the collected results.

2. Validation steps before final exercise

Before going into the final exercise, tests with selected end-users shall test the technical implementation, ensure sufficient usability of the PoC prototype, and validate the CIS approach – is the CIS usable, is the data protection sufficient is the potentially exchanged information helpful, is the taxonomy in place suitable etc.

2.1. Technical verification

Technical verification describes integration tests performed in order to verify the correct implementation of information exchange between the concerned tools, taking into account information security mechanisms and semantic interoperability.

Since the communication is bi-directional, each partner should check that he is able to both reach its distributor and receive messages from it. The verification procedure happens as followed:

1. The partners ensure they can reach their connector/core from their tool. Each partner is in charge of defining this verification process since it depends on their respective network infrastructure and the connector they implemented to connect to the CIS.
2. The partners that will perform a semantic translation action shall ensure that the semantic service provided by HITEC and the semantic box service provided by IES are reachable and available via PoC network. Each service shall be pinged or reached manually from PoC network to ensure connectivity.

First, any concerned partner shall enable the semantic translation from its connector/core device and define to which taxonomy he expects to be associated:

cis.translate.msg=true – enables message translation from CIS

cis.translate.endpoint=http://taxonomytranslation.iessolutions.eu:3030/TranslationService/services/TaxonomyTranslation/translateCAPToLocal – define the service in charge of semantic annotation

cis.translate.tax.schema=MRAS – Choice of the taxonomy to use when producing or addressing a message to the Mountain Rescue Association of Slovenia entity, called MRAS.

3. The partners verify that the communication between the connector/core - distributor is established. This section is partly guaranteed by design from the connector/core component as the CIS core has a health check feature that cannot start a connector/core unless its configured distributor is reachable and available.
4. HITEC will be specifically in charge of testing the communication between distributors. As they are hosted on their internal servers (see 3.5.5).

2.1.1. Common Information Space tests

The CIS prototype was developed and tested in an iterative way during a long period, starting in parallel with the specification of the Common Information Space architecture (D5.2 [2]). The final modifications were made just before the final proof of concept.

Beside of the tests that every partner performed individually or bi-laterally with the own tools and components and the technical verification described in 2.1, joint tests were run before several major events (synchronisation points) where the EPISECC CIS was demonstrated in front of an audience:

1. 2nd project review meeting in Leuven, July 2016
2. Dry run at Advisory Board meeting in Vienna, November 2016 (see 2.2.1)
3. Conference presentation at Critical Communications Europe in Copenhagen, February 2017
4. FP7 project synchronisation meeting in Brussels, February 2017
5. Dry run of PoC in Palmanova, March 2017
6. Final PoC in Palmanova, May 2017

Preparing these events, the current CIS implementation was tested in joint online meetings using screen sharing (GotoMeeting[4] conferences). These tests followed the intended demo scenario and used the messages to be shared during the demonstration or exercise.

The extended logging functions of the EPISECC CIS components, that were switched-on during tests, helped a lot with error detection and bug fixing. The test results led to further evolvement of the CIS components as well as to improvements of some tools and more accurate taxonomies.

2.1.2. Network interoperability tests

The interoperability between each application connected to the CIS relies on IP technologies. The connection from tool servers to mobile clients is based on public mobile telecom standards (3G).

No specific network tests are required on this level.

The wMDG links the TETRA users to the CIS. It is connected to the TETRA network through a TETRA terminal itself connected to a TETRA base station. The setup of the TETRA system (TETRA network and wireless MDG) is not in the scope of the EPISECC project but affects the PoC prototype and scenario. Therefore, several tests incorporating the TETRA terminals, base station and wMDG were set-up. One major problem is getting the license and radio frequencies for using an own TETRA network in several countries. That is the reason for simulating tracks of TETRA terminals in some cases, and for locating the TETRA users in Slovenia during the final PoC (Slovenia is actually not running any TETRA network we could interfere with).

During the 2nd project review in Leuven and the Dry Run in Vienna, the simulation tool was used. The mobile base station together with TETRA terminals was tested successfully in Paris on the Airbus premises and in the Dry Run in Palmanova. In addition, the direct mode without any base station was an additional option to test the interoperability without the need for licenses.

[4] https://www.gotomeeting.com

2.2. Validation of CIS concepts and prototype by end-users

2.2.1. Demo and Dry Run in Vienna

The demo and dry run took place in Vienna between the 28th and 30th of November, 2016. This dry run was a first occasion to test features and evaluate our interoperability capabilities. The exercise was executed by partners impersonating responders in an earthquake crisis situation defined as following:

- Frequentis by their tool LifeX COP was impersonating the Civil Protection authority for the Region of Friuli Venezia Giulia (PCRFVG)
- IES using JIXEL was playing the role of Fire Brigades from Italy (CNVVF),
- HITEC as portraying the Croatian fire brigade (JVP)
- Airbus was starring as the Austrian Red Cross (ORKHQ) with their MDG gateway and their TETRA devices

Scenario

The scenario depicted an earthquake at the border of Austria, Slovenia and Italy in the Alps mountains.

- The scenario starts when PCRFVG receives an alert through LifeX COP concerning a 6.2 magnitude earthquake that has occurred in Friuli.
- PCRFVG is then designated LEMA and starts a CGOR called GORIZIA to which it invites the fire brigades from both Italy and Slovenia (CNVVF and JVP) using CIS administration tool.
- As CNVVF starts sending reports, The Austrian Red Cross joins the effort in a separate CGOR called TETRA (also managed by the LEMA) and starts sending the positions of its assets. Each message sent by the Italian fire brigade is semantically annotated in English (for the LEMA) or in Croatian (for JVP) and displayed on both tools while the positions sent by the TETRA devices are not translated.
- The LEMA can also address CAP messages to the fire brigades and the TETRA devices for specific warnings.

Perspectives

This dry-run use case is quite similar to the scenario that will be run for the PoC as it involved almost all tools and stakeholder roles that will participate to the final exercise (LifeX COP, JIXEL, DISP, MDG, CIS-Admin). The dry run session allowed all partners to judge their ability to match their tool features and create a collaborative environment where they could exchange strategic information by relying only on their tools.

The general perception of the Advisory Board members was very positive. They registered significant progress in the concepts and the technical implementation of the prototype. The PoC scenario was discussed and practical hints were given in order to adapt it to a simpler and more realistic scenario.

Several questions were raised with regard to the deployment of the EPISECC concepts in a practically usable solution – mainly concerning security, data ownership, and exploitation (see 2.2.3).

The final PoC is designed now in order to follow the hints and to demonstrate the concepts in a way that explains the questioned topics. Anyway, not all of them could be implemented in the prototype and rather will be described in the final CIS architecture in the concluding Deliverable D5.4.

Yet, this dry run highlighted some missing points in the prototype we expect to fill for the final PoC. These issues and missing features were captured as backlog items in the issue tracking system of EPISECC Workspace, and followed-up by a Scrum based development process during the following four months.

2.2.2. Involvement of PCRAFVG and lessons learned

As a member of the Advisory Board PCRAFVG supported the EPISECC project from the very beginning. In addition to that PCRAFVG offered to host the PoC event in their premises in Palmanova and to act as LEMA in the PoC scenario. Starting from that offer the preparation of the scenario had a defined anchor point that determined all further considerations and decisions. It was clear that when having PCRAFVG acting as the LEMA the scenario and the procedures have to be aligned as much as possible with the prevailing situation in FVG when it comes to a disaster scenario with a cross-border dimension (e.g. engagement of international responders in FVG). To assure compliance with the existing structure and protocols two workshops have been conducted in Palmanova:

Workshop no. 1:

Disaster management system in FVG and ICT tools at PCRAFVG

This Workshop had two parts. The first part was dedicated to the introduction of the organisations in the emergency and disaster management system in FVG. It was of particular importance to understand the roles of the organisations in disaster operations. This knowledge is very important for the planning of the PoC scenario as well as for designing the evaluation process. Also, the second workshop topic – ICT tools at PCRAFVG – provided a more than valuable insight in the daily operations at PCRAFVG which will be very important when benchmarking the existing processes and means with the proposed EPISECC solutions.

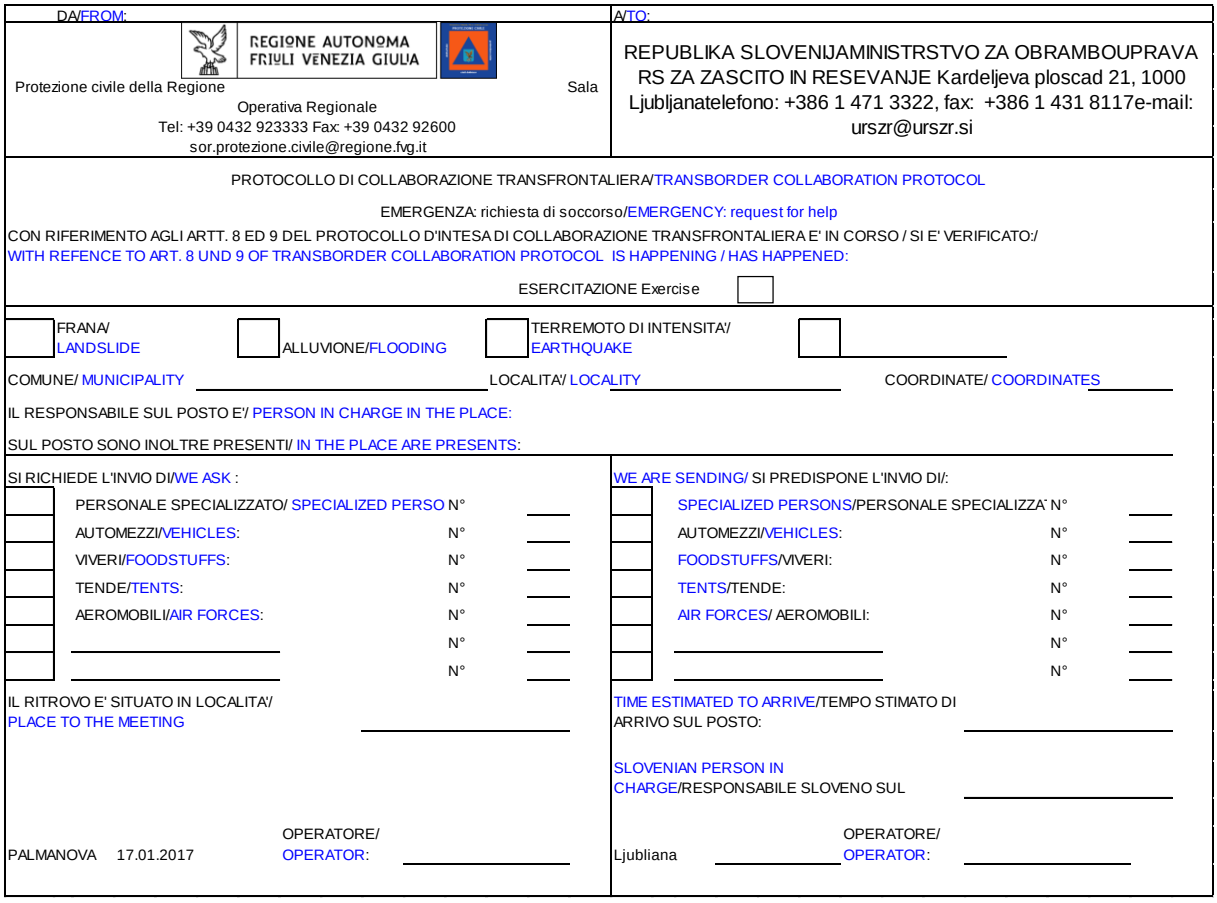
Workshop no. 2:

Collaboration protocols at PCRAFVG

In this workshop the active collaboration processes and protocols – national and trans-border – were discussed and analysed on their relevance for EPISECC. The existing trans-border collaboration protocol with Slovenia foresees one single form sheet (Figure 9) for exchanging

- information on the event
- information on requested response assets (sender of the form sheet)
- information on offered response assets (receiver of the form sheet)
- basic information on responsible personnel.

A lot of this content will be addressed by the EPISECC common information space concept in the PoC scenario play.



DA/FROM:

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

Protezione civile della Regione — Sala Operativa Regionale
Tel: +39 0432 923333 Fax: +39 0432 92600
sor.protezione.civile@regione.fvg.it

A/TO:

REPUBLIKA SLOVENIJAMINISTRSTVO ZA OBRAMBOUPRAVA RS ZA ZASCITO IN RESEVANJE Kardeljeva ploscad 21, 1000 Ljubljanatelefono: +386 1 471 3322, fax: +386 1 431 8117e-mail: urszr@urszr.si

PROTOCOLLO DI COLLABORAZIONE TRANSFRONTALIERA/TRANSBORDER COLLABORATION PROTOCOL

EMERGENZA: richiesta di soccorso/EMERGENCY: request for help

CON RIFERIMENTO AGLI ARTT. 8 ED 9 DEL PROTOCOLLO D'INTESA DI COLLABORAZIONE TRANSFRONTALIERA E' IN CORSO / SI E' VERIFICATO:/
WITH REFENCE TO ART. 8 UND 9 OF TRANSBORDER COLLABORATION PROTOCOL IS HAPPENING / HAS HAPPENED:

ESERCITAZIONE Exercise ☐

☐ FRANA/ LANDSLIDE ☐ ALLUVIONE/FLOODING ☐ TERREMOTO DI INTENSITA'/ EARTHQUAKE ☐ _____

COMUNE/ MUNICIPALITY _____ LOCALITA'/ LOCALITY _____ COORDINATE/ COORDINATES _____

IL RESPONSABILE SUL POSTO E'/ PERSON IN CHARGE IN THE PLACE:

SUL POSTO SONO INOLTRE PRESENTI/ IN THE PLACE ARE PRESENTS:

SI RICHIEDE L'INVIO DI/WE ASK :

☐	PERSONALE SPECIALIZZATO/ SPECIALIZED PERSO	N° ____
☐	AUTOMEZZI/VEHICLES:	N° ____
☐	VIVERI/FOODSTUFFS:	N° ____
☐	TENDE/TENTS:	N° ____
☐	AEROMOBILI/AIR FORCES:	N° ____
☐	_____	N° ____
☐	_____	N° ____

IL RITROVO E' SITUATO IN LOCALITA'/ PLACE TO THE MEETING _____

PALMANOVA 17.01.2017 OPERATORE/ OPERATOR: _____

WE ARE SENDING/ SI PREDISPONE L'INVIO DI/:

☐	SPECIALIZED PERSONS/PERSONALE SPECIALIZZA	N° ____
☐	AUTOMEZZI/VEHICLES:	N° ____
☐	FOODSTUFFS/VIVERI:	N° ____
☐	TENTS/TENDE:	N° ____
☐	AIR FORCES/ AEROMOBILI:	N° ____
☐	_____	N° ____
☐	_____	N° ____

TIME ESTIMATED TO ARRIVE/TEMPO STIMATO DI ARRIVO SUL POSTO: _____

SLOVENIAN PERSON IN CHARGE/RESPONSABILE SLOVENO SUL _____

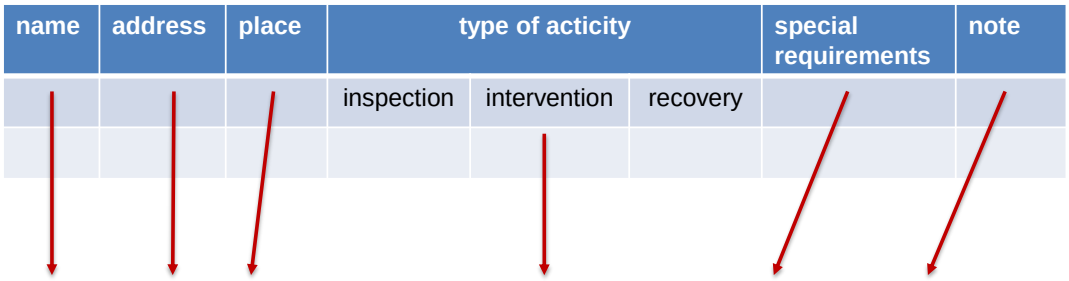
Ljubliana _____ OPERATORE/ OPERATOR: _____

Figure 9: Trans-border collaboration protocol between Italy and Slovenia

When looking at first responders in FVG (e.g. fire fighters) predefined spreadsheets (Figure 10) with mission specific data and information will be distributed from PCRAFVG via mail. The scheme includes data and information items such as:

- place and address of the intervention site
- name of the affected person
- type of requested activity
- special requirements/circumstances
- process related information.

The partly or even full substitution of such transactions has been identified as an additional aspect that will be covered in the PoC scenario.



N.	COGNOME	NOME	INDIRIZZO	LOCALITA'	TELEFONO	TIPO RICHIESTA			specifiche richiesta	NOTE	Data Richiesta	Data Intervento
						SOPRALUOGO	INTERVENTO	RECUPERO BENI				
						X		X				
							X		tetto	733907083		
									RICHIESTA LUCE			
						X			sopralluogo casa			
								X	RECUPERO BENI	fino a lun 14 non disponibile		
							X		POSIZIONAMENTO CONTAINER TRENTO			
									RECUPERO	SABATO 12		
								x	CONGELATORE/TELEVISORE			

Figure 10: Spreadsheet for information exchanged between PCRAFVG and responders

2.2.3. Recommendations from stakeholders

During the Dry Run in Vienna in November 2016 the focus was set on demonstrating the technical feasibility on the proposed solutions. Members of the End User Advisory Board (EUAB) joined the Dry Run and gave their recommendations about the current and future use of the CIS. The following table depicts the gathered recommendations during the Dry Run in Vienna, and splits the input into technical and organizational recommendations as well as comments which came up during the Dry Run.

Table 7: Recommendations from the End User Advisory Board (EUAB)

Organizational recommendations
The EPISECC consortium should identify ways to make recommendations to the European Union to make the Common Information Space visible.
For some organisations it is very important to have maintenance possibilities. If you want to have a viable product you need such kind of service or helpdesk?
It would be good for the future to show also interoperability between civilian and military systems. In the current paradigm only civilian interoperability was shown.
Show your solution to the Joint Research Center (JRC), they are maybe a good partner for a follow-up beyond project. Get also in touch with the distributor of the Incident Command System (ICS) in the US.
The consortium needs a minimum viable product; at the moment the solution is very wide.
In future the data for situational awareness could be collected via dedicated software e.g. Common Information Space.

Technical recommendations
Perform penetration tests e.g. according to ISO standards. You have to get sure that the system works during its use.
For future use and the final Proof of Concept specify in detail what kind of preparation is requested form the end users to use their IT tools (specify the necessary adaptation).
Describe in detail what your security framework looks like (e.g. asymmetric vs. symmetric encryption).
Describe in detail where the groups (CGORs) are hosted.
The consortium has to ensure that the data gathered during the use are treated according to the current legal framework (e.g. delete after transmission for privacy issues).
The consortium has to secure the performance of the system.

Other Comments
Important to have information across borders, not only EU but also the neighbouring countries.
Solution might be added to existing systems of the European Union to complement them.
Invite DG ECHO to your final Proof of Concept? The consortium has to prepare a big final event with many organisations. You have to give persons the chance to see your solution.
If you can show that your solution has solved a real problem (e.g. for the migration crisis) you will have success with your solution. Specify in detail for which problems your solution could be used. Define a "real world problem" for that purpose.
Include your solution in standardisation activities (CEN TC 391, CWA). Suggestion to contact ETSI.

The EPISECC consortium has taken the recommendations of the members of the End User Advisory Board into account since the Dry Run in Vienna and the Advisory Board meetings before. In the course of the creation of Deliverable 6.3 the EPISECC consortium will include the measures which were taken into account to the questions, comments and recommendations from the Advisory Board.

3. CIS Prototype implementation

The following paragraphs document how the CIS architecture which is specified in D5.2 [2] and the Protocol and network interoperability which is specified in D5.1 [3] are implemented as a prototype in a way that is suitable for the proof of concept. This prototype is validated in the final functional exercise in the Operation Centre of PCRFVG in Palmanova on 10.-11. May 2017.

3.1. Overview of EPISECC prototype

The EPISECC prototype is a software package consisting of the CIS components and adaptors developed within EPISECC, and the information processing tools connected with CIS provided by the EPISECC partners and the external party Teleconsult Austria. Examples for network interoperability in the prototype are the mobile TETRA base station and Mobile Data Gateway (based on TETRA/TETRAPOL standards), and mobile client devices of tools connected via 3G and LTE mobile communication to the respective tools.

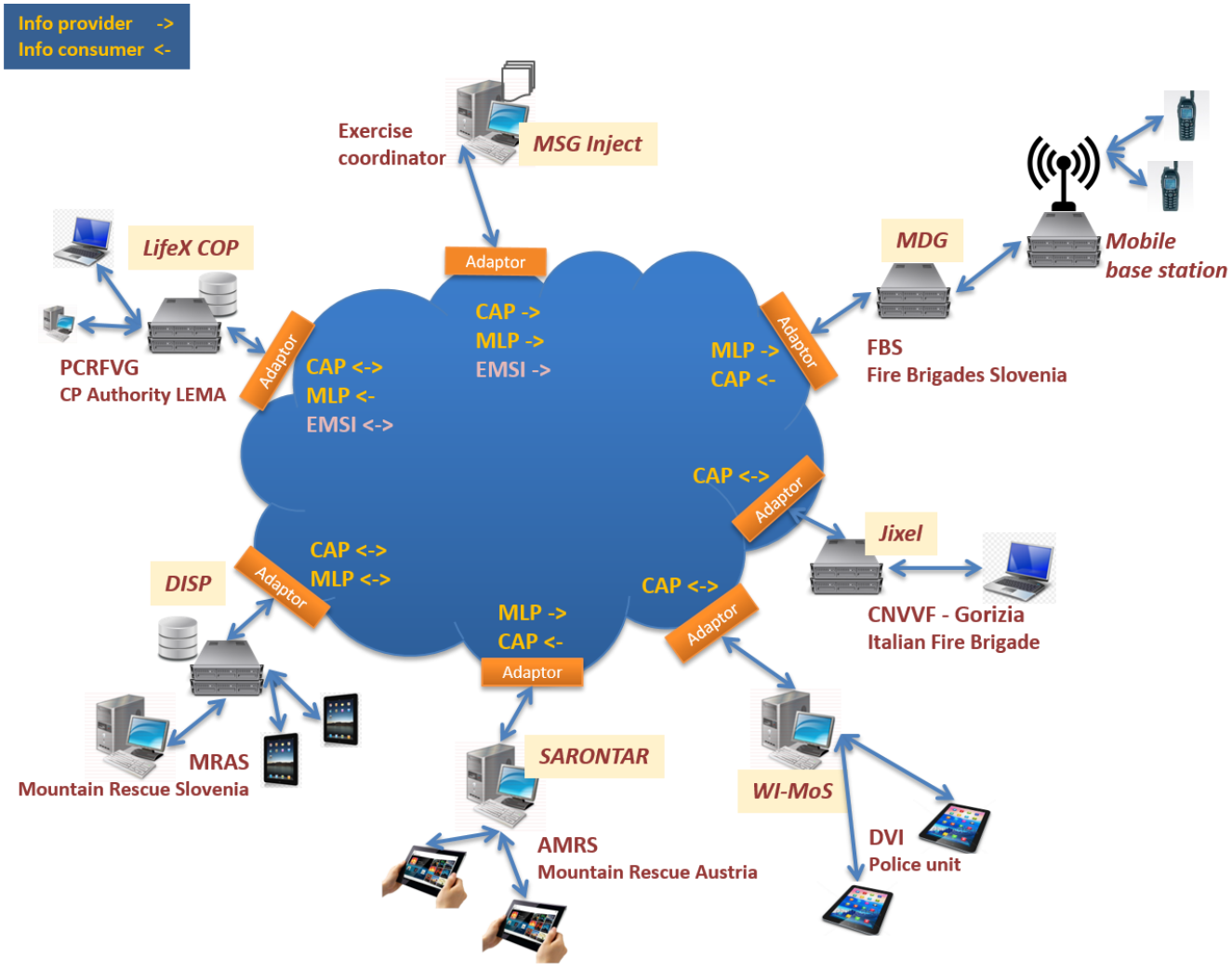


Figure 11 – CIS prototype participants; types of shared information

3.2. Protocol and network interoperability prototype

The following figures describe the two supported network architectures for the proof of concept:

- Case 1 – Connected mode
- Case 2 – Direct mode

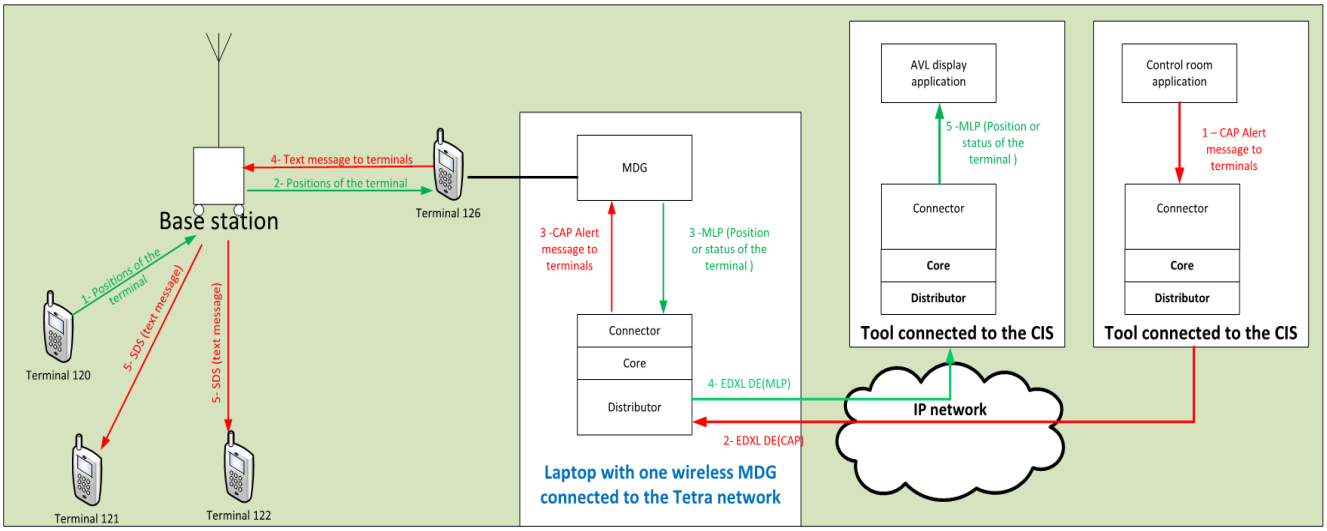


Figure 12 - Case 1 – Connected mode

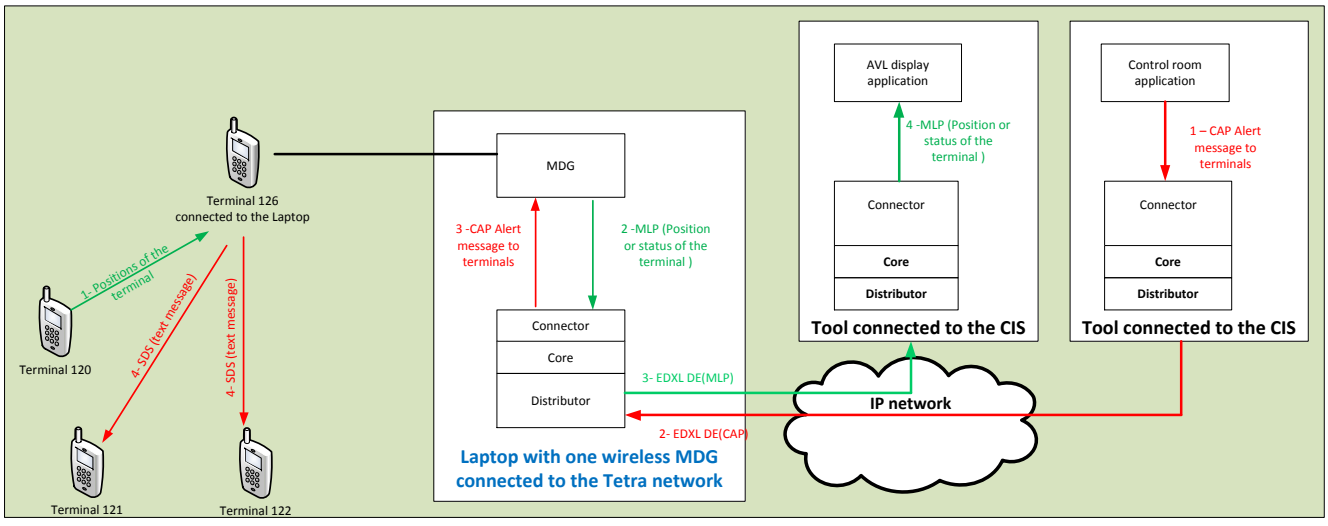


Figure 13 - Case 2 – Direct mode

The wireless Mobile Data Gateway (wMDG) is embedded in a laptop. A TETRA terminal (number 126 in the figure) is connected to this laptop (one USB port used).

In connected mode, the TETRA terminal is connected to the portable Tetra base station. The other TETRA terminals (numbers 120, 121, 122 in the figure) send their positions (standard TETRA Location Information Protocol used) and statuses (standard TETRA short data service used) to the TETRA terminal 126 that forwards them to the wMDG. Then, the received positions and statuses of the

TETRA terminals are sent by the wMDG to the control room applications (LifeX Cop, DISP or JIXEL) connected to the CIS. The format of the positions and statuses is Mobile Location Protocol (MLP) over the CIS. This messages exchange is represented in green in the previous figures.

The wMDG can receive from any applications connected to the CIS (LifeX Cop, DISP or JIXEL) a text message to send to one or more TETRA terminals on field in the form of a CAP alert message. The text message is then sent to the addressed TETRA terminals (standard TETRA short data service used). This messages exchange is represented in red in the previous figures.

In direct mode, the wMDG is connected to a TETRA terminal in direct mode (also called walkie-talkie mode). A TETRA terminal in direct mode listens to a pre-configured frequency to receive (voice or) data from other terminals also in direct mode that emit on this frequency. If the terminal needs to send anything it, it emits on this frequency.

The advantages of the connected mode compared to the direct mode are:

- the important range of the base station (several kilometres and only one or two kilometres for the direct mode);
- the capacity of the base station (hundreds of terminals and only up-to 10 terminals in direct mode).

The main advantage of the direct mode is that it does not require any infrastructure (TETRA network). The wMDG can be connected to the CIS with any kind of wireless connections (WiFi, 4G, Satellite, etc.). For the PoC, WiFi will be used.

3.3. Types of supported information in CIS

All information is shared by standardised messages. If a connected tool (CIS member) does not provide all data that are required as mandatory fields in the used standard, the Connector has to amend the data by default and compile a complete and compliant message according to the appropriate standard.

3.3.1. Message envelope

Every message exchanged in the Common Information Space is encapsulated in an EDXL DE envelope in order to provide routing information of encapsulated payloads. The time stamp of sending a message, the sender Id and the CGOR where the message is distributed are used in the prototype.

While the standard definition allows to combine different payload within one EDXL DE envelope, the CIS prototype supports only one content object per message. The packing/de-packing of messages (CAP, MLP) is performed in the Core, based on the well-formatted content object and a list of EDXL parameters provided by the tool/connector.

3.3.2. Alerts and warnings

Alerts and warnings provide new or updated information about current or potential events that require the attention of crisis managers and responders. Alerts are shared as CAP messages in the CIS.

Besides the mandatory CAP fields required by the standard, the information blocks used for EPISECC CIS are Event Code, Headline, Event Description and Instructions (text fields that are used for semantic annotations), and Area Polygon or Area Circle (geometry that is used for map representation in the connected tools).

Additional optional CAP fields and individual parameters can be included in the CAP message but are possibly not interpreted by some of the tools.

A specific case is addressing a message to devices within the area: that is resolved by sending a CAP message with Scope=private and the concerned Device-Id's in the Addressees field. This message is sent to a CGOR where the members are tools which control mobile field devices. The forwarding of the message to the mobile clients is implemented in the tools.

3.3.3. Unit positions and status

For sharing the position and status of field units, the position of assigned mobile devices is shared as MLP message to CIS. The devices themselves are clients of a server that controls the communication to the devices – a single mobile device can't be a CIS participant. The server, belonging to an organisation, is connected to the CIS via an adaptor and transforms the GPS positions gathered from the devices into MLP messages sent to defined CGORs in the CIS. Mobile devices may be TETRA terminals linked to MDG, or mobile clients of DISP and SARONTAR communicating via 3G/LTE.

Additional information concerning the unit assigned to the device can be obtained by a device registration process and displayed together with the device details in the common operating picture.

3.3.4. External information sources

MSG Inject simulator is a dedicated tool developed for simulated inject of any messages to the CIS. It is intended for testing as well as for simulating external information sources which are not actually available during the PoC exercise. The messages to be injected have to be prepared as XML files in a directory. MSG Inject sends the messages in these files via an adaptor to the CIS. There are two operation modes: The iterative mode repeats messages in a loop and is used mainly for load and performance tests. The time triggered mode sends a defined sequence of messages according to a parameter file, giving the intervals for sending the messages. It is intended to trigger an exercise with injects in a given time line.

The inject of an initial earthquake alert will trigger the start of the PoC exercise.

Italian Earthquake Alerting System

The "Istituto Nazionale di Geofisica e Vulcanologia" (I.N.G.V.) (http://istituto.ingv.it/the-institute/the-institute/view?set_language=en) in Italy, is a public institute involved in research activities in the seismic and volcanic fields. It is also the main institution in charge of monitoring and surveillance of volcanic and seismic events.

The seismic and volcanic monitoring and surveillance service for all the Italian territory is carried out in support of the National Civil Protection Department, with which INGV works in close cooperation.

The Institute continuously provides seismic and volcanic surveillance services on both local and national scale, 24 hours a day, either by communicating to the operating rooms of the Civil Protection Department every seismic event occurring in Italy and potentially perceived by the population, or alerting the Department to any significant activity of Italian volcanoes.

Earthquakes alerts with detailed information (e.g. epicentre, magnitude, depth, time, exact location), both nationwide but also related to worldwide seismic events outside of Italy, are also provided by I.N.G.V. through a dedicated twitter channel, @INGVterremoti.

In a typical emergency scenario such as the one simulated in the EPISECC PoC, alerts about a big earthquake affecting the population, are delivered by the I.N.G.V. to both the national and local regional Civil Protection authorities (in the EPISECC PoC scenario, the local authority is represented by the LEMA). For this delivery of alerts to happen in real time, the specific tools used by the Civil Protection authorities have to implement an adapter for each connected external data source, or the same adapters can be implemented as part of the EPISECC CIS, for getting information from external alerting systems. In the I.N.G.V. case the adapter would need to implement a) a reader of tweets from the @INGVterremoti channel, and b) a Tweet-to-CAP converter for the final ingestion in the CIS and distribution to the CIS participants (using a dedicated CGOR).

In the simulated EPISECC PoC scenario on the other hand, the initial alert triggering all the scenario activities was created starting from a typical CAP alert originated by the GDACS system. These CAP alerts are available at the following link: http://www.gdacs.org/xml/gdacs_cap.xml.

3.4. Tools used in PoC

The Common Information Space is an information sharing platform without own user interface for direct access to the information. It rather enables the tools that are used by the parties involved in disaster response to communicate and to access shared information. This means that the processing and representation of information is the duty of the tools.

The tools that are provided by the EPISECC partners are developed outside of EPISECC (background[5]) and are marketable products or prototypes. Some of them were slightly modified to be able to demonstrate the EPISECC goals and to fit with the requirements of the PoC. For every tool, a specific EPISECC adaptor is developed and installed (in EPISECC project, foreground) which links the tool to CIS.

In order to demonstrate that existing legacy tools can easily been integrated, the external partner Teleconsult Austria[6] could be allured to volunteer in the PoC with the tool SARONTAR that is deployed at the Austrian Mountain Rescue Service in Styria. The adaptor for SARONTAR is developed by the EPISECC partner FRQ.

[5] "Background" in FP7: see https://www.iprhelpdesk.eu/Fact-Sheet-Background-in-FP7

[6] Teleconsult Austria, Graz, http://www.teleconsult-austria.at/

3.4.1. LifeX COP

Tool description, functions

Frequentis contributed the LifeX COP prototype, a Common Operational Picture tool. It provides shared situational awareness on the tactical command level with a GIS based user interface, collection of data from various data sources and presentation of all data in selectable layers on a map. The purpose of the Common Operational Picture is providing and presenting data and views for decision makers in the field, in command and control centres, and in administrative headquarters, in order to support time critical decision processes and to give a near real time overview of the situation on site.

LifeX COP provides the following features:

- Shared situational awareness tool with a GIS based situation map
- Collection of data from various data sources, presentation of all input data on a map
- Items can be added and edited by the tool operator, in addition to the information collected from CIS and external data sources
- Incident handling and allocation of responsibilities to resources
- Each dataset is presented in form of a layer which can be switched on/off by the user
- Various options to filter and search for data.

A more detailed tool description is provided in deliverable D6.1 Proof of Concept Design [1].

Purpose in PoC

LifeX COP is intended as the tool used by LEMA in the Crisis Room during the EPISECC Proof of Concept exercise. It collects information from all other tools in the CIS and provides a comprehensive situational overview. LEMA may also insert information manually and share it with other CIS members.

As a specific feature, the COP operator can address alerts via Tetra MDG or SARONTAR to mobile devices which are currently located in a defined area and which have submitted their position in CIS.

For vertical reporting, authorized users (e.g. civil protection authorities) can log-in to LifeX COP as read-only users and get the common operational picture only with such layers and information items that are released for reporting by the COP operator.

Interfaces towards CIS

The EPISECC prototype generally supports CAP (alerts) and MLP (mobile device position and status). LifeX COP can send and receive CAP messages, and receive MLP messages. In addition, LifeX COP is also able to process EMSI messages sharing situational information on incidents, resources, and tasks.

LifeX COP is integrated with the CIS CGOR concept, meaning that the COP operator can select the appropriate CGOR from a list of all available CGORs when sharing a COP information item.

3.4.2. DISP

Tool description, functions

DISP is a mission-centric management organized in 3 segments called a portal (to visualize data), a middleware (to manage DISP features and services) and a reporter (for report and assessment on the field). This ecosystem therefore provides 3 main tactical features:

- **Mission management:** It consists in creating, reading, updating and deleting events, places, responders and resources like devices or vehicles used in the crisis context. Besides, the responders are given authorization access based on their role. Moreover, the management feature can assign devices to responders to enable the coordination feature.
- **Coordination:** This features allows the tool operator to track the positions of crisis responders who were assigned devices with GPS capabilities, take localized pictures with camera devices, follow battery level among others possibilities. The coordination feature also includes a file sharing tool that enables document exchanges between all mission participants based on their authorization levels.
- **Report and assessment:** This feature allows to report and/or assess events from the fields directly to the command centre (on a DISP portal) on a map. It can be done either from the portal (by the tool operator) or by using a field reporter. Thanks to the middleware layers, 2 DISP tools can always synchronize together to update their respective operator on what is currently happening on the field.

Users can create an account and associate themselves to one or several organizations and access mission either on demand or on invitation. The vertical reporting is defined by the rights given to a user at his creation. Any user that create another user can only give him authorizations lower than its own. This implies that only the tool administrator can give the highest accreditation level to his collaborators.

A more detailed tool description is provided in deliverable D6.1 Proof of Concept Design [1].

Purpose in PoC

The DISP ecosystem (portal, middleware and reporter) will be used by the Italian mountain rescuers form CNSAS-FVG and their Slovenian equivalent from MRAS to track their responders on the field. Aside from tracking purpose, the rescuers will also collect data from the CIS (provided by partners' tools) under form of CAP messages to define crisis areas and aggregate them on a DISP map to oversee the global situation and intervention status. If required, a DISP reporter user can write a message that will be formatted into CAP standard and forwarded to CIS partners.

For Specific feature, DISP can warn any responders when they are entering or leaving a reported dangerous area by sending a message in CIS. This message has instructions requiring targeted responders to leave or avoid the danger zone.

As DISP is not a message-oriented common operational picture, it will provide a perspective of what can be achieved when a tool is not designed around standard protocols like CAP for reporting or MLP for location tracking but operates with other tools that have such capabilities.

Interfaces towards CIS

To interact with the CIS, we chose to generate specific CAP messages corresponding to an action performed by the tool operator. DISP can therefore receive and process CAP messages and map them to local events, places or mission concept based on their content. Moreover, DISP can process incoming MLP messages and associate them to a local existing user position. Concerning the CGOR concept implemented in the CIS, DISP associates a CGOR to a mission. This implies that all CAP alerts can be either associated to a single mission or just to an event as part of a mission depending on its content. Only CAP updates are held within the same mission. Other alerts describing incidents happening in a different area will generate a different mission from DISP perspective.

This also signify that any tool operator can decide to which CGOR he addresses a message based on the current mission he is operating from.

3.4.3. JIXEL

Tool description, functions

Besides providing the Semantic Web Service (see 3.5.7), IES Solutions contributes to the PoC with the JIXEL software components.

JIXEL is a production-ready suite of services and UI tools for emergency management and interoperability. It is already used in Italy by the National Corp of the Fire Brigades and by the Regional Civil Protection Department of Sicily. For the specific purposes of the PoC, a version corresponding to the one currently customised for the Italian Fire Brigades is used, providing the following features:

- ability to receive and visualise information generated / shared by other interoperating tools (e.g. by the LEMA using the LifeX COP tool)
- ability to create, update and share events with other interoperating tools (e.g. LifeX COP and DISP)
- ability to create and share with other interoperating tools (e.g. LifeX COP and DISP) situation reports about:
    - currently handled events
    - specific activities
    - deployed resources

A more detailed tool description is provided in deliverable D6.1 Proof of Concept Design [1].

Purpose in PoC

In the PoC scenario, JIXEL is used as the Command and Control room system of the Italian Fire Brigades in Gorizia (Italy). It receives information about the ongoing situation by other cooperating

organisations (including the initial alert with the characteristics of the simulated earthquake from the LEMA), and mainly provides reports about the activities carried out by Italian Fire Brigades teams in the field. See the scenario description in Section 1.3 for further details.

Integration with EPISECC and Interfaces towards CIS

JIXEL can send and receive CAP messages to / from other tools connected to the CIS. To this end, Inbound and Outbound software interfaces and a CIS Standalone Adapter have been implemented and configured for the purposes of the PoC.

3.4.4. Mobile Data Gateway

Tool description, functions

In the EPISECC project, the MDG is the gateway between the CIS and the TETRA network. Control room applications will be able to send and get information to the MDG through the CIS. Control room applications will typically be able to:

- Get location of a specific first responder;
- Get status information (emergency, on incident scene, etc.) of a specific first responder;
- Get radio status information of a specific first responder;
- Send messages to a specific first responder;

A more detailed tool description is provided in deliverable D6.1 Proof of Concept Design [1].

Purpose in PoC

For the PoC, a wireless MDG and a portable TETRA base station will be deployed with several TETRA terminals connected under it. These terminals will send periodically their positions to the MDG. The MDG also connected to the CIS will:

- Allow an application connected to the CIS to send text message to the TETRA terminals;
- Forward the locations of the TETRA terminals to the applications connected to the CIS.

The TETRA terminals represent the first responders on field.

Interfaces towards CIS

The MDG supports CAP (alerts) and MLP (mobile device position and status). The MDG can send MLP messages (locations of the Tetra terminals) and receive CAP messages (text messages to the Tetra terminals).

3.4.5. WI-MoST Wrapped Information Mobile Sharing Tool

The WI-MoST is an information sharing tool built to demonstrate the concept of wrapped information and how attribute-based sharing of information can be deployed to secure authorised access to information. It currently runs on an Android-based mobile device. It is used to share

information allowing end-to-end security independent of whether the underlying communication layer is secure or not. It uses Wrapped Information to secure authorised access to information based on the attributes of the individual recipients.

The tool has the following features. It

- Enables sender to add selected wrapped information features, which are:
  - Allow selected recipients authorised access based on their attributes
  - Select - from a pre-defined list - access conditions, which would be tied to the shared information
- Enables the user of the tool to select and send map coordinates to other connected devices in CAP standard
- Generates, sends and receives messages in CAP-standard

Purpose in PoC

In the context of EPISECC and CIS, one WI-MOST tool user can send a CAP message that is received by all connected devices. However, she can also select parts of the CAP message to be accessible only to a sub-group of recipients based on their attributes.

During the PoC, the tool will be used by emergency services responsible for Disaster Victim Identification (DVI) effort. They will use the tool to send and receive CAP messages, which will contain information elements that identify victims. The messages will be received by all devices and other tools connected to the CIS and on the same CGOR. However, the CAP elements that contain DVI information will be decrypted only by other Wi-MOST devices, whose attributes include membership of the DVI team. Other devices and tools that receive the CAP messages but do not have the correct attribute (i.e. being member of the DVI team), will not be able to decrypt the DVI-information element, yet they will be able to access the rest of the CAP elements.

Interfaces towards CIS

CAP messages can be shared. CAP elements that contain DVI information (as selected by the tool user), will be accessible only to other Wi-MOST devices, which have the correct attributes pre-configured. That demonstrates the mechanism of protecting specific parts of information, following a defined information security policy.

3.4.6. SARONTAR

Tool description, functions

SARONTAR is a satellite-based operations control system for a more effective and a more coordinated guidance of rescue forces in alpine accidents. The key issue of this innovative system is the integration of positioning, navigation, geo-information, and communication techniques. In addition to the essential information on the position of the search and rescue teams, a special emphasis was put on the hybrid communication in remote alpine areas and also in the case of natural disasters. After such incidents, the availability of terrestrial communication is often limited or

missing at all due to damages in the disaster zone. Hence, it is important to be independent from terrestrial infrastructure by additionally relying on satellite communication which is an essential part of the SARONTAR concept. Geo-information is another issue that is very important for alpine rescue teams. In the Austrian province Styria, the teams use to the maps provided by the local government (Austrian topographic map and ortho-photos).

The system basically consists of the Mobile Terminal delivering position information to a central server and the Mission Control Centre receiving and visualizing the positions. Additional (geo-)information is exchanged on request. Therefore, the mission controller equipped with this system is able to get a visual impression of the actual situation, in order to analyse the situation rapidly and make precise instructions to the search crews.

Mobile Terminals for rescue teams:

- Automatic continuous position transmission
- Exchange of messages with Mission Control Centre (text, POIs, locations, etc.)
- Map view with sent/received geo-information
- Offline maps (topographical map, OpenStreetMap)

Mission Control Centre for mission controller:

- Mission administration
- Collection and forwarding of preliminary information
- Assignment of Mobile Terminals
- Map view with mission-related geo-information and current locations of the Mobile Terminals (topographic map, orthophotos and OpenStreetMap)
- Exchange of messages with Mobile Terminals (e.g. search areas/routes)
- Export of the complete mission documentation

Purpose in PoC

SARONTAR Mobile Terminals are intended to be used by the Austrian Mountain Rescue Service in the field during the EPISECC PoC exercise. The continuously collected positions are forwarded to the CIS as well as status messages (text and POIs). Vice-versa, the Mobile Terminals receive status messages and geo-information messages out of the CIS. Through the SARONTAR Mission Control Centre, the exchange of messages is documented and positions and geo-information are visible in the integrated map.

Interfaces towards CIS

Information is made available via REST interface at the SARONTAR server. Positions and status messages from the Mobile Terminals can be requested via GET method, status and geo-information messages can be forwarded to the Mobile Terminals by POST method.

3.5. Common Information Space components

The architecture and functions of the CIS components are specified in deliverable D5.2 Informational Interoperability Specification [2]. These details are not repeated in this document; this section describes how the CIS architecture is implemented in the EPISECC prototype and which features are available in the PoC exercise. A more detailed technical description will be provided in the public deliverable D5.4 Architecture of the Common Information Space.

Some of the concepts outlined in D5.2 are not or only partly implemented due to time and budgetary limits. Concepts which cannot be integrated in the PoC scenario will be explained and demonstrated in separate sessions and discussed with the practitioners with the goal of getting a sound evaluation of future extensions of the CIS.

3.5.1. CIS overview

The EPISECC prototype as demonstrated in the PoC exercise (PoC prototype) consists of information processing tools which are not part of the EPISECC development (background of the involved partners), and of components which implement the CIS architecture (EPISECC foreground, blue boxes in Figure 14). The PoC exercise shall evaluate the interconnection of the given tools and the added value of information sharing, rather than the tools themselves.

Figure 14 shows a basic block diagram of the components used to establish a CIS instance which connects tool A and tool B. The registration and routing information is stored in the Directory Agent and Segmentation services, the taxonomies provided by the tool owners in the Semantic repository and services. These are central (global) CIS components. The Adaptors (Connector, Core and Distributor) are specific instances for every tool; the Connector is a tool specific implementation based on the EPISECC Connector Template.

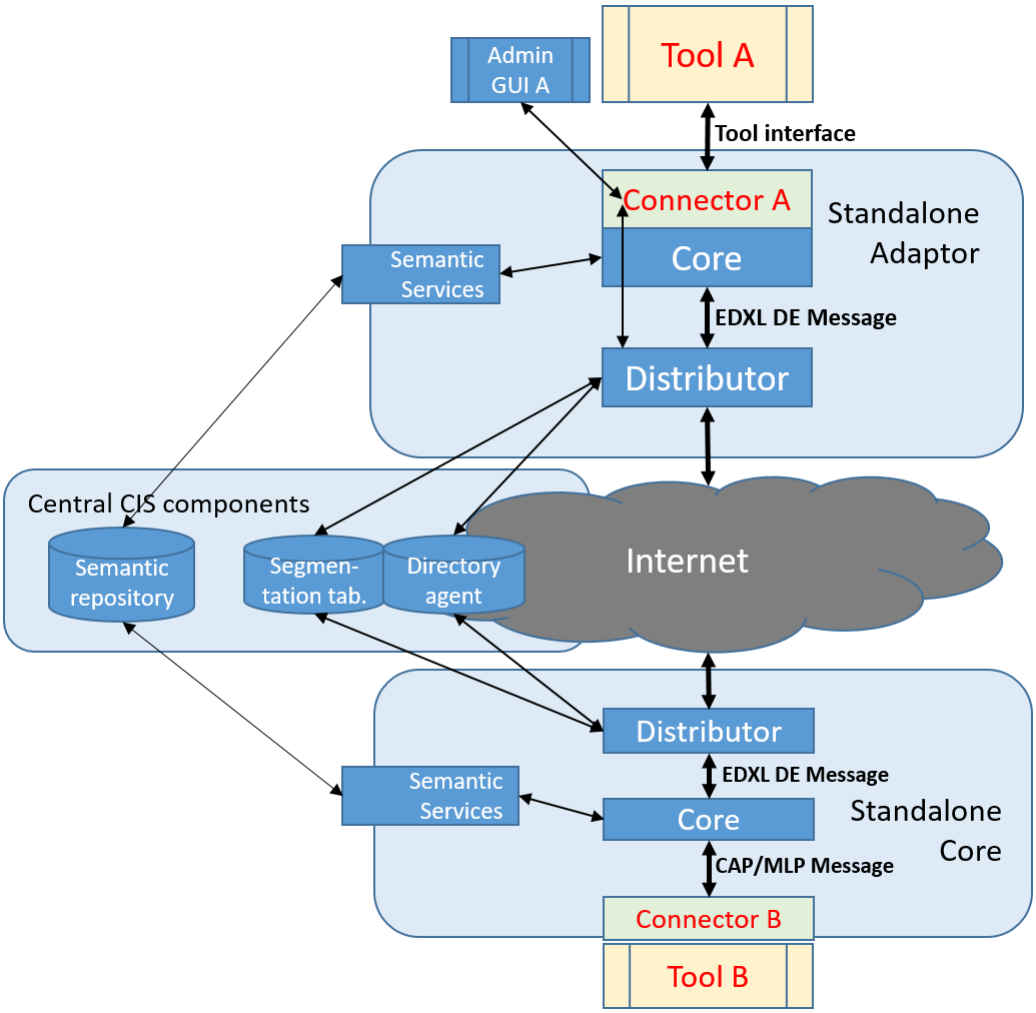


Figure 14 – CIS component diagram

3.5.2. CIS-Adaptor

Every tool has a dedicated Adaptor linking it to the CIS. As described in D5.2 [2], the Adaptors handle the transformation of tool specific data to the standards used for messages in CIS, create semantic annotations, and manage the message distribution according to the data ownership constraints given by the CGOR concept.

In addition, the Adaptors provide a service interface for the Admin GUI that allows every CIS participant to manage his CGOR membership (to create a new CGOR, to invite other participants, and to accept or refuse CGOR invitations from others).

There are two different implementations for the integration of tool and Adaptor:

Stand-alone Adaptor combines Core and Connector in one process. It exposes a REST endpoint to the tool for data to be sent to CIS and a http POST REST endpoint callback for hand-over of data received from CIS. Data and parameters are packed in a tool specific JSON structure which is parsed rep. filled by the Connector part of the stand-alone Adaptor.

In the EPISECC prototype, stand-alone Adaptors are implemented for tools that are not aware of CIS formats and mechanisms: JIXEL, MDG, SARONTAR, WI-MoST.

Stand-alone Core provides only the standard Core functions of the Adaptor and with standard interfaces, corresponding to the standard data formats used in CIS. The Connector functions have to be integrated into the tool (JAVA deep integration) if needed. This architecture suits for tools which already use the applied standards (e.g. CAP) for their interfaces and which have implemented CIS specific features: DISP, LifeX COP.

3.5.3. Connector template

The connector is the CIS component directly linked to the tool. Its task is the transformation of the particular interface data and formats to the standards adopted in EPISECC. In addition, specific pre-processing of messages to be sent to or received from the CIS can be located within the connector, e.g. filtering of messages, or selection of addressees. This can be done based on the message content or on the envelope parameters.

All these features are very specific for the tool. Therefore, the implementation of the connector is in the responsibility of the tool providers. We published a template in EPISECC, that covers the transformation of a given data structure into the XML format of the standards and that provides a sample for the link to the tool interface. Towards the CIS, the connector template exposes a REST interface and callback which communicates with the CIS Core module. On this side, a well-formatted XML message and a JSON object with EDXL DE parameters is submitted.

3.5.4. CIS Core

The Core is in between the Connector and the Distributor and handles central features of the EPISECC concept. Although it is part of the adaptor usually installed on the tool server, the core must not be modified by the user in order to ensure the information processing integrity.

- Packing/de-packing the message content in the EDXL DE envelope
- Checking the message syntactically (only valid messages are processed)
- Adding semantic annotations to received messages (calls the Semantic Services)
- Applies information security (only the CGOR mechanism is actually implemented in the prototype, but here is the place for additional security features)
- Separates message processing from message distribution.

3.5.5. Distributor

As detailed in Deliverable 5.2, once a message passes the connector and the core, it is sent to the distributor embedded in an EDXL envelop through a REST request that mentions the destination CGOR as parameter. Based on the addressed CGOR, the distributor builds a recipient list by interrogating the directory structure service (partition) and the discovery agent service (Eureka).

Distributors do not address messages to themselves, which implies that there can only be one connector/core per distributor.

In a final concept, the distributor would be part of the adaptor which is installed on the server and secured intranet of the tool owner, in order to establish secured data access. In the PoC prototype,

all distributor processes run on a dedicated server of Hitech for practical reason. That makes the deployment of adaptors easier and allows a much simpler testing and monitoring of the information distribution. From a user's point of view, the deployment mode of adaptors is completely transparent and has no influence on the proof of concept evaluation.

3.5.6. Semantic Repository and queries

Purpose:

The EPISECC Semantic Repository hosts sets of concepts, either organized as taxonomies, dictionaries, etc. or unstructured, that are linked (see chapter 0). The challenge of semantic annotation consists in associating the concepts of one set with their respective matches (corresponding concepts) in other sets used in CIS participants' tools.

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

Design:

To create the link between sets of concepts, we rely on paths in directed graph {(term1) ==> (term2)} called triples. The first term is designated as the subject as it represents the concept we would like to match while the second word defines the object, which is the result of the semantic relation represented by the directed edge or arrow (representing predicate).

Implementation:

To fill and access the EPISECC Semantic Repository, we rely on 2 main tools: Protégé and Apache JENA:

- **Protégé:** In this free tool developed by Stanford University, we can add concepts one by one then first we link them together (provided the existence of a predicate between them), afterward we associate them to their EPISECC taxonomy equivalent following our taxonomy schema. This operation is done manually for this proof of concept.

When the concepts are manually linked, we still can generate automatically additional relations thanks to the commutability and transitivity nature of the triples. For this purpose, we rely on Protégé's reasoner to search and create any inferred link between concepts. The created links are then saved and added to our triple store storage solution: Apache JENA.

The result is that we have 3 sets of concepts combining more than 300 of the most recurrent concepts used for crisis communication between responders from Italy and Slovenia.

- **Apache JENA:** JENA is a free and open source framework used to link and build linked data applications and semantic web. It embeds a triple datastore database (TDB) that can be queried from a REST-based SparQL query server (Fuseki). In this project, due to the micro-service architecture

(described in deliverable 5.2), the effort was organized around the SPARQL REST interface to build dynamic queries to retrieve most suitable data.

3.5.7. Semantic Web Services

The Semantic Web Service is used for enabling Semantic Interoperability in EPISECC. In a typical interoperability scenario, it provides the software interfaces (API), used by the calling software components (CIS Connector Core) to ask the runtime semantic matching (and related semantic annotations) between concepts of senders and receivers of messages. Upon reception of a semantic matching request, the Semantic Web Services:

- select from the message received in input, the information that needs to be semantically annotated, and prepare a JSON structure with the same information inside. Such JSON structure represents the so called *semantic annotation request object*
- send the *semantic annotation request object* to the downstream component (the Semantic Service built using Apache Jena and the Fuseki SparQL query server), in charge of building and executing the query to the underlying EPISECC semantic repository (TDB);
- receive back the original information together with the corresponding semantic annotations (a JSON structure which represents the so called *semantic annotation response object*), to enclose them in the original message, or to directly deliver them to the calling component (the CIS Connector Core on the receiver side)

The Semantic Web Service is implemented as a SOAP Web Service.

For a proper and reliable functioning of the semantic interoperability between different organisations cooperating in disaster management, the EPISECC semantic repository must be populated with the EPISECC taxonomy concepts, as well as with proprietary (end users' organisations) taxonomies and schemas, and the mapping between proprietary concepts and EPISECC semantic concepts must be performed beforehand (configuration time).

Figure 15 below shows the integration of the Semantic Web Service in a typical communication scenario, targeted at realising both syntactical and semantic interoperability:

1. On the CIS Core on sender side, a message is prepared containing semantic concepts from organisation A (sending organisation)
2. The message is distributed by the organisation A Distributor to the Distributor on the receivers' side (organisations B, C, etc.)
3. The message is then forwarded to the CIS Core on the receiving side
4. The CIS Core receives the message and create a semantic matching request for the Semantic Web Service, which is delivered using the provide SOAP interface
5. The *semantic annotation object request* structure is created and delivered to the downstream component based on Apache Jena and Fuseki server
6. The *semantic annotation object response* is provided back to the Semantic Web Service
7. The original together with the annotated concepts are provided back to the calling CIS Core component

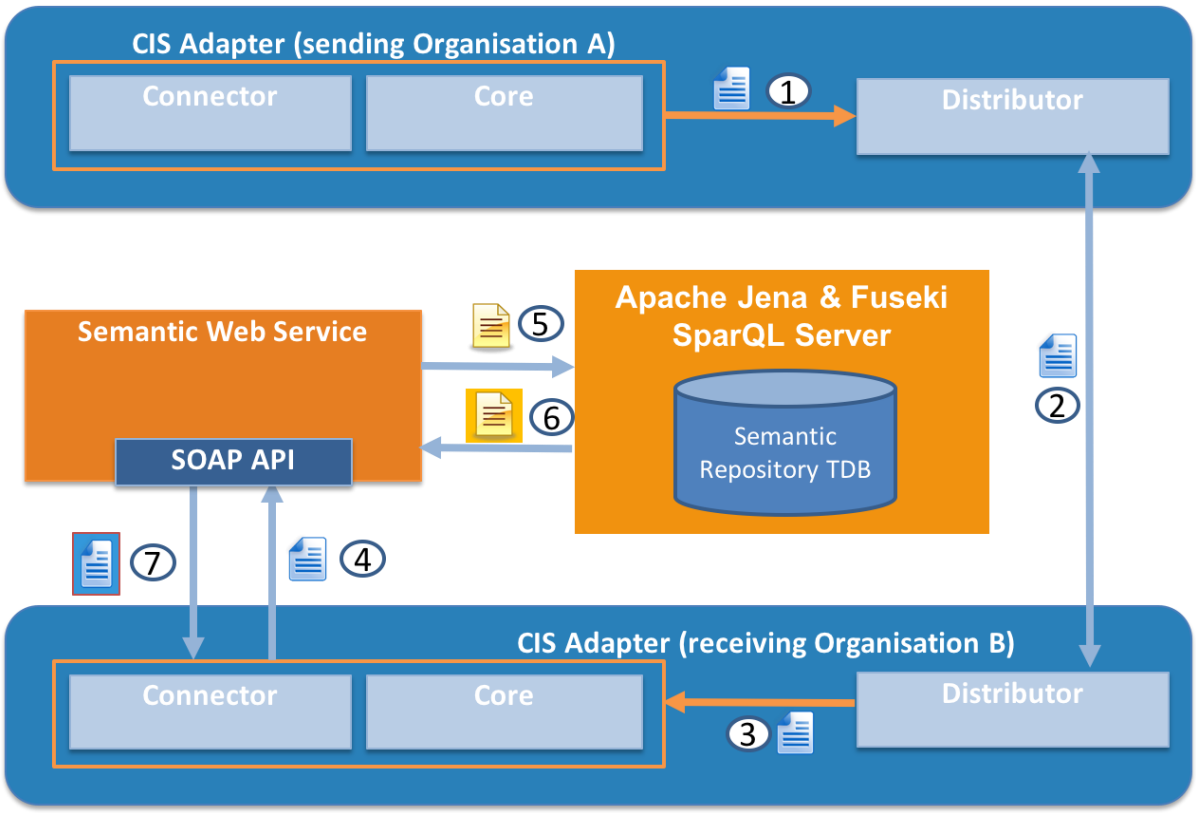


Figure 15: The Semantic Web Service and its integration in a typical communication scenario

3.6. Semantic mapping and matching

The semantic interoperability is validated through message exchange process of two organisations coming from different countries: Mountain Rescue Slovenia and Fire Fighters Gorizia. PCRFVG which acts as LEMA uses terms and concepts from EPISECC Taxonomy. Therefore, three different languages will be represented in the CAP messages: Italian, Slovenian and English. Since the process of identifying concepts consumes time, a set of relevant concepts for each organization is selected. The selected concepts are closely related to the PoC scenarios and use cases. Such an approach ensured that the exchanged messages have common concepts from both organizations and include semantic annotations.

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

The matching is preformed using queries and results with semantic annotations. It happens when one organisation, in PoC case either Italian Fire Brigade or Slovenian Mountain rescue or CP Authority, sends CAP messages. The Semantic Service sends a request for querying over the EPISECC Semantic Repository and finds the matching concepts in other organisations. The annotations are

inserted in parts of the CAP messages where end users may enter free text. Matching retrieves the concepts' terms and inserts them into the message next to the original term. The process also adds two different marks next to the receiver's concept: one in the case when concepts from both organisations are mapped as "exact" to the connecting concept in the EPISECC Taxonomy and other in cases when there is at least one concept mapped as broad. The necessity and usefulness to mark annotations with more details, for example to note or interpret mapping type of users' concepts to the connecting EPISECC Taxonomy concept, will be discussed with end users and observers after the PoC.

During the PoC the EPISECC approach to solve the interoperability problem is observed and analyzed afterwards considering the following aspects:

- usefulness of the semantic annotations,
- efficiency of the matching process,
- functionality of the EPISECC database, i.e. Semantic Repository,
- effectiveness of the approach.

Usefulness of the semantic annotations is discussed with organisations representatives after the PoC exercise via adequately prepared questionnaires and discussion session (Chapter 1.4). Even though semantic annotations resulting from the situations when organisations' concepts have exact meaning as EPISECC Taxonomy ones are worth, it is very important to have opinion about semantic annotations which are results of mapping with broad meaning. It should be discussed how useful they are and to what extent they may help end users in understanding messages, particularly in the case when matched concepts are vaguely connected considering their meaning.

The efficiency of the matching process is measured through the complexity of the queries and implementation. However, it depends on deployed data model and comprehensiveness of the Semantic Repository. CIS solution to store users' concepts in a database independently of software code allows users to continuously update and enhance matching process.

The functionality of the EPISECC database, i.e. Semantic Repository, which may be considered through returns of correct results in a reasonable time, highly depends on implemented interfaces and underlying telecommunication infrastructure as well as of central CIS components infrastructure.

The effectiveness of the approach is summary of the above perceptions and analysis, which comprise both end users' assessment and technical capabilities.

3.7. Information segmentation (CGOR) and administration

For the configuration of CGOR and the process of group building the "Administration GUI" is used. It allows the dynamic creation and management of so called CGORs (Cooperation Group Online Rooms), The Administration GUI (also called "eppisecAdmin") can be used by each organization, who want to connect their own tool to the CIS and to manage the CGOR configuration.

The Administration GUI can be started in a Firefox or Chrome Browser (HTML-4 is needed) from Web location http://episecc.eu/episeccAdmin.

At startup the access to the corresponding CIS connector is needed. The network address has to be configured in the “configuration Page” in the field “URL to Connector Service”.

After restart the GUI displays on the right side all information about organisations, and on the left side all information about CGORs.

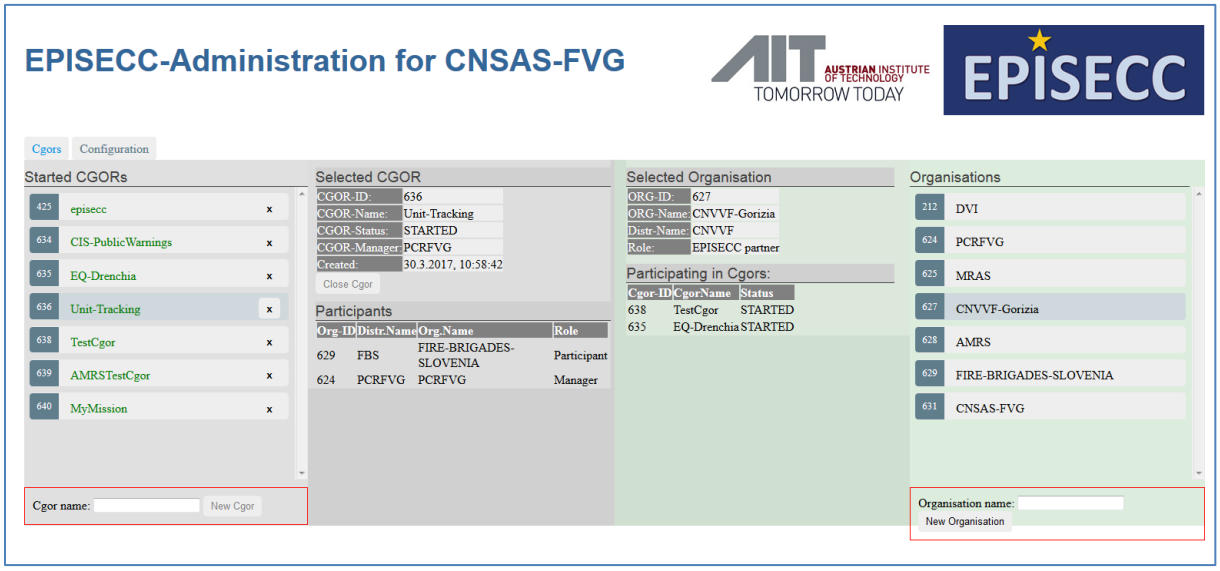


Figure 16: CIS Admin GUI

Actions for organisations:

The list of all defined organisations is shown in the page.

If you click on one of the organisations, the details of this organisation is displayed in the column “Selected Organisation”

It is possible to add a new organisation by inserting the name of the new organisation and pressing the “Add organisation” button.

Actions for CGORS:

The list of all started CGORs is refresh dynamically each 5 seconds.

Each partner can create a new CGOR and he becomes the “Manager” of this new created CGOR.

The manager can invite other partners to participate in the selected CGOR. The manger can also remove Participants of his managed CGOR.

An invited organisation can accept or reject an invitation to a CGOR.

3.8. CIS installation and configuration

3.8.1. CIS Adaptor Installation

The CIS Adaptor is deployed as a zipped package that contains everything to run the Adaptor. The software itself is an executable jar which contains an embedded tomcat for exposing the REST Endpoints to/from the Application and to/from the CIS Distributor. The CIS Adaptor needs an installed JDK 8 on the machine where it is to be executed.

3.8.2. CIS Adaptor Configuration

The Adaptor needs to know some predefined data that are provided by properties files, located in the config directory which is also part of the Adaptor zip file. Configuration changes are only recognized during the Adaptor startup sequence.

Following configurations need to be done / defined:

On which port is the tomcat listening

server.port = 8090

Distribution config: The Adaptor supports connecting to different distribution environment and also mechanisms for testing; can be FILE, KAFKA, EPISECC, LB

distribution.env=EPISECC

For the EPISECC Distributor the host, port and node configuration (which is responsible for this Adaptor Instance) has to be provided

distributor.hitech.host=api.nextgen-lab.net

distributor.hitech.port=80

distributor.hitech.node=CNSAS

For general communication a default CGOR is used

cgor.default.name=episecc

For which organisation this Adaptor is deployed

cis.org.name=CNSAS-FVG

How is the semantic translation connection, and is the translation enabled or is organisation able to understand the original messages

cis.translate.endpoint=http://taxonomytranslation.iessolutions.eu:3030/TranslationService/services/TaxonomyTranslation/translateCAPToLocal

cis.translate.msg=true

To which schema (language) has the data to be translated

cis.translate.tax.schema=JVP-SPLIT

4. Implementation of legal and ethical requirements

In order to ensure that the general architecture of the CIS is in compliance with the applicable data protection rules and enjoys trust of all parties involved, the CIS should guarantee an adequate level of security that is appropriate to the risks associated with its data processing activities.

The main objective of the CIS is to provide an open-ended exchange tool enabling the interaction and coordination of civil protection assistance in case of a cross-border disaster. For the purposes of the proof of concept (D6.1) it has been agreed to narrow down the number of connected tools to a defined set of data sharing mechanisms. Within the framework of the proof of concept exercise the HITEC and SARONTAR mobile apps and the MDG TETRA devices used by the Slovenian fire brigade will be capturing location data on natural persons that will subsequently propagate throughout the CIS network. All other data processed by the CIS prototype during the proof of concept exercise will be simulated data that do not qualify as personal data in the sense of the EU Data Protection Directive (Directive 95/46/EC). Nevertheless, the processing of these location data will trigger the applicability of the EU Data Protection Directive[7], which means that certain precautions should be taken to ensure the safe and secure handling of the location data within the CIS prototype that will be set up. To this end the consortium has undertaken several steps that will be briefly discussed in this section. First of all, the requirements table of D5.2 was updated to illustrate how the proof of concept integrates these requirements (4.1). Secondly, the consortium engaged in a process of concluding a series of agreements to commit to the secure handling of the location data and other personal data such as pictures and photographs that will be processed during the proof of concept exercise (0).

4.1. Update of the requirements table

While the currently applicable regulatory framework is defined by the EU Data Protection Directive (Directive 95/46/EC), it is recommended to anticipate the more stringent security requirements of the future General Data Protection Regulation (GDPR) which will enter into force on the 25th of May 2018. By doing so the tools provided for the proof of concept exercise will remain privacy compliant when the GDPR becomes enforceable. Article 32 of the GDPR imposes a general obligation, for controllers and processors alike, to implement appropriate technical and organisational measures in order to ensure an adequate level of security for the data-processing. In Deliverable 5.2 a requirements table was set up, drawing from the obligations imposed by article 32 of the GDPR. In the table below we will illustrate how these requirements will be put into practice for the implementation of the proof of concept exercise.

[7]Article 4(1) of the GDPR that will replace the EU Data Protection Directive, explicitly qualifies location data as personal data.

Requirements according data protection regulation

The requirements below stem from a combined reading of the current EU Data Protection Directive and the future General Data Protection Regulation. The table indicates for each of the identified requirements to which extent the CIS is affected and how the requirement is addressed in the CIS architecture.

Table 8: Legal requirements

No.	Requirement description	Measure type
1.	Implement appropriate organisational measures to ensure a level of security appropriate to the risk *Is in the responsibility of the owner (provider) of a CIS. D5.3 proposes appropriate procedures and measures in order to make a CIS instance safe.*	Policy, procedure
2.	Implement appropriate technical measures to ensure a level of security appropriate to the risk. *Is essential part of the architectural design in this document D5.2 (security box, trust handling and registration) and will be implemented in an exemplary way in the CIS prototype D6.2.*	Procedure, practice
3.	Implement appropriate organisational measures for pseudonymisation and encryption of personal data. *All participating organisations and their tools need to be registered and trusted by the owner of CIS (e.g. LEMA).* *The CIS itself does not care about the transmitted data content – this has to be covered by the connected tools and the tool users.*	Policy, procedure
4.	Implement appropriate technical measures for pseudonymisation and encryption of personal data. *All data sent to the CIS is encrypted in order to limit messages to the intended recipients. Specific handling of personal data (e.g. pseudonymisation) is outside the scope of CIS, and stays in responsibility of the connected tools.*	Procedure, practice
5.	Implement appropriate organisational measures ensuring the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and service *The ownership of information shared in CIS always stays with the producer (sender) of the information. Messages sent to CIS are logged and stored locally, on the participants' servers and can be analysed by the owning organisations.*	Policy, procedure

6.	Implement appropriate technical measures ensuring the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and service *The concept of secured CGOR (Cooperation Group Online Room) and the related encryption of all messages is designed to ensure confidentiality and integrity.* *Availability and resilience are considered by the distributed CIS structure, hosted at the participants' servers, and the peer-to-peer message distribution and synchronisation design. This architecture allows the CIS to continue working even if the connectivity is partly down, and to resume the full information after re-connection.*	Procedure, practice
7.	Implement appropriate organisational measures ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident *No specific handling of personal data in CIS itself – it is the responsibility of the participating organisations (see also RQ 3, 5)*	Policy, procedure
8.	Implement appropriate technical measures ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident *No specific handling of personal data in CIS itself – it is the responsibility of the connected tools (see also RQ 4, 6)*	Procedure, practice
9.	Implement appropriate organisational measures ensuring a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing *Not applicable for the EPISECC research project (we are not a "real" CIS provider). The experience gained in the proof of concept exercise will be analysed accordingly in the lessons-learned reports D6.3 and D5.4.*	Policy, procedure
10	Implement appropriate technical measures ensuring a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing *The data traffic in CIS is completely logged in the participants' servers. These log-files will be analysed after the PoC exercise. Specific security tests might be included in the PoC (t.b.d.).*	Procedure, practice

11	Take steps to ensure that any natural person who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. *No specific handling of personal data in CIS itself – it is the responsibility of the participating organisations.* *The CIS is designed for the communication of systems (servers) rather than persons. Personal credentials of users have to be checked by the connected tools. If a tool is a trusted partner, the users of this tool are considered as trusted, too.*	Policy, procedure, practice

4.2. Controller-processor agreements and informed consent forms

In order to assure that all partners involved in the proof of concept exercise will handle the transferred location data in a safe and secure way data controller-processor agreements will be concluded between AIT and all the consortium partners who provide one of the processing tools. In the proof of concept exercise AIT will fulfill the central role of data controller since they are the entity responsible for the overall project management and the coordination of the proof of concept exercise. Consequently, they have a decisive voice in determining the purpose of the data processing, being the proof of concept exercise. The other project partners involved in the proof of concept exercise have developed the software tools that will process the location data and are considered to be data processors acting on behalf of AIT. This means that the other project partners will only process the data concerned on instructions of AIT and will commit vis-à-vis AIT to process the data in a secure and privacy-respecting way. The end-responsibility for the secure data processing and compliance with the applicable data protection legislation will lie with AIT, but in case one of the data processors does not fulfill his obligations under this agreement, AIT can seek compensation from the party in breach of the agreement. To this end AIT will conclude such agreements with each of the tools providers (and thus data processors) involved in the proof of concept exercise.

Secondly, informed consent forms have been drafted and will be handed out. The informed consent forms will legally cover two types of data processing activities. On the one hand the consent will be sought from the physical persons whose location data will be processed. By signing the informed consent form they will provide the required legal basis for the legitimate processing of their location data in conformity with article 7(a) of the European Data Protection Directive and article 6(1)(a) of the GDPR. On the other hand, all other physical persons taking part in the proof of concept exercise will be asked consent to disseminate pictures or videos that could be recorded during the event. The consent form informs the persons involved on their rights and of the possibility that such images could be used as dissemination materials to promote and raise stakeholder awareness concerning the outcomes of the EPISECC project.

5. Operational interoperability in the Proof of Concept

This Proof of Concept aims to demonstrate the interoperability between heterogeneous tools. As we focused on creating a Common Information Space, we made following assumptions:

- All organizations involved for the Proof of Concept applied and registered to the EPISECC project
- Each login provided by users is virtual and do not represent a real usable login on a production environment. Users are created only for exercise purpose
- Each tool operator was or will be given a proper training before the proof of concept to ensure that he is able to conduct the proof on concept steps efficiently
- Each partner involved in the proof of concepts represents an organization fully trusted by other participants
- The name of the participants will be disclosed to all partners as their identity are not hidden to other responders when safety messages are sent to CIS (DISP danger zone alerts)

Before the CIS implementation, organizations needed to coordinate themselves by relying on phone communications and documents shared through faxes and emails. The CIS simplifies these exchanges as tactical information can be followed directly by each partner despite operating different tools. Plus, the standards used to communicate within the CIS support file transfer, which implies that the CIS becomes a centralized place where documents can be exchanged directly and more efficiently. This collaboration process aims to reduce the decision-making duration and improve response efficiency.

Bibliography

[1] EPISECC deliverable, D6.1 Proof of Concept Design, 2016.

[2] EPISECC deliverable, D5.2 Informational Interoperability Specification, 2016.

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

[4] EPISECC deliverable, D5.3 Operational Interoperability, 2017