Cloud-based Semantic Services for Pan-European Emergency Preparation and Planning

Christina Schäfer, Torben Sauerland,
Jens Pottebaum, Robin Marterer
C.I.K.
Faculty of Mechanical Engineering
Paderborn University, Germany
Email: {schaefer, sauerland, pottebaum, marterer}@cik.upb.de

Daniel Behnke, Christian Wietfeld
Communication Networks Institute (CNI)
Faculty of Electrical Engineering and Information Technology
TU Dortmund University, Germany
Email: {daniel.behnke, christian.wietfeld}@tu-dortmund.de

Peter Gray, Bogdan Despotov
CloudSigma
Email: {peter.gray, bogdan.despotov}@cloudsigma.com

***Abstract*—Todays emergency management especially in cross-border incidents is still underlying communication and interoperability barriers. By the introduction of a Common Information Space (CIS) as a socio-technical system, concepts for bridging between involved first responder and Police Authorities becomes evident. Within this paper technical elements of the concepts are described to also demonstrate the practical realization of a CIS.**

I. Introduction and Motivation

If a training exercise planner gets the task to develop new ways for training or significant scenarios to be prepared for, i.e. against larger CBRN incidents, an odyssey of search and grapping pieces of information begins. The planner starts to search similar incidents but also involved organisations in these events, even in other countries. To support this work a trusted system to ensure adaquate information exchange between first responder is needed.

Fig. 1. Basic Scenario

SecInCoRe envisions a Common Information Space (CIS) as a socio-technical system, co-designed and co-developed between end user, researcher and designer, to support first responders and Police Authorities in emergency management. The overall concept of a common information space was introduced by Bannon in the early 9os: "Cooperative work is not facilitated simply by the provision of a shared database, but requires the active construction by the participants of a common information space where the meanings of the shared objects are debated and resolved, at least locally and temporarily." [1]. Even in this definition the relevancy of CIS participants' involvement and a required common understanding about terminology and procedures become obvious. To overcome this situation, several technical components and socio-based concepts of a CIS have to fit together. This task has been addressed by the SecInCoRe project. The development of a modular CIS concept, adaptable to the needs of the respective end user groups and proofed with the development of reference implementations are in line with the project objectives (see www.secincore.eu). The different concepts and respective reference implementations will be introduced within the paper using the task for an exercise planner as reference scenario.

II. Current State of Technology: Lack of Communication and Interoperability

Lack of communication and / or interoperability within and between different organizations is a crucial problem for first responder and Police Authorities. Even in the same country information are often not shared consequently. In cross border incidents the lack of information exchange becomes even more evident.

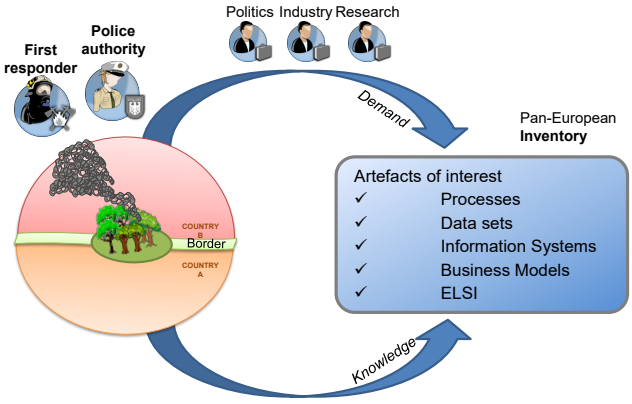

Fig. 2. Lack of Information Sharing

Fig. 2 depicts the demand and availability of information. To identify the state of the art and missing parts of information sharing practices, the SecInCoRe project conducted an inventory of past disaster, processes used in emergency management and also available information and communication systems. This leads to comprehensive overview about available

technologies in that domain. Results are public accessible via secincore.eu/search. Another point of interest is to identify used standards to exchange information in response but also in preparation. In the preparation phase data is less standardized and in many cases the exchange is related to personal contacts. These circumstances enforces the need-ability of SecInCoRe to rely on the vision of a socio-technical system and elaborate the CIS.

III. Socio-technical CIS Concept design and visualizations

The essence of SecInCoRe is the development and documentation of a socio-technical concept design. In [2] the CIS concept, as depicted in Fig. 3, was introduced and the main components of the CIS concept were outlined. The intention of the concept design is to enable interaction and cooperation for the emergency services.

In *Reference Implementations* the *CIS Specification* is converted into a living system which is used for demonstration and evaluation purposes.

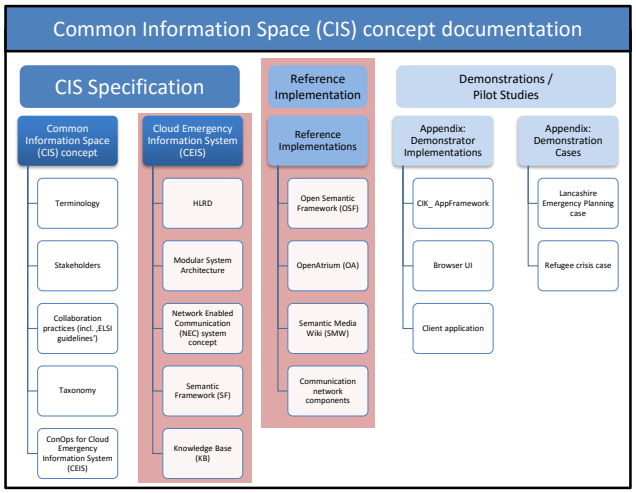

Fig. 3. CIS concept - Red components are in focus of this work

The complexity of the *CIS Specification* as a documentation for a socio-technical system constitutes the need to adapt the concept visualizations to address different stakeholder groups. In order to implement the concept on a pan-European level decision makers regarding politics, technology and end users have to be identified. To start with the grassroots, a visualization was derived based on the original CIS concept that address the benefits of using a CIS and the potential for upcoming collaboration between existing and new partnerships. This visualization is shown in Fig. 4. Here technical aspects are grouped to a modular system architecture and further social elements are combined to define a framework to enable a trusted and useful CIS. Based on this flexible assembled CIS in relation to elements integrated in the system architecture or defined in rules or guidelines of the CIS, the overall benefits become visible.

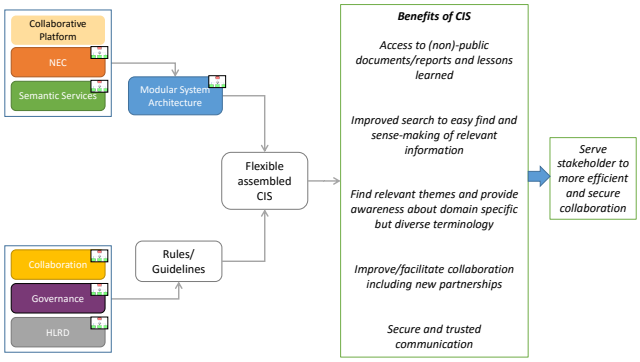

Fig. 4. Benefit oriented Visualisation

In a next step relevant themes are addressed in a visualization to highlight various parts of a CIS. Fig. 5 depicts the five-pillar model of the CIS, the pillars address different aspects of the concept and therefore different stakeholders as well.

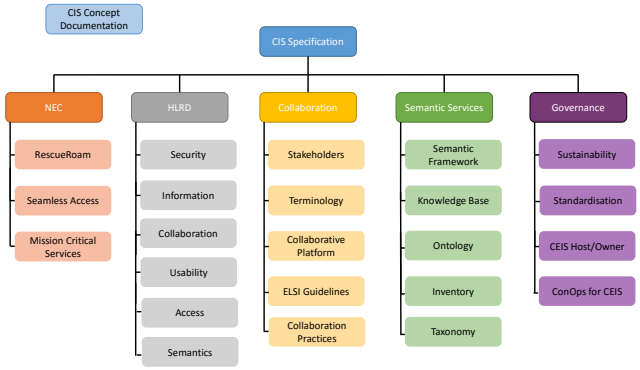

Fig. 5. Theme-based CIS Visualization

All pillars are described and explained in detail in the *CIS Concept Documentation*. In Tab. I the pillars are connected to stakeholders and interest groups which have been identified. The intention is to present more details of the relevant pillar(s). The mentioned *Reference Implementations* explained in the following sections help to demonstrate the functionalities of the system and hence, provide a better understanding of the concept in general.

The following Table link interest groups with the identified pillars before and hence give a first hint how the adaption to specific requirements happen. But the assignment is not limited to the stakeholders. By focusing on dedicated end user needs the demonstrator implementations can be realized to match these needs during the evaluation of the concept.

To visualize the foreseen reference implementations in detail the system architecture is presented in Fig. 6.

The Figure gives a compact overview about the technical connections within SecInCoRe. The end user uses the NEC to access the collaboration platform, where the Semantic Framework enables an integrated access to the contents of the Knowledge Base.

The first step to access the SecInCoRe system is to use

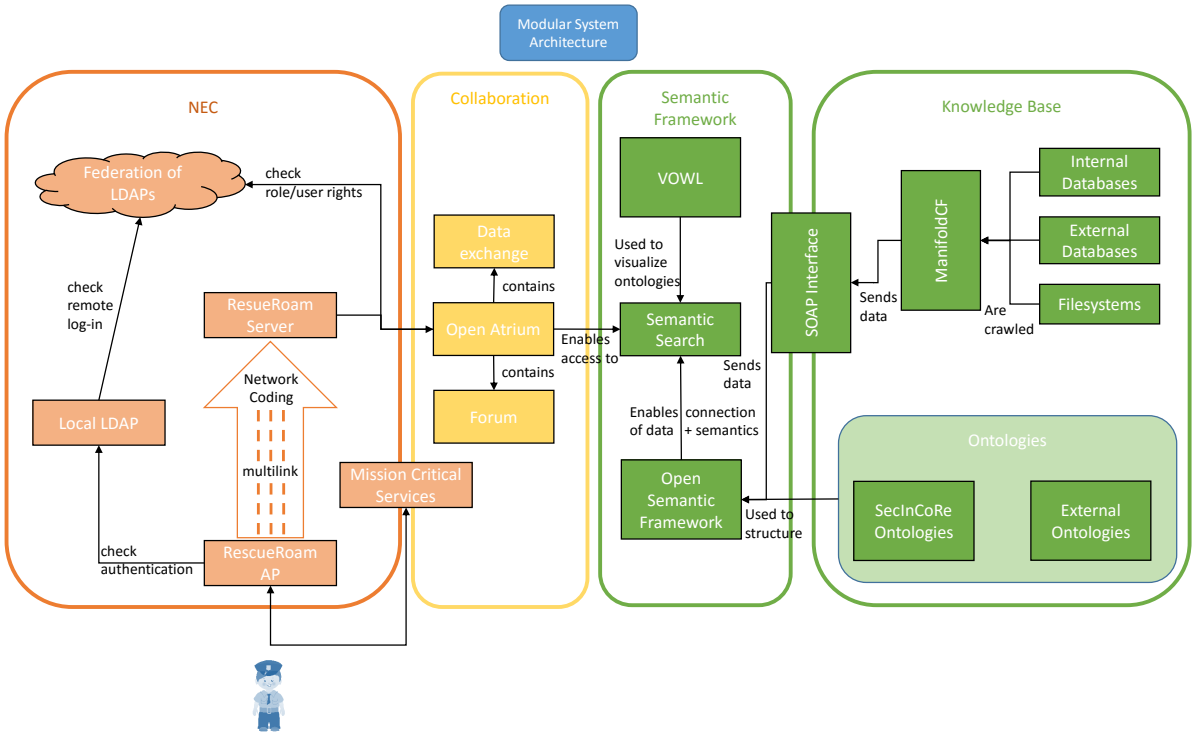

Fig. 6. System Architecture

TABLE I
STAKEHOLDER IDENTIFICATION

Pillar	Stakeholders
RescueRoam	Engineers, e.g. JRC
High Level Requirements Documentation	Engineers, Management
Collaboration Practices	End-users, Management
Semantic Services	Engineers, End-users
Governance	Decision-makers, e.g. ERCC

the RescueRoam access point, to connect with the Mission Critical Services and using the multilink and network coding the RescueRoam server. After the credentials are checked with LDAP servers, the collaboration platform can be accessed. Open Atrium contains functions as a forum, data exchange capabilities and the connection to the Semantic Search. The Semantic Search combines data and structuring approaches from different sources mainly from the Knowledge Base: Different databases and filesystems are crawled with ManifoldCF to collect all data which should be searchable. To structure the data, SecInCoRe and external ontologies are integrated. The Open Semantic Framework integrate the data and the ontologies and provides the backend for the Semantic Search. After that the VOWL component is used within the Semantic Search, to demonstrate the connection of the ontologies and the data, enabling a Graph View.

All elements of the architecture are described in more detail in the following section.

IV. Reference Implementations to Provide Semantic Services

A. Knowledge Base

The Knowledge Base is constituted as a living system including a data layer and a semantic layer. Several internal and external data bases are consolidated. Together with other kinds of data sources these mentioned databases build the data layer of the knowledge base. The results of the state of the art analysis (Inventory of data sets, processes and information system) are an significant part of the Knowledge Base.

Fig. 7. Grass-root of information

Fig. 7 references to the reference scenario demonstrating the needs of first responders for different data sources and data types. Existing plans, related incidents but moreover, contacts to other first responders or Police authorities are required. Trust in information is directly linked to trust in the person who provides this information. The SecInCoRe project gathers data in accordance to used or available information and communication systems, information management processes and business models. This inventory was used to identify structures and hence define database models to store the data in the Knowledge Base.

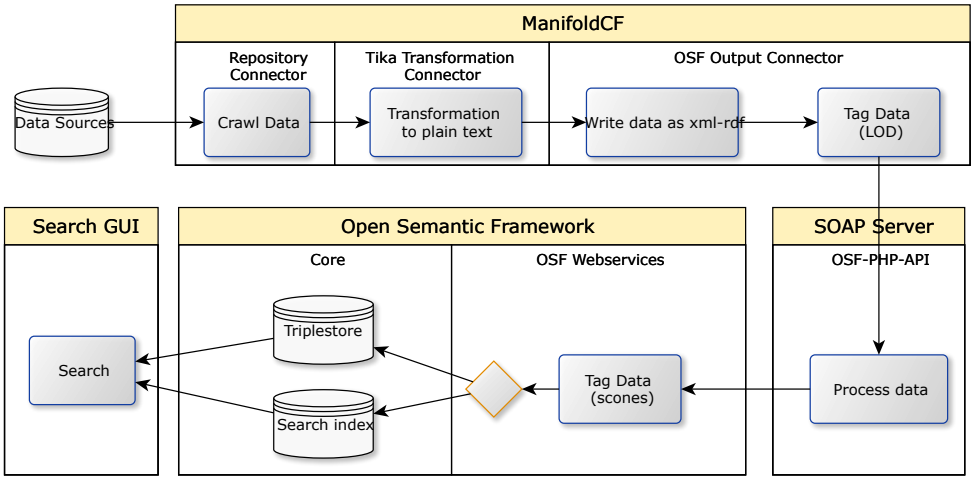

Fig. 8. Data Crawling

The semantic layer describes relationships and crosslinks between the inventory data using an ontology (based on the SecInCoRe taxonomy). The SecInCoRe ontology was also created by reusing existing vocabularies, glossaries and semantic approaches.

Fig. 8 shows the process of crawling data from different data sources and the data provisioning to be used in the semantic framework. This demonstrates the cross-link between the Knowledge Base and the semantic framework, described later on in this work. In the crawler *ManifoldCF*, a new repository connector is created for the respective database e.g. of representative disaster events as required by the exercise planner. This connector crawls the database in defined timeslots. The data is not processed by the Tika plain text extraction, as the database is already in a readable format. The data is sent to the Open Semantic Framework Output Connector, which writes the data in a xml-rdf format and sends them to a SOAP Server. There the data could be translated, if needed. In the following, the data is tagged with concepts, which are found in the SecInCoRe ontologies. When the data is processed, every row of the database is stored in Open Semantic Framework e.g. as a record of the dataset representative disaster events. The storage is done in a triplestore and in the search index. Therefore, the data is accessible in a semantic readable format as well as searchable through a keyword search. Further functions connected to the semantic framework are described in the section below.

B. Network-Enabled Communication

The Network-Enabled Communication system provides secure and resilient access to the Knowledge Base and the underlying services and hence, is an enabler for the usage of semantic services and community interaction. One core concept of the NEC is the establishment of a RescueRoam access network for all European emergency services.

Maintaining on the already mentioned example of the planner of a training exercise, the need to collaborate with various emergency services and therefore a requirement for getting internet access on foreign fire stations become evident (cf. Fig. 9).

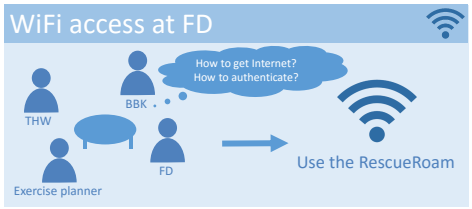

Fig. 9. UseCase for RescueRoam

The RescueRoam concept describes a federated communication system which enables the usage of the SecInCoRe Knowledge Base from different locations. More concrete it is the aim to provide network capability using the same user credentials (WiFi-Access + SecInCoRe Knowledge Base Access - Single-Sign-On) at Fire Station A, Fire Station B, etc. It adapts the eduroam concept [3] to the special needs of emergency services.

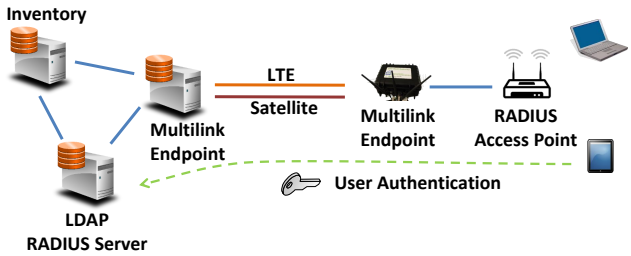

Fig. 10. Network Enabled Communication concept

Fig. 10 depicts the NEC system architecture. The Inventory and the LDAP Radius server as accounting component represent the cloud-based CEIS. On the other side, a Radius-based WiFi access point connects the users to the CEIS. The connection will be managed by a multilink component.

The RescueRoam concept describes principles how to setup such a system and what requirements have to be fulfilled.

In order to demonstrate the benefits of such approach the RescueRoam reference implementation (R^3I) is setup. The R^3I consists of one or many LDAP directories which provides the user account management, a RADIUS server which is used to identify the Wi-Fi Access Points and the access points themselves. Combining these components users can login to the Wi-Fi network and access the Knowledge Base.

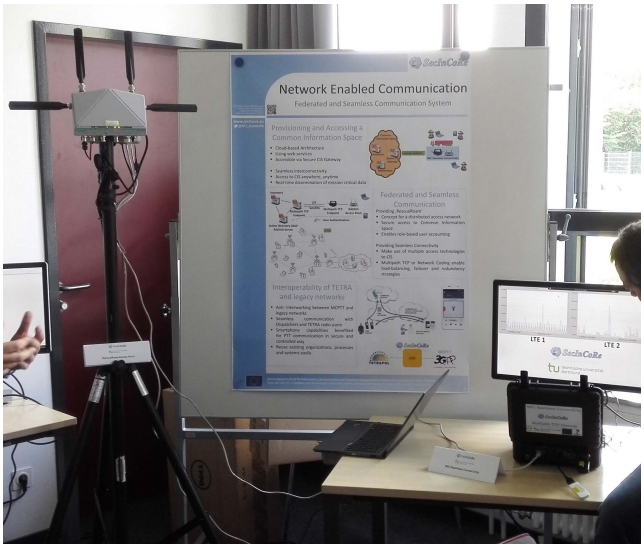

Fig. 11. NEC demonstration during 2nd Review Meeting

Seamless communication is strongly connected to a dynamic and reliable network and communication link management combined with intelligent failover mechanisms and network monitoring tools. The secure access and resilient access is realized using methodologies like Network Coding [4] and Multipath TCP (MPTCP) to enable the use of different radio communication technologies, e.g. WiFi and LTE.

MPTCP [5] is an extension of TCP, using multiple TCP flows for transmission. One master flow is divided in several sub flows that are handled dynamically and are using various wireless interfaces. Currently, some network parts could block signaling traffic, because of missing MPTCP features.

Fig. 11 shows the setup of Multipath TCP and RescueRoam on the first day of the 2nd review meeting. An embedded PC was connected to the Internet via two mobile LTE modems. The RescueRoam access point was connected to that Internet gateway providing the WiFi for the participants of the meeting. On the embedded PC MPTCP was running in order to improve the stability and reliability of the Internet connection. The effect was demonstrated using a shielding box to shield one modem. Connection was ongoing on the other modem.

Besides MPTCP, the transmission principle of Network Coding is used. When a document is requested from the Knowledge Base, the data is splitted into different data packets filling an encoder buffer. When this buffer is full, Network Coding takes place. The content of packets in the buffer is analyzed at the same time, encoding it by mathematical algorithms. Afterwards the packets are transferred using the multiple available communication links. In order to increase the reliability of the transmission despite possible channel noise, which leads to packet errors, the Network Coding is creating additional packets.

On the receiving node, a decoding buffer is filled with incoming data packets. For a generation size of 16 packets, at least 16 packets have to be received for this generation. Afterwards, the decoding process is started and the gained information is forwarded to the application layer. Each successful decoded generation is acknowledged to the sender by an message containing the generation ID.

Fig. 12. Network Coding reference implementation

A Network Coding reference implementation was demonstrated during the 3rd Advisory Board Meeting of SecInCoRe (cf. Fig.12). The setup contains a Laptop representing the cloud-based inventory and an embedded PC in rugged box representing an Internet gateway box. These two components were connected using two wired Ethernet connections via a network switch. With a Qt-based graphical interface the experiment setup was parameterized. The available parameters are the packet error rate for both links, the size of sent data and the number of reliability packets for Network Coding using smooth parameterization between a reliable and a fast setup. For the Network Coding the kodo [6] library was used.

C. Semantic Framework

The Semantic Framework is an approach to cope with four main problems with information exchange in the emergency domain. The information within the domain is:

- Distributed - The information about domain specific topics is stored in most cases at the level of different emergency organizations within the EU. Mostly on a municipal or county level. Therefore, there are thousands of data sources out there.
- Unstructured - The information is stored in an unstructured way. There are different file types with plans, lessons learned, reports etc. with no comparable layout to save all this information.

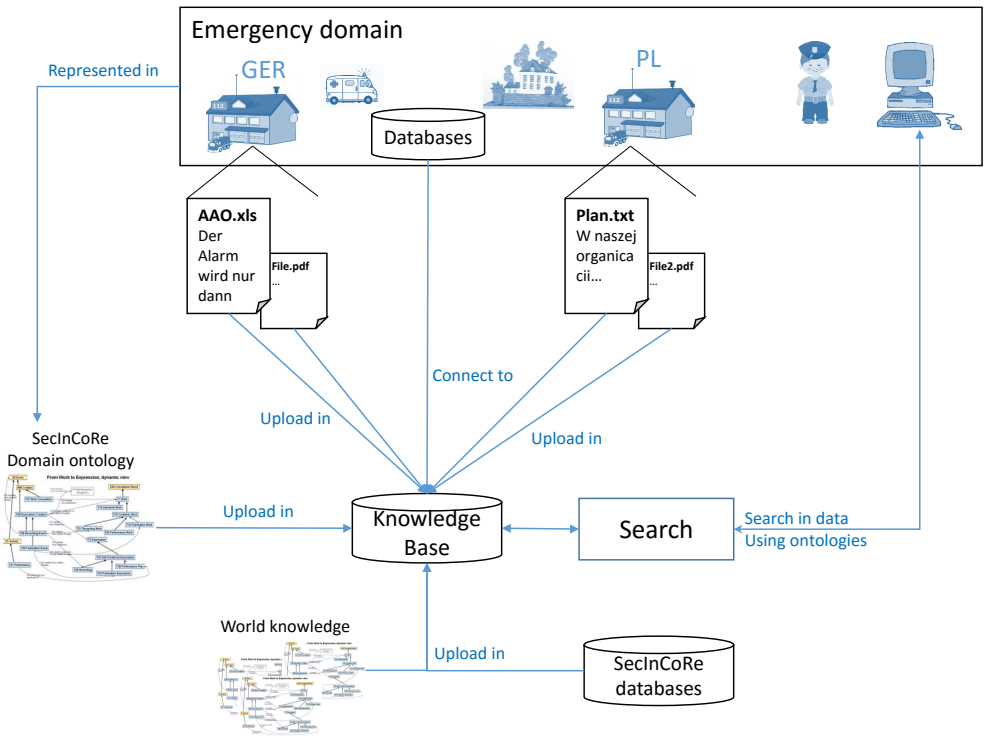

Fig. 13. Semantic Services

- Multi-lingual - Many people within the emergency domain are speaking English, but the working language is in nearly all organizations the national language. Working documents or results are not saved in English and therefore not readable by foreigners.
- Restricted - Information has different levels of sensitivity. Organizations care at different levels about the security of different parts of their data. A common phenomenon is information, which is not really restricted, but should not be public for everyone as well. It is more like sensitive data, which should mainly remain within the domain.

Overview

To address these problems, the Semantic Framework (cf. Fig. 13) is created as a set of organizational concepts and analysis methods. The data in the domain is stored either in databases or in file systems, spread among all organizations The data is inserted into the Knowledge Base either connecting the databases directly or uploading the contents of the file systems In addition to these data sources, the SecInCoRe databases are connected to the Knowledge Base. Within SecInCoRe different ontologies and semantic approaches were developed, representing broad parts of the emergency domain. These ontologies as well as semantic approaches representing the world knowledge are used to structure the data within the Knowledge Base. Finally, members of the domain could search within the Knowledge Base using the Semantic Search.

Hosting

This process is organizational supported by establishing a CIS within a group of organizations within an EU-nation. This CIS is established by one managing authority, which has to be capable to manage such a system, is able to accept the responsibility to run it and is very trustworthy in the eyes of potential participant organizations Caused by these requirements, the managing authority has to be on a national level or lower and a governmental institution (e.g. the national home office). Different national systems could be connected to a bigger i.e. European conglomerate managed by a European body, where the details of responsibility and data exchange should be negotiated among the different managing authorities

Analysis

After the CIS is established and the data is collected in the Knowledge Base, several analysis steps are done, to enable foreigners to get at least an overview of the collected documents. First the data is translated, if they are not in English to enable the semantic analysis to work. After that the datasets are analyzed, to generate a summary, find the main topics of it and to categorize the datasets within the PPDR domain taxonomy, explained above. Using these approaches, foreign people can get a short overview what a dataset is about. Adding the information about the origin organization and the author of the dataset, all members of the CIS can get in contact with the author. The Semantic Framework enables the exchange of information and the establishing of new contacts within the emergency domain. One example for this analysis is shown in Fig. 14.

Technical implementation

The technical core of the Semantic Framework is the

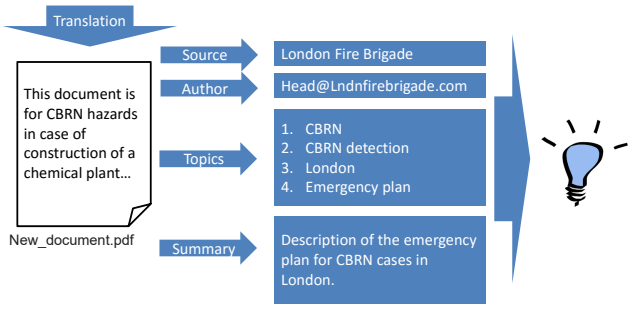

Fig. 14. Semantic Framework Analysis

Open Semantic Framework (OSF) [7]. In this component, all Knowledge Base content is stored RDF-based to enable the semantic search in them. After that, the content analysis using the SecInCoRe ontology (described above) is done by this component. The OSF consists of several separate components (as the Virtuoso triple store as RDF storage, a Solr Search Index etc.) which offers the functionalities on strong interaction. The whole system consists of several components which communicate through a common interface. The GUI is the frontend component which allows to search for document contents and displays the results and the details of each document (e.g. summary, topics etc.). Additionally, it provides the ability to filter the search results based on the ontology which is used in the OSF system for indexing and searching. In addition, the GUI has a view for the upload of documents from a file system. The OSF system and the GUI are connected via the OSF-PHP API that is an abstraction layer to the underlying OSF-Webservices, which contains methods for the creation, update, deletion, read, and search of records. ManifoldCF is responsible for crawling and processing the documents and database entries and accesses the previous mentioned PHP API to store the processed documents in the Open Semantic Framework.

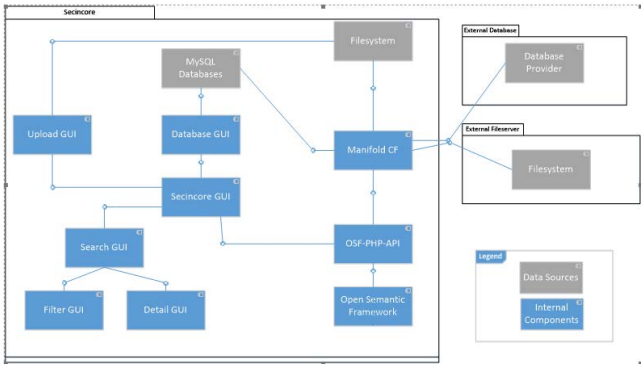

Fig. 15. ManifoldCF

V. Conclusion and Future Work

In this work we introduced an innovative concept for a socio-technical system providing cloud-based semantic services. We focused on the technical design principles and used reference implementations to demonstrate the system's benefits and evaluate the concept in strong cooperation with emergency services as the upcoming end-users of such a system. We developed a methodology using different visualizations of the common information space concept to disseminate the results of the project and to overcome the valley of death of research projects.

Acknowledgment

The research leading to these results has received funding from the European Union Seventh Framework Program (FP7/2007-2013) under grant agreement n°607832 (project SecInCoRe). The text reflects the authors' views. The European Commission is not liable for any use that may be made of the information contained therein. For further information see http://www.secincore.eu/.

References

[1] Schmidt, Kjeld, and L. Bannon, "Taking cscw seriously: Supporting articulation work," vol. 1, pp. 7–40, 1992.

[2] J. Pottebaum, C. Schäfer, M. Kuhnert, D. Behnke, C. Wietfeld, M. Büscher, and K. Petersen, "Common information space for collaborative emergency management," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, May 2016, pp. 1–6.

[3] K. Wierenga, S. Winter, and T. Wolniewicz, "The eduroam architecture for network roaming," RFC 7593, http://www.rfc-editor.org/info/rfc7593, Tech. Rep., 2015.

[4] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "Xors in the air: Practical wireless network coding," *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, pp. 497–510, June 2008.

[5] (2017, 02) Multipath tcp - linux kernel implementation. [Online]. Available: https://www.multipath-tcp.org/

[6] (2017, 02) Kodo network coding library. [Online]. Available: http://steinwurf.com/products/kodo.html

[7] (2017, 02) Open semantic framework. [Online]. Available: http://opensemanticframework.org/