



SECURE DYNAMIC CLOUD FOR
INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY
BASED ON PAN-EUROPEAN DISASTER INVENTORY

Deliverable 4.4

Report on Interoperability Aspects

Daniel Behnke¹, Tobias Kleinschmidt¹, Niklas Goddemeier¹, Matthias Priebe¹, Christian Wietfeld¹, Christina Schäfer², Torben Sauerland², Jens Pottebaum², Olivier Paterour³, Peter Gray⁴, Bogdan Despotov⁴

¹Technical University Dortmund/CNI, ²Universität Paderborn/CIK, ³Airbus Defence and Space, ⁴CloudSigma

February 2017

Work Package 4

Project Coordinator

Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme

for Research and Technological Development

COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems
and data set used by first responders and police authorities



Distribution level	Public
Due date	28/02/2017 (due month 34)
Sent to coordinator	
No. of document	D4.4
Name	<i>Report on Interoperability Aspects</i>
Type	<i>Report</i>
Status & Version	<i>0.11</i>
No. of pages	<i>64</i>
Work package	<i>4</i>
Responsible	<i>TUDO</i>
Further contributors	<i>UPB, CS, ADS</i>
Authors	<i>Daniel Behnke, TUDO Tobias Kleinschmidt, TUDO Niklas Goddemeier, TUDO Matthias Priebe, TUDO Christian Wietfeld, TUDO Christina Schäfer, UPB Torben Sauerland, UPB Jens Pottebaum, UPB Olivier Paterour, ADS Peter Gray, CS Bodgan Despotov, CS</i>



Keywords		<i>Taxonomy, Communication System, Semantic Modelling, Secure Cloud, Mission-Critical Services</i>		
History	Version	Date	Author	Comment
	V 0.1	01/04/2015	TUDO, MK	Initial version
	V0.2	08/06/2015	TUDO, MK	update
	V0.3	11/06/2015	TUDO, MK	Integration of Input from UPB
	V0.4	31/05/2016	UPB	Shift exchange format content from D6.2 to D4.4 (PRML and xHelp)
	V0.5	06/10/2016	TUDO	Updated structure
	V0.6	02/01/2017	TUDO	Integrated input from UPB, CS, ADS
	V0.7	06/01/2017	TUDO	Updated structure, fixed format, updated communication chapter
	V0.8	09/01/2017	TUDO	Draft for review
	V0.9	31/01/2017	TUDO	Integrate updated UPB input
	V0.10	22/02/2017	TUDO	Integrate AB meeting input
	V0.11	24/02/2017	TUDO	Integrated QA review and monitoring comments

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.



Authors



TU Dortmund
CNI

Daniel Behnke

Email: daniel.behnke@tu-dortmund.de

Tobias Kleinschmidt

Email: tobias.kleinschmidt@tu-dortmund.de

Niklas Goddemeier

Email: niklas.goddemeier@tu-dortmund.de

Matthias Priebe

Email: matthias.priebe@tu-dortmund.de

Christian Wietfeld

Email: christian.wietfeld@tu-dortmund.de



University of Paderborn
C.I.K.

Christina Schäfer

Email: c.schaefer@cik.upb.de

Torben Sauerland

Email: sauerland@cik.upb.de

Jens Pottebaum

Email: pottebaum@cik.upb.de



Airbus Defence and Space

Olivier Paterour

Email: olivier.paterour@cassidian.com



CloudSigma

Peter Gray

Email: peter.gray@cloudsigma.com

Bogdan Despotov



Email:

bogdan.despotov@cloudsigma.com



Reviewers



CloudSigma

Peter Gray

Email:

peter.gray@cloudsigma.com



T6 Ecosystems

Simona De Rosa

Email: s.derosa@t-6.it

ELSI Monitor



Lancaster University

Monika Buscher

Email:

m.buscher@lancaster.ac.uk



Executive summary

This deliverable scopes the final results of WP 4. Therefore, many aspects of the deliverables D4.1, D4.2 and D4.3 are taken up here. The main focus is on interoperability aspects to foster the developments of a cloud emergency information system and to enhance collaboration between different emergency organisations.

WP4 has strong interconnections to WP2, WP3 and WP5. The understanding of ethical, legal and social issues (ELSI) as provided by WP2 has direct impact on the technological research and development. ELSI have been considered during concept development and are part of the final concept descriptions.

The creation of a Pan-European inventory in WP3 raises the question of analysing and accessing this data. A secure dynamic cloud has to provide secure access to such a data base and provide access via highly-sophisticated search algorithms.

One aim of SecInCoRe is to present verification results of the developed concepts. Hence, the developed conceptual results of WP4 are transferred to reference implementations used for validation as described in the deliverables in WP5. This is the distinction between D4.4 and D5.4/D5.5. In the latter deliverables, the reference implementations are described in more details. In D4.4 the focus is on presenting the final concepts and first scientific results.

The deliverable is structured in six chapters and the literature index:

- Chapter **one** introduces the purpose of this document. Furthermore, the relation to other SecInCoRe deliverables is presented as well as a glossary and a list of figures.
- In chapter **two** the taxonomy research is presented. It starts with the depiction of the final taxonomy in the domain of SecInCoRe. Starting there, an ontology is derived and its usage in the semantic search is described. Visualisation concepts for validation purposes are presented as well.
- With the expiration of SecInCoRe the promotion and sustainability of the project results become urgent. In chapter **three** different approaches of Common Information Space (CIS) visualisations are given. The aim is to present the set of concepts in a general holistic view but go into the details depending on the target audience that is addressed. Additionally, the final system architecture is described here as well.
- Part of the Cloud Emergency Information System (CEIS) is the secure and reliable access to the cloud and its services as presented in D4.3. Chapter **four** introduces the final concepts for a seamless communication platform, the RescueRoam concept for a distributed and easy-to-use WLAN-based access network and novel developments regarding mission-critical push-to-talk services.
- In order to gain the potential users trust, the security and integrity of the provided data is a very important aspect. In chapter **five** methodologies are presented to ensure the security of the cloud and its services. The cloud architecture is developed considering potential threats for the cloud integrity and SecInCoRe's



answers to these threats. The secure access is strongly connected to the communication system presented in the previous chapter.

- In the previous chapters, cloud services, semantic search services and the communication system to use these services have been introduced. Besides the pure possibility to connect to a cloud system, the protocol and the format of the data transmission is of importance as well. In chapter **six** several data exchange languages are introduced and analysed.



Table of contents

1	Introduction	9
1.1	Purpose of this document.....	9
1.2	Validity of this document.....	9
1.3	Relation to other documents.....	9
1.4	Contribution of this document.....	10
1.5	Target audience	10
1.6	Glossary	10
1.7	List of figures	11
2	Taxonomy	12
2.1	Final version of Taxonomy	12
2.2	Defining new relations	16
	2.2.1 Results of semi-automatic alignment methods and tools	17
	2.2.2 Alignment methodology in SecInCoRe	17
2.3	Application of Taxonomy	19
	2.3.1 Ontologies in the Semantic Search.....	20
	2.3.2 Find proper results	21
	2.3.3 Interpret the results	24
	2.3.4 Sustainable ontology.....	25
2.4	Internal Verification and Validation of Taxonomy	25
3	CIS Concept Visualisation	32
4	Seamless and secure communication system.....	37
4.1	Seamless communication platform.....	37
4.2	RescueRoam Architecture.....	46
4.3	Single Sign-On using OpenLDAP under Linux	47
4.4	MCPTT & MCS.....	47
5	Cloud Security	50
5.1	Secure Cloud Architecture.....	50
5.2	Secure Cloud Access	54
6	Pan-European Information Exchange.....	55
6.1	Protection and Rescue Markup Language (PRML)	55



6.2	xHelp and DIN Spec 91287	56
6.3	Further approaches	58
7	Conclusion.....	60
8	Literature index	61



1 Introduction

SecInCoRe envisages a Common Information Space (CIS) for cooperation and collaboration among all relevant stakeholders in all phases of crisis management, based on an intense interoperability analysis focusing on first responder organisations and Police authorities. WP4 focuses on the conceptual design for the semantic framework incl. the taxonomy, secure cloud services and the Network Enabled Communication.

1.1 Purpose of this document

In this document, the final design of the taxonomy and the communication system is presented. Therefore, the authors consolidate the concepts and methodologies introduced in the deliverables D4.1, D4.2 and D4.3.

The purpose of this document is to provide the technical design principles for a secure dynamic cloud in the domain of emergency services.

1.2 Validity of this document

Most aspects of the secure cloud system are validated using reference implementations (cf. D5.4). In this deliverable the main ideas and technical basics of the implementations are introduced to allow for a reproduction of the different system components. Hence, the description should be complete and understandable for a scientific and engineering audience.

1.3 Relation to other documents

The Relationships with other documents created as part of the SecInCoRe project include a general framing through:

- [1] Grant Agreement
- [2] Consortium Agreement
- [3] Description of Work (DOW)

Further, this document has relationships with other documents created within the SecInCoRe project. The following documents are referred to in terms of foreground literature:

- [4] D2.7 ELSI in crisis management through the Secure Dynamic Cloud (Drafts of this deliverable and implementation at isITethical.eu)
- [5] D3.3 Second publication of inventory results including ethnography and holistic process models and statements on future evolutions
- [6] D4.1 Requirement Report
- [7] D4.2 System Views and Concept of Operations (CONOPS)
- [8] D4.3 Network enabled communication system concept and common
- [9] D5.1 Common information space for internal use



- [10] D5.3 Validation strategy and first functional evaluation model of communication system concept
- [11] D5.4 Validation report and final evaluation model of communication system concept

The outputs described in this document are related to further activities in WP4 as well as validation and evaluation activities in WP5 and standardisation activities in WP6 and are therefore related to the following documents directly:

- [12] D5.5 Evaluation and Validation report for SecInCoRe stakeholders
- [13] D6.4 Standardisation, Exploitation and Dissemination Report

1.4 Contribution of this document

In this document the authors provide the description of the design for the technical implementation of a cloud-based emergency information system. Therefore, different aspects will be addressed.

A technical implementation of the ideas behind a common information space as described in e.g. D4.2 has to consider various components. The domain-specific taxonomy and its technical representation, and the ontology build the basis for highly-sophisticated document analysis and search. The communication system lays the foundation for the interaction with the cloud services. Access to the cloud system has to be provided under different environmental circumstances.

Security plays an important role in building trust in using cloud services. The secure cloud architecture and the federation of access servers is introduced to describe the efforts performed to build trust.

1.5 Target audience

The document is public and of relevance for engineers and scientist using this work as a basis for the implementation of a cloud based emergency information system.

1.6 Glossary

Abbreviation	Expression
3GPP	3rd Generation Partnership Project
CEIS	Cloud based Emergency Information System
CIS	Common Information Space



DoW	Description of Work
ELSI	Ethical Legal and Social Issues
FoI	Freedom of Information
LTE	Long Term Evolution (of 3GPP)
MCPTT	Mission Critical Push To Talk
NEC	Network enabled Communication

1.7 List of figures

Figure 1 Taxonomies overview	12
Figure 2 Workshop approach	13
Figure 3 Extract of the process chain during the arrival of refugee in Dortmund (perspective of the fire department of Dortmund).....	15
Figure 4 Extract of the process chain to prepare for a soccer game	16
Figure 5 Web-Protégé project	18
Figure 6 Extract of documentation of new relations	19
Figure 7 Extract of Relation definitions.....	19
Figure 8 Overview of the Semantic Search.....	20
Figure 9 Setting filters in the search process	21
Figure 10 Activate GraphView	22
Figure 11 GraphView functionality	23
Figure 12 SecInCoRe ontology	24
Figure 13 Topic and abstract.....	25
Figure 14 CIS concept.....	32
Figure 15 Theme-based visualization approach [Sch17]	33
Figure 16 Benefits-oriented visualization approach [Sch17].....	34
Figure 17 Component-based visualization approach [Sch17].....	35
Figure 18 Modular system architecture visualisation [Sch17].....	36
Figure 19 Seamless communication in SecInCoRe	37
Figure 20 Network Enabled Communication architecture	38
Figure 21 Mobility management and handover solutions at different layers	39
Figure 22 RescueRoam & Multipath TCP demonstration during 2nd review meeting.....	40
Figure 23 MPTCP Laboratory demonstration during 2 nd review meeting	41
Figure 24 MPTCP Laboratory setup.....	41
Figure 25 Network Coding in SecInCoRe [Sch17]	43
Figure 26 Network Coding setup during 3rd Advisory Board Meeting	43
Figure 27 Parameterization of Network Coding	45
Figure 28 Data transmission via two channels with 25% packet error rate	46
Figure 29 ETSI TCCE MCS-Tetra Interworking	48
Figure 30 Information exchange using a cloud-based system	55
Figure 31 First layer of PRML structure (PRML.xsd)	56
Figure 32 Three core elements of xHelp: a) Ontology, b) Process model, c) data format.....	57
Figure 33 Reference implementation for DIN Spec 91287	58

2 Taxonomy

The following chapter demonstrates the progress and final research results dealing with taxonomy and ontology in the SecInCoRe project. The approach to define new relationships will be described in detail, further the embedded ontologies are introduced, and the use in semantic services.

2.1 Final version of Taxonomy

As depicted in the previous deliverable D4.3 the main objective in deriving taxonomy is based on the defining of relationships in existing ones as shown at a meta-level in the following Figure.

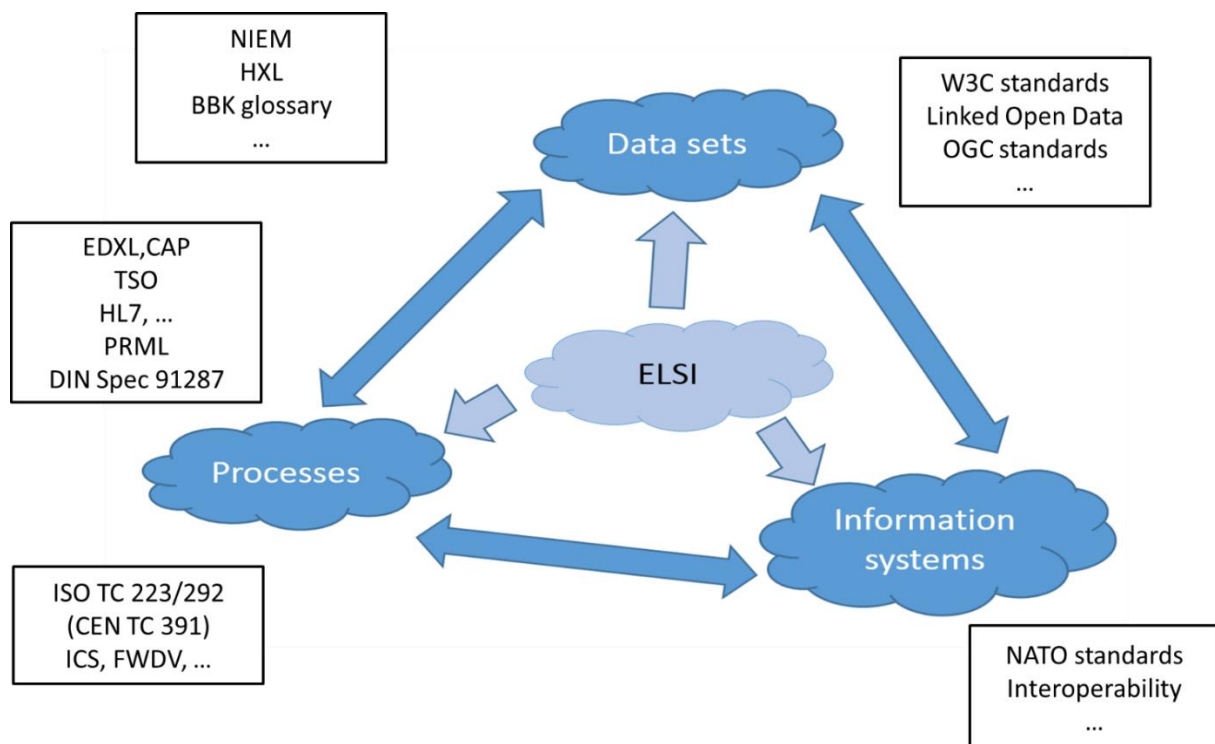


Figure 1 Taxonomies overview

In D4.3, the criteria for selecting relevant semantic approaches was given and on this basis existing taxonomies or vocabularies are used and combined or new taxonomies are developed, i.e. the ELSI-taxonomy. In the following section, research results on how relationships between data sets, processes and used information systems are manifest and build the grassroots for defining the technical implementation of taxonomy in the form of an ontology.

To build the basis for defining relationships, different workshops have been conducted. The workshop set-up included specific, real processes of first responders or Police Authorities. Within these processes used information systems and moreover used, needed or available data was identified. To demonstrate the progress, two example processes will be shown in the following section of this deliverable: the first wave of

refugees arriving in Dortmund main station and, secondly, the planning process to ensure safety and security for large soccer games. Both examples are framed to a certain scale of incident, include the involvement of several stakeholders and have in some points similarities. In Figure 2 the overall approach of the workshop is given. Underlying with black colour the process definition of first responder is shown. Based on that relations to the Information system taxonomy was derived targeting in the end instances of systems. A first workshop was conducted during the demonstration case in Lancaster in May and based on that further internal workshops were organised to elaborate the processes and connection in more detail. Participants in Lancaster were asked to choose relevant processes of their daily work and address information systems used or data to different processes steps. This supported the SecInCoRe research staff to identify relevant connections and implications between the different artefacts.

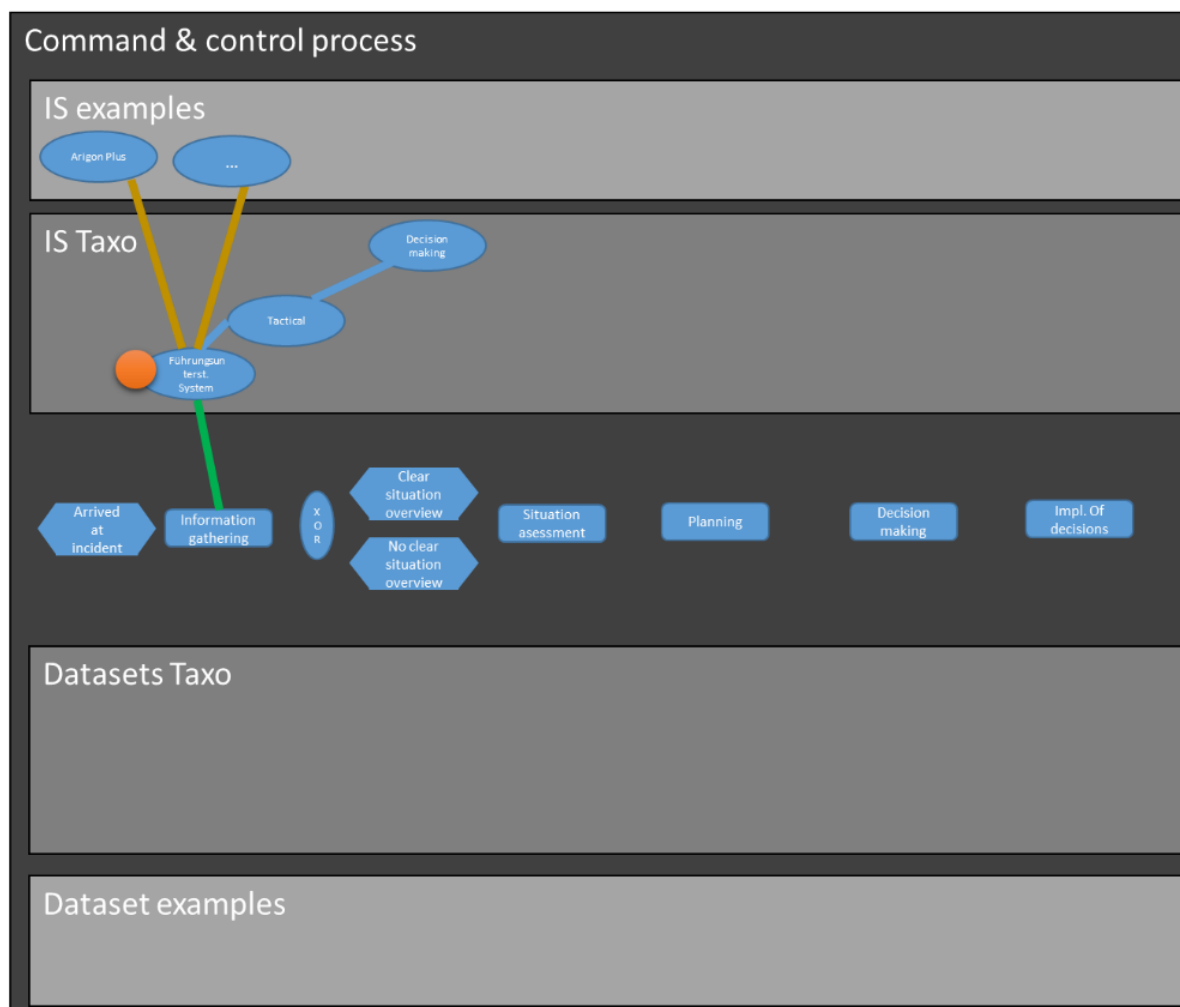
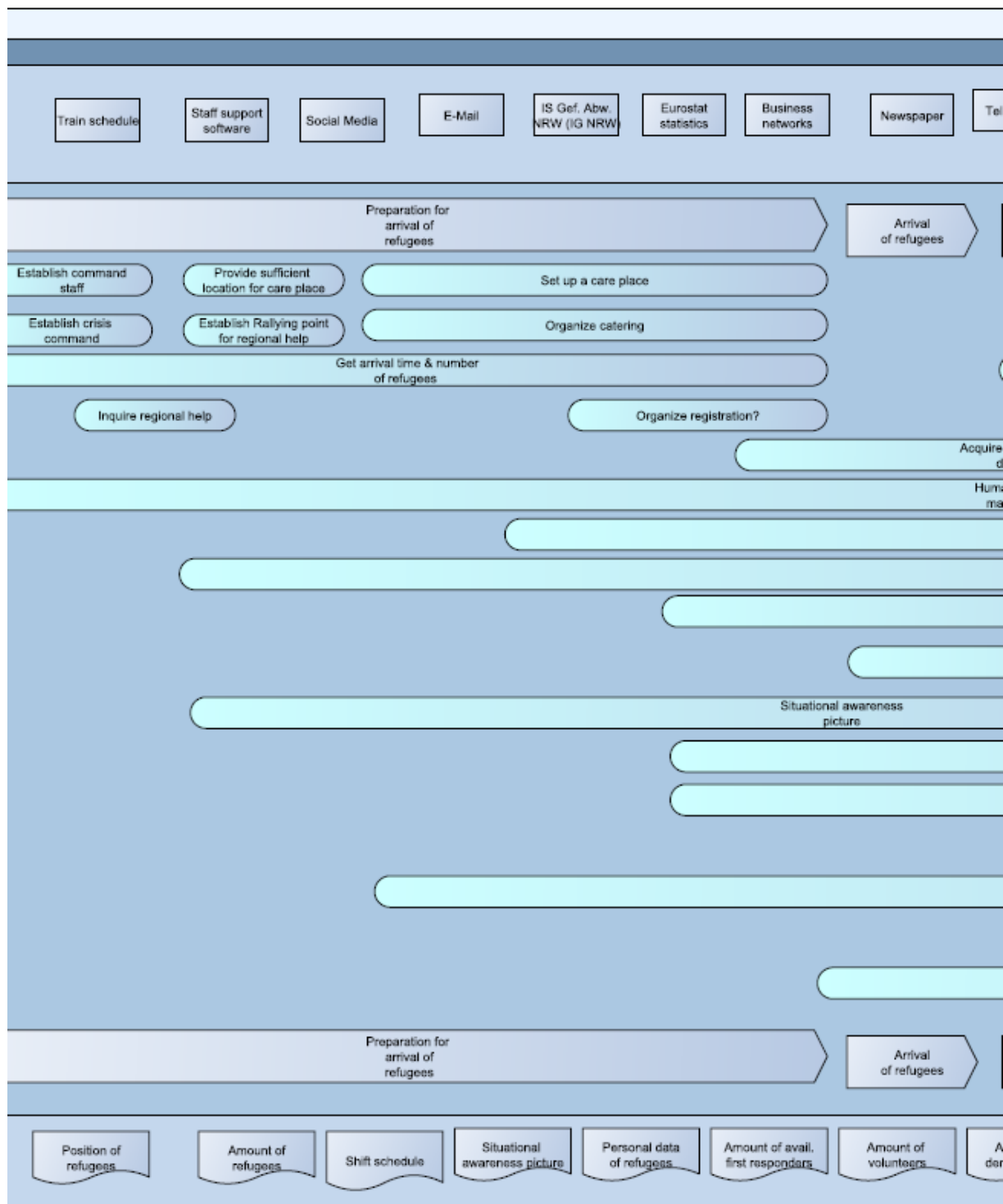


Figure 2 Workshop approach

The next two Figures illustrate results of the workshops and the identification of several main- and sub-processes. To demonstrate the amount of processes and sub-processes Figure 3 and 4 are given. Each process requires the use of data or even information



systems (i.e. the time of arrival and the amount of refugees are relevant to run the process “channel to care place”). To extract the relevant processes and required information, internal documents from the fire department were analysed and interviews with involved parties were conducted. This method was used for the analysis of required information in D3.3 and will support the analysis of used processes in D3.4.



*Figure 3 Extract of the process chain during the arrival of refugee in Dortmund
(perspective of the fire department of Dortmund)*

Figure 3 highlights the various sub-processes in the first wave of refugee arrivals in Dortmund, starting with the announcement of the refugees, to their transportation to

federal reception centres the processes were documented as mentioned in the daily information sheets of the fire department. For each documented process, all required information and further used systems were gathered and the relation to each record was clustered to define the relations needed and to combine the different vocabularies and existing ontologies. To verify this approach a similar type of incident was elaborated and relations between data, process and information system was collected. In this case, the crises situation takes place in a soccer stadium, begins similarly to the refugee reception centre process with the announcement of the fans arrival. Both example incidents contain data sets like the time of arrival or number of people. In accordance with that, a repeating sequence of main processes take place. The sequence starts with the preparation process followed by the arrival of the human crowd and the transportation. An impression of further results is provided in Figure 4. The overall activities led to a highly detailed understanding of processes. Of course, the processes also consider the differences i.e. the responsibility of police, fire departments or other organisation.

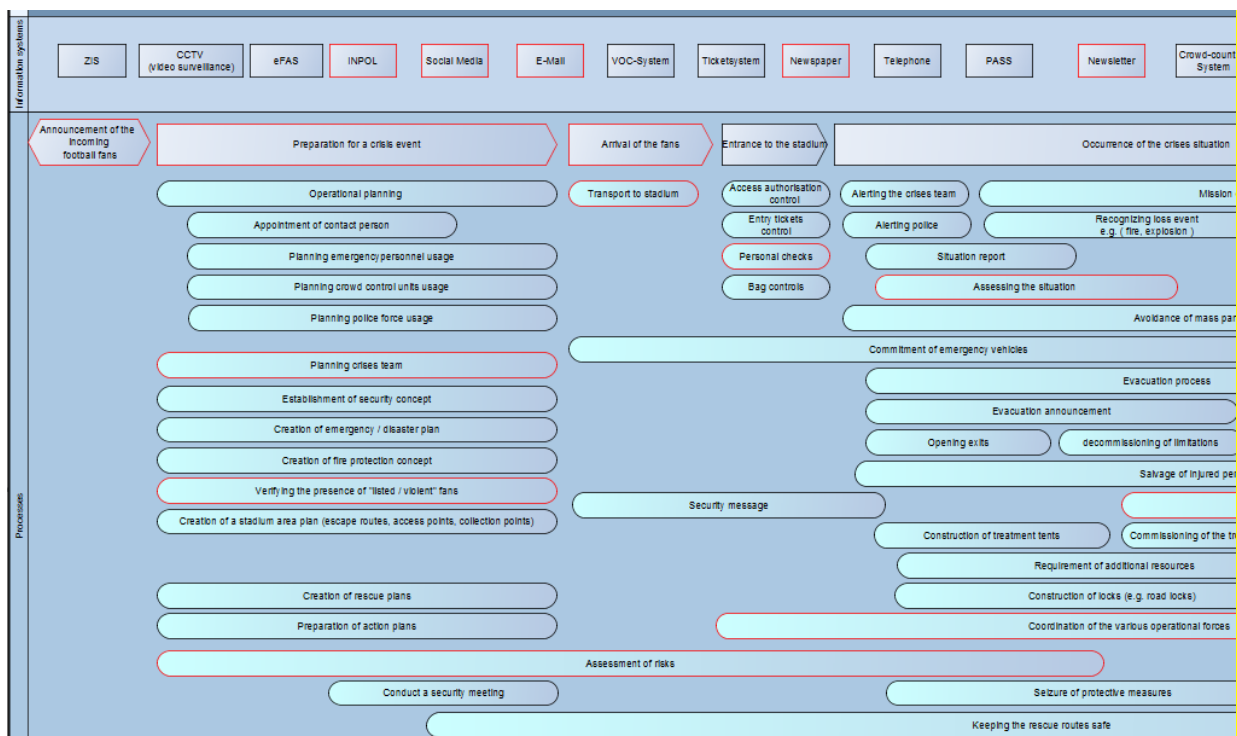


Figure 4 Extract of the process chain to prepare for a soccer game

In the following section, we describe how these new relations between exiting concepts are drawn and also documented.

2.2 Defining new relations

One aim of the SecInCoRe project is to define new relations between selected vocabularies or ontologies. In this sense we started with the analysis of tools and methods to combine the concepts of the respective ontologies. In the following section the results of this sub task are documented.



2.2.1 Results of semi-automatic alignment methods and tools

Different methodologies can be used to build connections between different ontologies. Overall all methods mentioned below use a kind of mapping of ontologies (for further information see [KHK05, S. 1], [EhSt04, S. 3], [Su02, S. 4ff], [ELBB+04, S.17ff]).

- Semi-automatic alignment – Ontology Alignment aims to connect different ontologies by drawing connections between the concepts used in the different approaches. Tools to support a semi-automatic alignment were analysed and documented in D4.3 but are also reviewed in the recent project period to give a final statement of using such tools. No tool can fulfil all criteria and present satisfying results.
- Automatic merging - aims to create one single ontology from different ontologies, which cover the same topic. (see [KHK05, S. 1]) Automatic tools do not provide useful and satisfying results at this point of time. Producing just one single ontology does not cover the ELSI request of allowing diversity and autonomy of first responders and Police Authorities. Therefore, an automatic merging is not an option for the SecInCoRe project.
- Manual alignment – this method requires alignment by hand of different concepts of various ontologies and is therefore time intensive but very profound.

The ontology-alignment began with the search for tools that would allow at least the semi-automatic alignment of the ontologies created for SecInCoRe with existing ontologies. Some projects seem to be abandoned (Optima, MatchIT). Others did not produce useful results (AgreementMakerLight). So due to time constraints it was decided, rather than developing another tool for aligning the ontologies, to accomplish the task manually. Web-Protégé (<https://webprotege.stanford.edu>) was used to achieve this because despite its drawbacks (using an older OWL standard for example) it provides a collaborative platform with built-in version control.

2.2.2 Alignment methodology in SecInCoRe

The definition of relations between different concepts is conducted in a Web-Protégé project to ensure a close cooperation between all involved parties. Even if Web-Protégé is not as powerful as Protégé itself the cooperation aspect is a main criterion in our perspective. To have a look at the current status of the alignment please see: <http://webprotege.stanford.edu/#Edit:projectId=8beaef3c-56fe-429d-8030-da7da0e3ba8d>

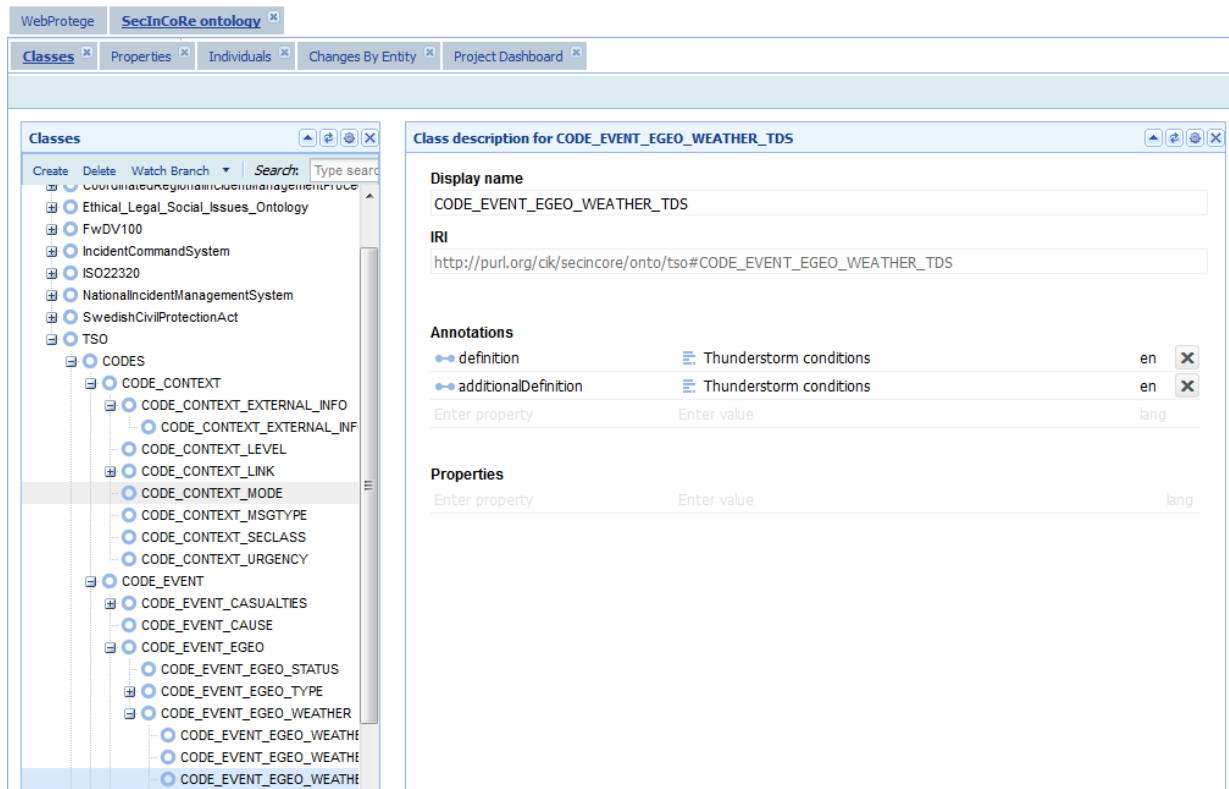


Figure 5 Web-Protégé project

Relations are seen, if Hyponymy exists between ontology concepts. Hyponymy describes the relationship between more general terms (hypernyms) and more specific instances (hyponyms). The hyponym is an element that shares a type-of relationship with the corresponding hypernym. The hypernym (superordinate) is in its meaning broader than the hyponym. In general hypernyms consist of one or more hyponyms. The hierarchical structure can be observed from top to bottom and the degree of specification increases from the higher levels to the lower levels. [www1]

The relationship between the hyponyms of the same hypernym can be defined as co-hyponyms. [www1] One example for the identification of homonymies are given below.

For example, the starting point for the development of a Reference Command System is the analysis of the already existing command systems by using their taxonomies and by the identification of relations between the systems. Because of the smallest amount of elements in the ISO 22320, this command system functions as the basis for the comparison. The elements of the ISO 22320 are respectively compared to elements out of the other command systems that seem to have the same purpose and similar positions in the hierarchical structure. Following the definitions of those identified, elements are compared and analysed in relation to entire accordance. If the definitions of four elements, each out of a different command system, is almost identical, then a representative element replaces them and is integrated into the taxonomy of the

Reference Command System. The hierarchical structure of the combined taxonomy is developed individually and refers to logic relationships of the incorporated elements.

By conducting such comparison of existing taxonomies and ontologies new relationships between existing approaches arise and will be documented.

To further document the status of new relationships created by SecInCoRe, dedicated documents were created, to guarantee the common understanding of types of relations and the different related concept. In the following Figure 6 and Figure 7 show an Figure 6 extraction of the documents to do record the ongoing process to define new relationships.

ISO22320		R
(ISO)CommandAndControlSystem	- (SCPA)CommandSystem	equal
(ISO)InformationSharing	- (ELSI)Information_Exchange	equal
(ISO)Coordination	- (NIMS)MultiagencyCoordinationSystems	type of
(ISO)CooperationAndCoordination	- (CNC)CoordinationAndCooperation	equal
(ISO)RolesAndResponsibilities	- (ICS)Responsibilities	type of
(ISO)Humans_Security_Insecurity	- (ELSI)Humans_Security_Insecurity	type of
(ISO)CommandAndControlStructure	- (CNC)CommandAndControlStructure	equal

Figure 6 Extract of documentation of new relations

In Figure 6, first relations are defined between concepts of the newly developed ELSI taxonomy and command and Control structures based on the merging of different incident command systems in Europe or the different individual command systems. The meaning of the individual relation is gathered and documented in the Figure 6. Both just represent extracts of the whole documentation process and will be extended as further relations are identified.

<p>Relationships:</p> <p>Equal: Having the same quantity, measure, or value as another.</p> <p>Creates: A class that requires an other class for activities or events.</p> <p>Type of: A subdivision of a particular class to an other class.</p>

Figure 7 Extract of Relation definitions

2.3 Application of Taxonomy

While researching methods for the visualisation of search results and also combining with the needs based on the results of ELSI studies implies another way of searching, especially to deal with terminologies and taxonomy in a way to allow diversity and enable users to understand different meanings and interpretations of data. The overall aim to

visualize search results and documents based on ontology is to outline the relationships between content and topics and support the use to make sense of presented data.

2.3.1 Ontologies in the Semantic Search

The Semantic Search is developed to help prospective users to utilise the ontology to find relevant content in the Knowledge Base. The aims are therefore, to enable the user to access the KB content and to give an idea of how semantic approaches could be used within a CIS. This chapter will give an overview about the application of ontologies in the Semantic Search. Technical details of the semantic Search and the connection of the Semantic Search and the Knowledge Base will be explained in D3.4.

A structural overview of the Semantic Search is given in Figure 8. In the emergency domain, data is distributed in local organisations and stored in several formats. When these organisations join a CIS, they can connect their databases and filesystems with SecInCoRe. The data is therefore accessible in the Knowledge Base, together with the data collected within the SecInCoRe project. To structure the data, different ontologies are used. The emergency domain is represented as well as possible within the SecInCoRe ontologies. To enable also a structuring and analysis of the content concerning general topics, general ontologies are also used, which represent the “World Knowledge”. Matching all these sources together enables users from within the emergency domain to search from one single point in all connected data sources, using emergency as well as general ontologies to structure and interpret the data.

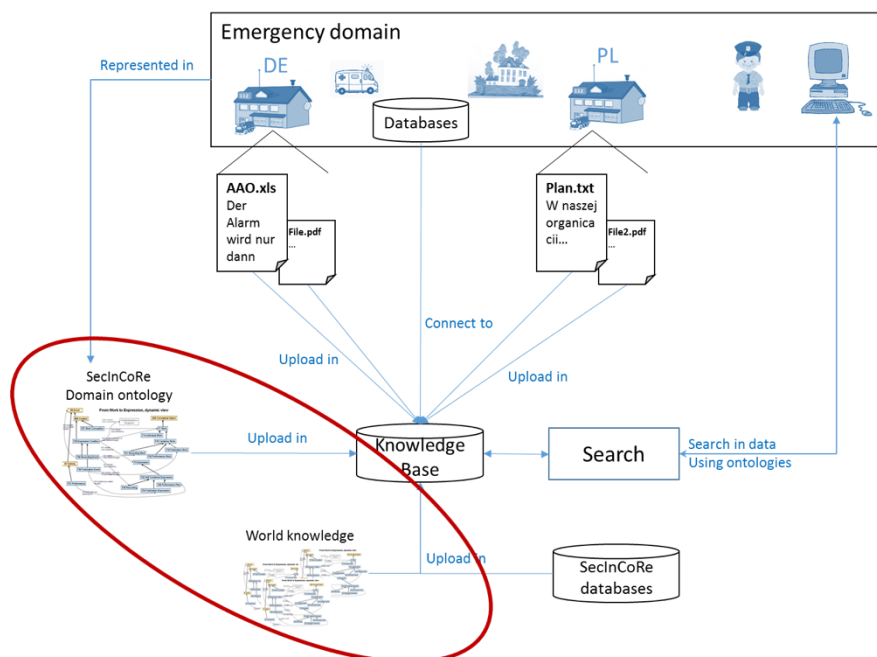


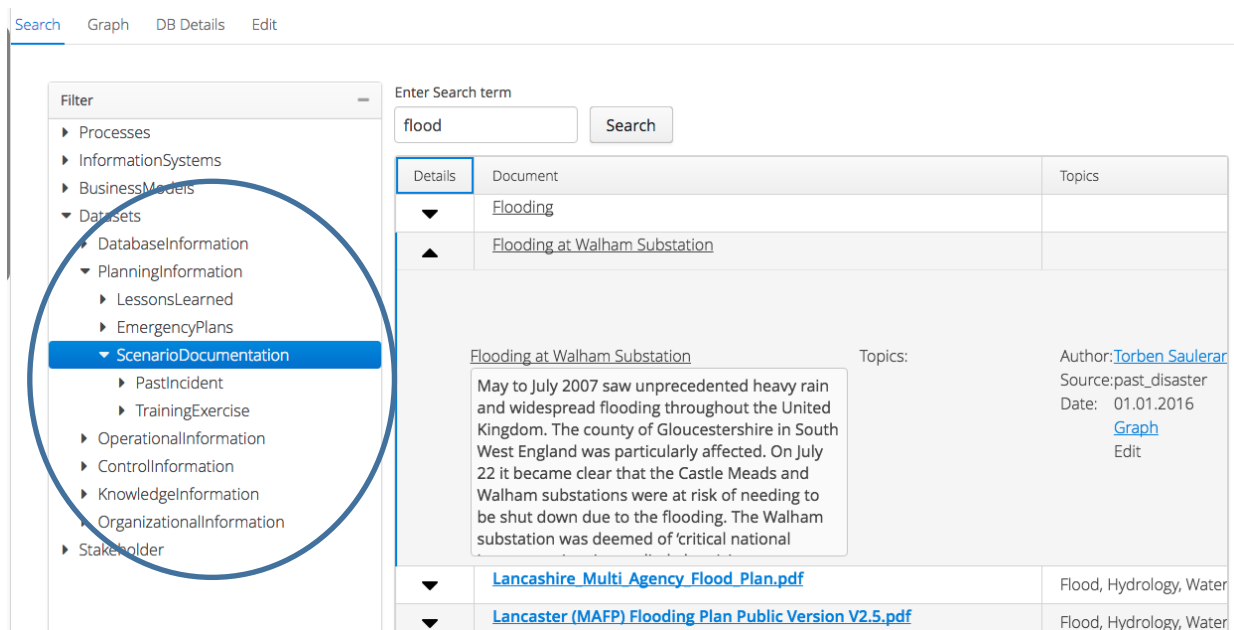
Figure 8 Overview of the Semantic Search

In the following sections two aims of integrating the ontology in search mechanism are described. The ontologies are on the one hand used to enable users to find the results, they search for, faster and easier. On the other, the ontologies are used to enable a better overview of the content of a document. These two aims and the different approaches used to reach them are described in detail in the sections below.

2.3.2 Find proper results

The first use case for the ontologies is to improve the speed in which results are found. Web search engines like google use several parameters to define the “pagerank” of a website, i.e. the amount of links to other highly ranked pages and the keywords provided by the website host. In the SecInCoRe environment, this is not possible. We are mainly searching in documents, which are not tagged, do not have a great description and often not even a useful document title. To enable a structured and fast search, ontologies could be used.

Filters can be used, to give the data a structure and to refine the search results in the direction, the user prefers. Therefore, the data is tagged, using the “Scones” tagger of the open Semantic Framework. Every document is tagged with the concepts, contained in the SecInCoRe ontologies, if they are relevant for that document. After the tagging is done, the search results could be filtered, to show only the results, concerning a special topic. In Figure 9 a screenshot of the Reference Implementation is shown, where a part of the SecInCoRe ontology is used to filter the search results.



The screenshot shows the SecInCoRe search interface. On the left, a 'Filter' menu is visible with a tree structure. The 'ScenarioDocumentation' category is selected and circled. The main area shows search results for the term 'flood'. The results are displayed in a table with columns 'Details', 'Document', and 'Topics'. The 'Document' column contains a text snippet about flooding at Walham Substation. The 'Topics' column lists 'Flood, Hydrology, Water'.

Details	Document	Topics
▼	Flooding	
▲	Flooding at Walham Substation	
	<p><u>Flooding at Walham Substation</u></p> <p>May to July 2007 saw unprecedented heavy rain and widespread flooding throughout the United Kingdom. The county of Gloucestershire in South West England was particularly affected. On July 22 it became clear that the Castle Meads and Walham substations were at risk of needing to be shut down due to the flooding. The Walham substation was deemed of 'critical national</p>	<p>Topics:</p> <p>Author: Torben Sauler</p> <p>Source: past_disaster</p> <p>Date: 01.01.2016</p> <p>Graph</p> <p>Edit</p>
▼	Lancashire Multi Agency Flood Plan.pdf	Flood, Hydrology, Water
▼	Lancaster (MAFP) Flooding Plan Public Version V2.5.pdf	Flood, Hydrology, Water

Figure 9 Setting filters in the search process

Another approach is to **improve the search rank**, using the ontologies. To do that, the attributes of a document could be used. Usually every word within the document has the same influence on the search rank of it (despite several unimportant “stop words”, which are filtered). Once the document is tagged with topics, documents could be ranked higher if the topic contains the keyword, searched for. How strong this influence is, could be modified using an internal parameter. After that there are several options to improve the search ranking, using semantic similarities. It is possible, to compare the semantic similarity between the results and the query, to modify the ranking of the documents. After that the keyword searched for could be extended, adding synonyms of it, extracted from domain ontologies.

The **GraphView** is a functionality to change the view on search results. It is possible to use the “Graph” Button as shown in the following Figure 10 and switch to another visualisation.

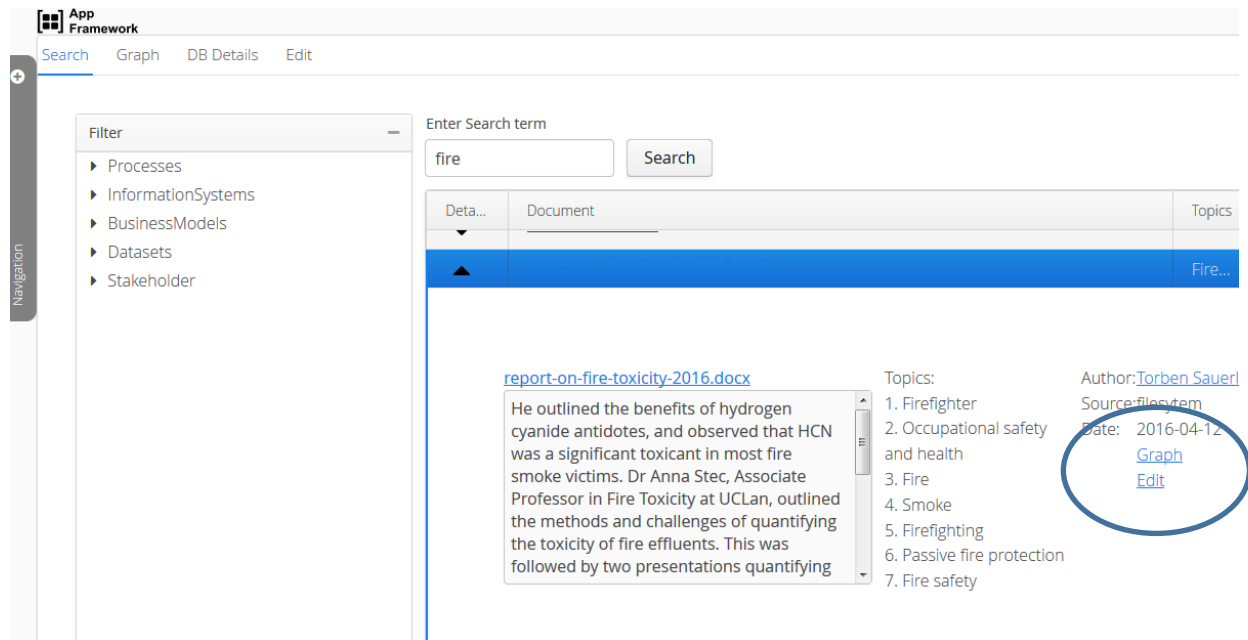


Figure 10 Activate GraphView

To enable the visualisation of the ontology and the documents placed in the ontology, **Visual Notation for OWL Ontologies (VOWL)** was used. VOWL is a specification to define a graphical representation of OWL (web ontology language) ontologies.

WebVOWL (<https://github.com/VisualDataWeb/WebVOWL>) is an open-source implementation of the VOWL notation as an interactive web application using HTML and JavaScript. It was used to build up the GraphView functionality. Therefore, an interface to the existing VAADIN infrastructure, used by the SecInCoRe project to implement the semantic search, was necessary. Further adaptations were needed to connect the WebVOWL based visualisation of the ontology and the OSF search functionality which was at first accomplished by creating a JSONP workaround to circumvent the same-origin policy of contemporary browsers. This method became obsolete at a later stage when the WebVOWL application was further integrated with VAADIN.

The **Result of the application** in form of the **GraphView functionality** will be described below. After the choice to see a document embedded in the ontology has been made, a one degree relationship becomes visible as depicted in the Figure 11. The document is represented by a rectangle containing the filename in the middle and related concepts of the ontology are placed around. The current version of the GraphView covers functions like:

- Provide more information about the document by clicking on the respective documents. In the right abstract and topics of the document occur.
- By selecting one of the related concepts, further concepts appear.

- Via double-clicking on either a concept or a document, users are able to navigate through the ontology and stored documents.
 - A double-click on a concept loads a maximum number of three hundred documents related to that concept. These documents appear in no particular order.
 - When double-clicking on a document the related concepts are being displayed (as seen in Figure 11).

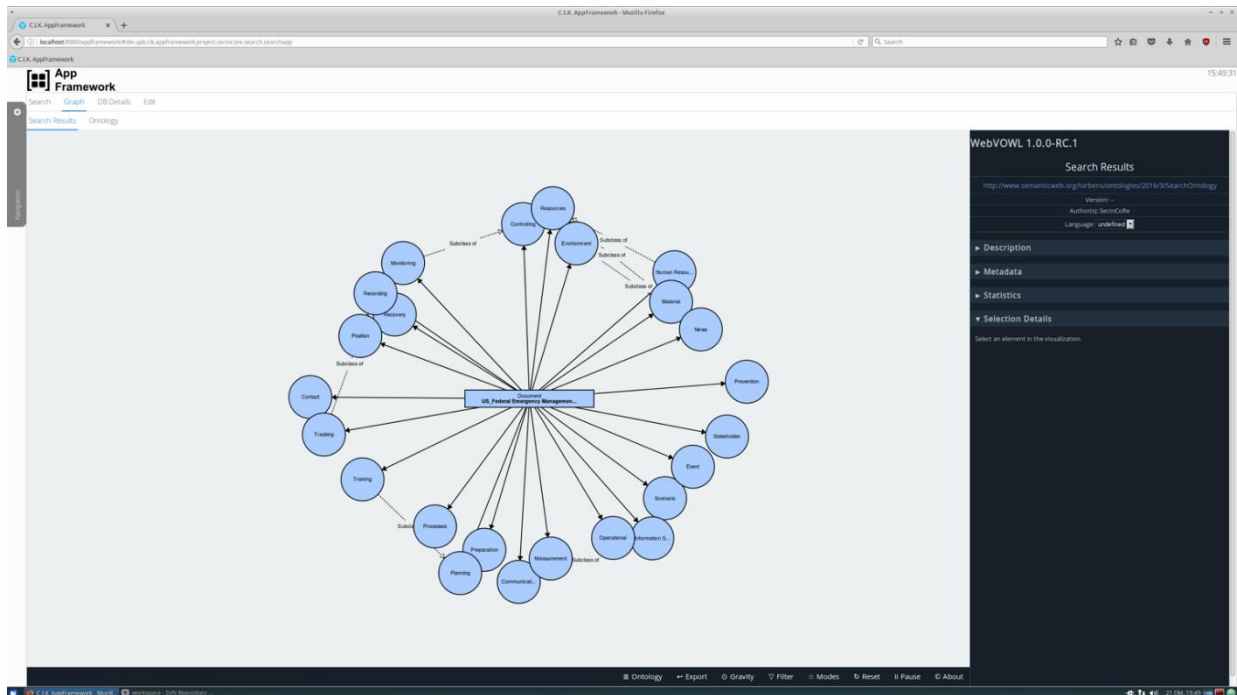


Figure 11 GraphView functionality

In the upper left of the user interface is the possibility to switch between the GraphView functionality in accordance to the search results or to take a look on the whole SecInCoRe ontology. Figure 12 demonstrates this opportunity.

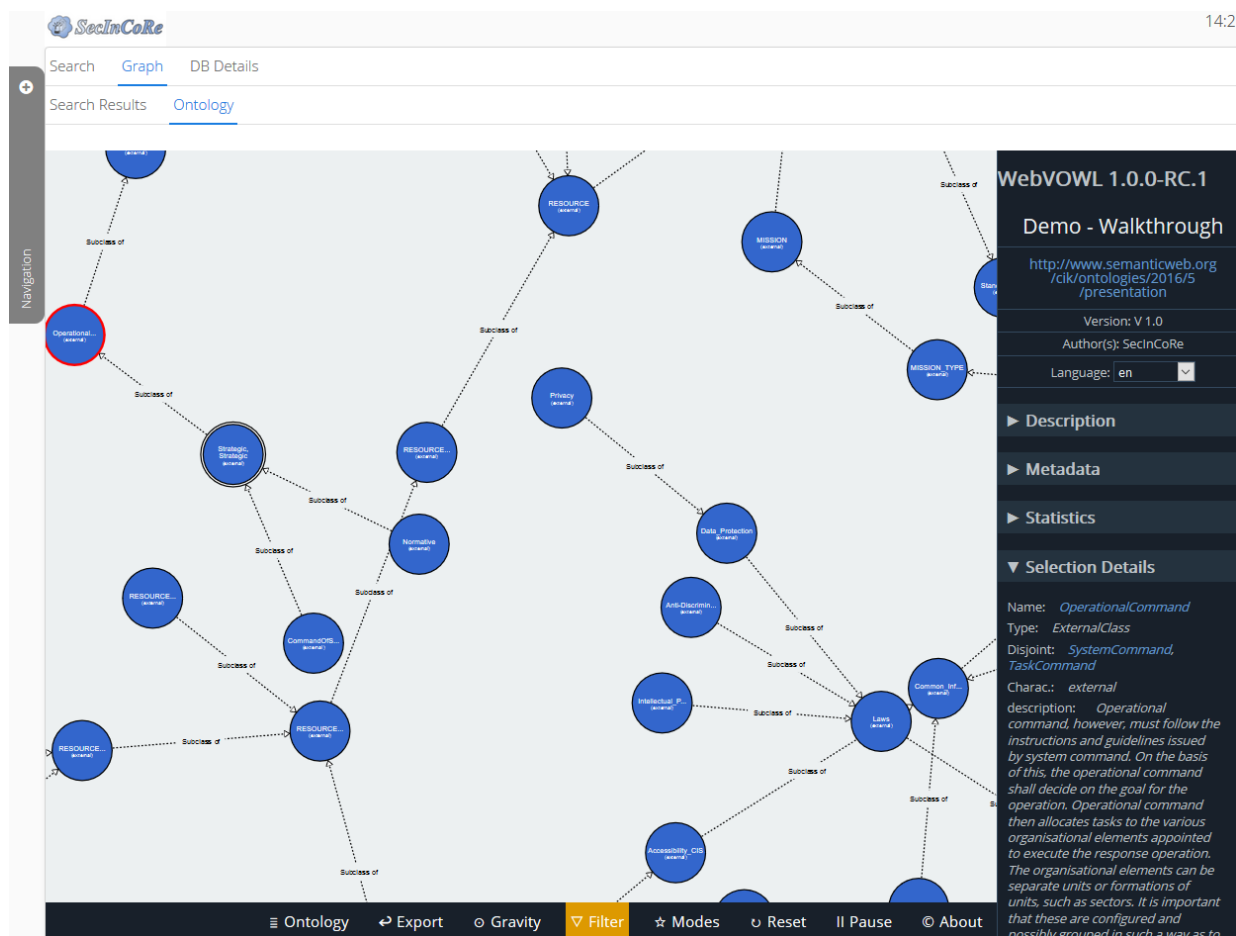


Figure 12 SecInCoRe ontology

2.3.3 Interpret the results

The second aim using semantics in the search is to improve the chance to interpret a document with richer appreciation of its contents and how it was intended. Besides the aforementioned problems with unclear document names and missing descriptions, the documents are in different languages and therefore it is difficult for foreigners to understand what a document is about.

The first approach to improve interpretability is the automatic **translation** of the documents. This is done by external translation APIs, which use their own semantics to translate between all European languages.

After the documents are translated, the AlchemyAPI is used, to identify the most relevant **topics** of a document. This is a framework, which uses general ontologies and the dbpedia database. The topics are extracted from the document and ranked in order of relevance.

To further improve the idea of what a document is about, an **abstract** is generated, analysing the structure of a document and the content contained. The aim is, to find the most fitting section, to describe the overall meaning of the document, or to generate a new section, if no fitting section is found within the document.

The screenshot shows the 'App Framework' interface with a search bar containing 'fire'. The search results are displayed in a table with columns 'Deta...', 'Document', and 'Topics'. The first result is highlighted in blue. The document title is 'report-on-fire-toxicity-2016.docx'. The abstract text is: 'He outlined the benefits of hydrogen cyanide antidotes, and observed that HCN was a significant toxicant in most fire smoke victims. Dr Anna Stec, Associate Professor in Fire Toxicity at UCLan, outlined the methods and challenges of quantifying the toxicity of fire effluents. This was followed by two presentations quantifying'. The topics listed are: 1. Firefighter, 2. Occupational safety and health, 3. Fire, 4. Smoke, 5. Firefighting, 6. Passive fire protection, 7. Fire safety. The author is 'Torben Sauerl' and the source is 'filesystem'. The date is '2016-04-12'. There are links for 'Graph' and 'Edit'.

Deta...	Document	Topics
	report-on-fire-toxicity-2016.docx He outlined the benefits of hydrogen cyanide antidotes, and observed that HCN was a significant toxicant in most fire smoke victims. Dr Anna Stec, Associate Professor in Fire Toxicity at UCLan, outlined the methods and challenges of quantifying the toxicity of fire effluents. This was followed by two presentations quantifying	1. Firefighter 2. Occupational safety and health 3. Fire 4. Smoke 5. Firefighting 6. Passive fire protection 7. Fire safety

Author: [Torben Sauerl](#)
Source: filesystem
Date: 2016-04-12
[Graph](#)
[Edit](#)

Figure 13 Topic and abstract

2.3.4 Sustainable ontology

Persistent Uniform Resource Locator (PURL) enables persistent access to a web resource and redirects to another web address. Hence even if the URL changes, the pointing of a PURL can be updated and the user can use the same link to request web content. This is especially useful for Linked Data applications since the data can be developed independently and still be interlinked with other data sources or applications. PURLs are created to subsist for decades.

To ensure sustainability for all SecInCoRe ontologies purl.org (<https://archive.org/services/purl/>) was used to set up PURLs for all of them. A GitHub repository (<https://github.com/upb-cik/SecInCoRe>) was utilised in accordance with PURLs to publish the created ontologies.

2.4 Internal Verification and Validation of Taxonomy

The taxonomy will also be validated in accordance with the overall SecInCoRe validation and evaluation strategy and results will be presented in D5.4 and D5.5. Nevertheless, an internal verification and validation done by the developing party against the defined requirements and transformation based on D4.3 is shown in the following table.



Number of requirement	Description of requirement	Transformation	Verification and Validation result
SICR-169	Support translation through taxonomy	The ontology is a description of concepts and relations between concepts. SecInCoRe-Ontology will combine definition for every concept based on several sources. This guarantees the possibility for translation.	SecInCoRe defines relations between several semantic approaches as shown in chapter 2.2. The kind of approaches cover data sets, information systems, processes and ELSI. To support an ongoing work on defining relations a web protégé project was implemented and is open to use in the consortium. Drawn relations are illustrated in chapter 2.2 Even if not all relations and existing approaches are combined the overall approach support defining new relationships and dependencies. Therefore the SecInCoRe ontology combines concepts based on several sources.
SICR-149	Information aggregation should be based on reliable sources of information	The SecInCoRe-Ontology will be based on literature, existing semantic approaches and ontologies. Every integrated concept recommits on literature or published ontologies. This requirement also needs to be addressed at the level of using the CIS.	In D4.3 the sources of the existing semantic approaches are listed. The reliability was also used as one of the selection criteria to address this requirement. Therefore, only reliable sources were used for the SecInCoRe ontology. In the selection process the weight for reliability was between 0 and 1. If the approaches rely on governmental sources, they are scored with 1.
SICR-139	ELSI in the structuring and representing of data	The SecInCoRe-Ontology will include ELSI related concepts and therefore ensure the representation of ELSI in the structuring of data.	SecInCoRe ontology include ELSI in two ways: first, a dedicated ontology of ELSI concepts was developed and also described in a first version in D4.3. Further in the design of the GraphView functionality, the research results especially of WP2 was involved including concepts to allow diversity or support the sense-making of information.



SICR-125	Support people in cooperating without infringing on the sovereignty of other organisations	The SecInCoRe-Ontology will support cooperating of first responder and police authorities through achieving a common language by the nature of ontology. The sovereignty is independent from the ontology development.	The ontology provides definitions to all concepts and therefore ensures a common understanding of different concepts. Documents / search results can be viewed directly in the ontology to show related concepts.
SICR-124	Support people in recognising CIS as a common space	The SecInCoRe-Ontology will support cooperating of first responder and police authorities through achieving a common language by the nature of ontology. This enables people in recognizing CIS as a common space.	To support collaboration and sense-making of information the GraphView functionality was designed. Here people see different concepts and themes placed around a selected document and therefore enable the user to see the relationships between different domain relevant concepts.
SICR-114	Support inclusiveness through search	The SecInCoRe-Ontology will be based on literature, existing semantic approaches and ontologies and will prompt references to ELSI guidelines. The guidelines will help to identify missing voices in the current situation.	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user involvement and co-design approach including end user, developer and ELSI experts had taken place.
SICR-113	Support informational self-determination	Rejected – The concept of a semantic media wiki, where users can examine and adjust the taxonomy/ontology, some support for informational self-determination is provided’.	Rejection was explained in D4.3
SICR-111	Support practices of managing privacy or Design FOR privacy	The SecInCoRe-Ontology will include ELSI related concepts, , which include specification of privacy relevant aspects..	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user involvement and co-design approach including end user,



			developer and ELSI experts had taken place.
SICR-110	Support obtaining informed consent or exception	The SecInCoRe-Ontology will include ELSI related concepts. which includes specification of relevant issues relating to consent and exceptions.	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user involvement and co-design approach including end user, developer and ELSI experts had taken place.
SICR-109	The number of persons performing data aggregation should be limited	Rejected - The SecInCoRe-Ontology will not aggregate inventory content, which includes specification of relevant issues relating to persons performing data aggregation.	-
SICR-108	Support compliance with the freedom of information act	The SecInCoRe-Ontology will include ELSI related concepts which includes specification of relevant issues relating to Fol requests.	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user involvement and co-design approach including end user, developer and ELSI experts had taken place.
SICR-107	Support compliance with data minimization principles	The SecInCoRe-Ontology will include ELSI related concepts, which includes specification of relevant issues relating to data minimization.	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user involvement and co-design approach including end user, developer and ELSI experts had taken place.
SICR-106	Support users in complying with privacy by design and privacy by default principles	The SecInCoRe-Ontology will include ELSI related concepts, which include specification of privacy relevant aspects.	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user



			involvement and co-design approach including end user, developer and ELSI experts had taken place.
SICR-104	Support practices of sense-making and information management	The SecInCoRe-Ontology will support sense-making by structuring data and showing relations between data.	The GraphView functionality of the semantic search enables a view on documents related to the ontology and therefore to close-by relation and highlight the structure of data.
SICR-103	Support users in respecting human rights	The SecInCoRe-Ontology will include ELSI related concepts.	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user involvement and co-design approach including end user, developer and ELSI experts had taken place.
SICR-102	Support users in balancing security (as in resilience to disasters) against the right to privacy.	The SecInCoRe-Ontology will include ELSI related concepts.	The process to select existing approaches is illustrated in D4.3 and ensures the use of reliable sources. During the development of the semantic search several demonstration cases with end user involvement and co-design approach including end user, developer and ELSI experts had taken place.
SICR-92	Enable different level of detail of information	The level of detail of information depends on the respective information in the inventory and external sources. The SecInCoRe-Ontology will provide concepts in different level of detail.	I.e. the GraphView functionality support in a first step a one degree distance from the selected documents to related concepts of the ontology. If needed, the degree of collapsing can be changed and further concepts come up.



SICR-88	Search based on location/ type of disaster	The SecInCoRe-Ontology will cover concepts to describe different incident scenes.	SecInCoRe relays the work regarding taxonomies also on existing approaches. I.e. the TSO vocabulary defines concept to describe different incident scenes.
SICR-87	Search capabilities on specific date(s)	The SecInCoRe-Ontology will integrate a concept to define the date of an incident.	SecInCoRe relay the work regarding taxonomies also on existing approaches. I.e. the TSO vocabulary defines concepts to describe data in different incident scenes.
SICR-75	Focus on relevant information	The SecInCoRe-Ontology will cover concepts to describe different incident scenes and process of PPDR. The relevance depends on the focus of the ontology.	The vocabulary of the ISO 22320 and the TSO vocabulary describe relevant processes on incident scenes. The focus of each approach is very different and implies a variation of the focus of information, but both are used to define the SecInCoRe Ontology. This depends also on the way a user search for information and the way of visualizing the information (list of search results, GraphView)
SICR-63	Service for the identification related auxiliary facilities in range	The SecInCoRe-Ontology will classified inventory content in accordance to the definition of the included concepts.	The research to select relevant vocabularies starts with the high level approach of combining data sets, processes, information systems and ELSI. Therefore the used approaches includes the inventory content so far.



SICR-61	Indicator of available resources	The SecInCoRe-Ontology will integrate concepts regarding resources.	Various used semantic approaches or vocabularies describe concepts in relation to resources, e.g. TSO, ISO 22320. The definition of the resources is covered by the ontology, the availability do not result from the ontology and depends on the integration to other PPDR systems.
SICR-59	Status of involved assets	The SecInCoRe-Ontology will integrate concepts regarding assets.	The SecInCoRe ontology is based on exiting approaches and includes concepts regarding assets.
SICR-58	Status of engaged agencies	The SecInCoRe-Ontology will integrate concepts regarding agencies.	The SecInCoRe ontology is based on existing approaches and includes concepts regarding agencies.
SICR-56	Advanced search capabilities	The SecInCoRe-Ontology will integrate concepts regarding capabilities.	The SecInCoRe ontology is based on existing approaches and includes concepts regarding capabilities.
SICR-54	Search Categories Options	The SecInCoRe-Ontology will cover concepts to describe different incident scenes.	SecInCoRe relay the work regarding taxonomies also on existing approaches. I.e. the TSO vocabulary defines concept to describe different incident scenes.
SICR-24	Support for classification of information	The SecInCoRe-Ontology will classified inventory content in accordance to the definition of the included concepts.	The research to select relevant vocabularies starts with the high level approach of combining data sets, processes, information systems and ELSI. Therefore the approaches used include the inventory content so far.
SICR-20	Classification of information	The SecInCoRe-Ontology will classify inventory content in accordance to the definition of the included concepts.	The research to select relevant vocabularies starts with the high level approach of combining data sets, processes, information systems and ELSI. Therefore the used approaches include the inventory content so far.

3 CIS Concept Visualisation

The overall CIS concept is divided in three main areas as described also in D4.2:

- First the specification of relevant technical and non-technical elements to enable the creation of a CIS are listed.
- Next reference implementations are defined to give a tangible representation of used concepts.
- In the end a basic strategy for evaluation and validation is part of the CIS concept framework.

This structure is illustrated in the Figure below.

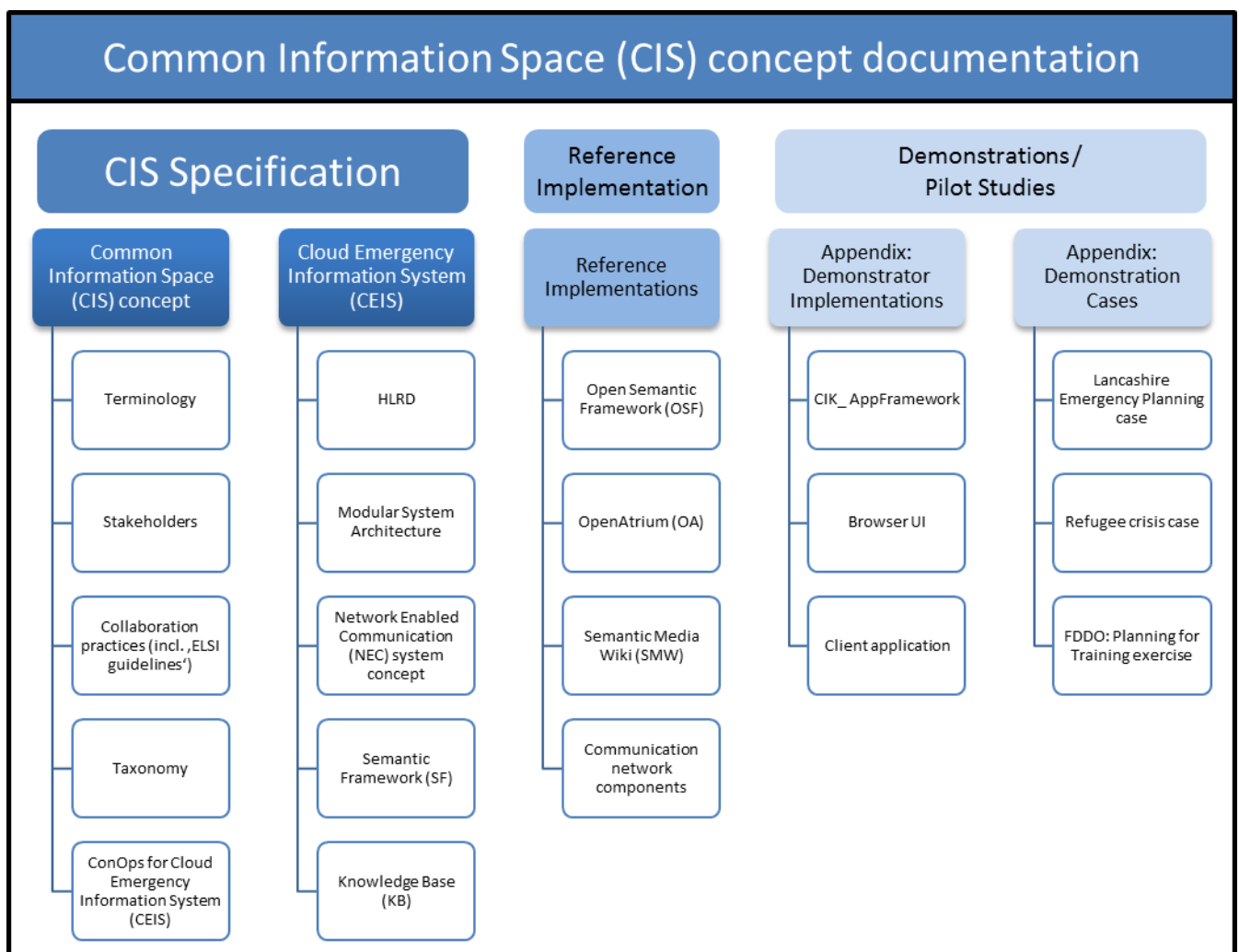


Figure 14 CIS concept

The CIS concept demonstrates the complexity of dealing with the conceptualisation and implementation of a socio-technical system for the PPDR domain. The concept and visualisation of the concept above demonstrate the loosely coupled system to adapt directly on the respective needs of the end-user. Therefore, research work in all parts

are conducted and lead to a list of reference implementations to show way to realise the concept design. In Discussion with various end-user the request to review the visualisation of the SecInCoRe CIS concept has become clear.

To derive new ways of visualising the SecInCoRe CIS concept, the respective interest groups have to be identified. First, there are several stakeholders engaged with our CIS elements in demonstration cases. Moreover, the interest of parts of our concept changes due to the research interests of the stakeholder. In this sense, a first adaption targets a theme-based approach which highlight relevant themes coming up in the concept. In the Figure 15, the topics network enabled communication (NEC), high-level requirement definition (HLRD), Collaboration (C), Semantic Services (SemS) and Governance (G). Subsequently, each of these elements contain a different research topic addressing various identified needs of first responders and Police authorities. A dedicated colour identifies each research area for recognition in further visualisations.

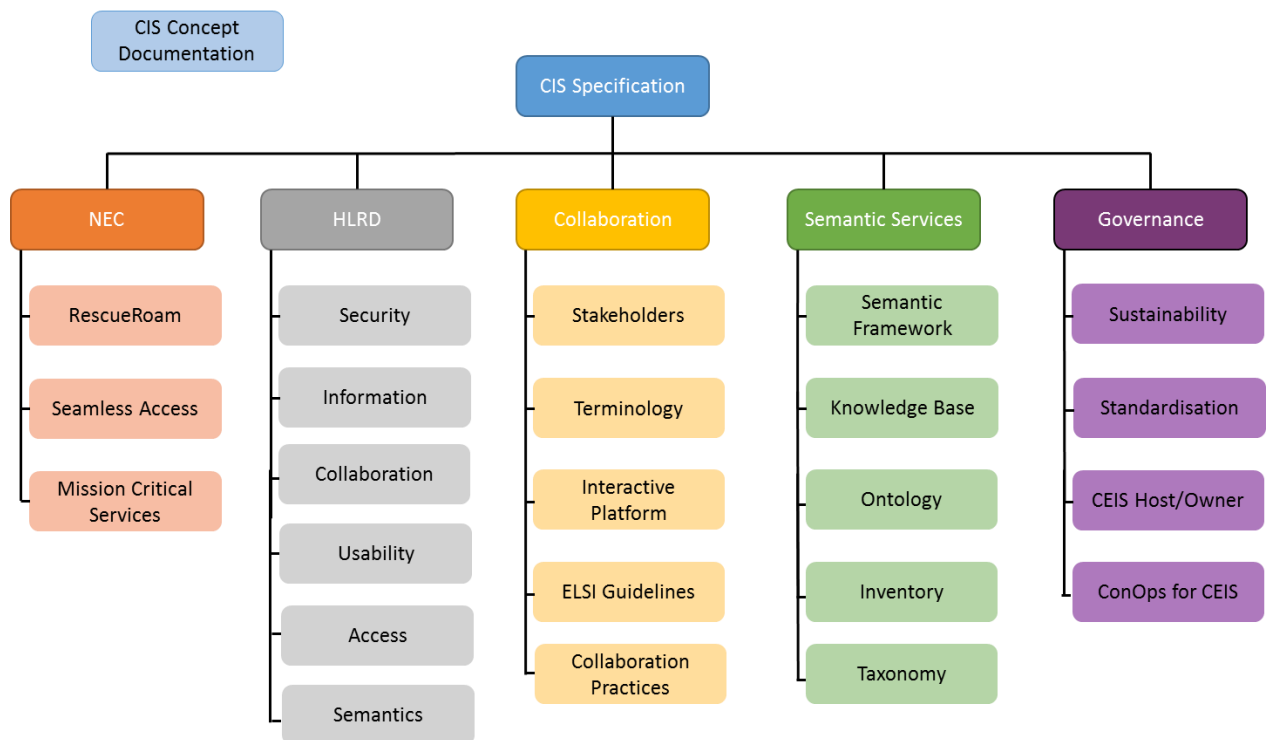



Figure 15 Theme-based visualization approach [Sch17]

In a next step, visualisation of the CIS concept directly targeting the benefits of using a CIS was in focus. 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.

To show underlying elements and sub-topics of a listed element of a CIS the symbol  was introduced.

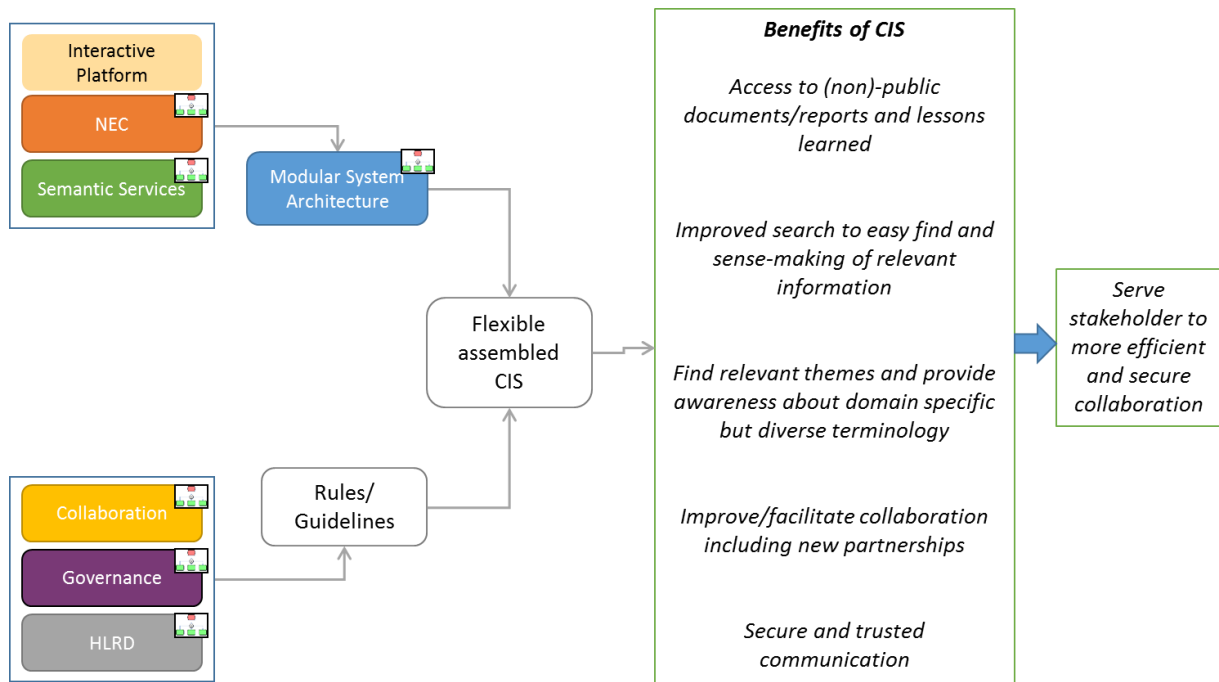


Figure 16 Benefits-oriented visualization approach [Sch17]

In the end, visualisation approaches addressing technical issues are realised. This visualization aims to show relationships and interfaces between relevant technical concepts or implementations of the SecInCoRe project and support the stakeholder to understand the approach taken to connect to a CIS, interact with other involved participants of a CIS and receive information. As shown in the Figure below, the user is connected with the secured space of the Rescue Roam and additional Mission Critical Services (e.g. data transmission in the highly secure TETRA/TETRAPOL networks), using Seamless Access. Within the Rescue Roam the user can access the collaborative platform. Integrated in the platform is the Semantic Search, which enables the access to the Knowledge Base, structured by the contained ontologies.

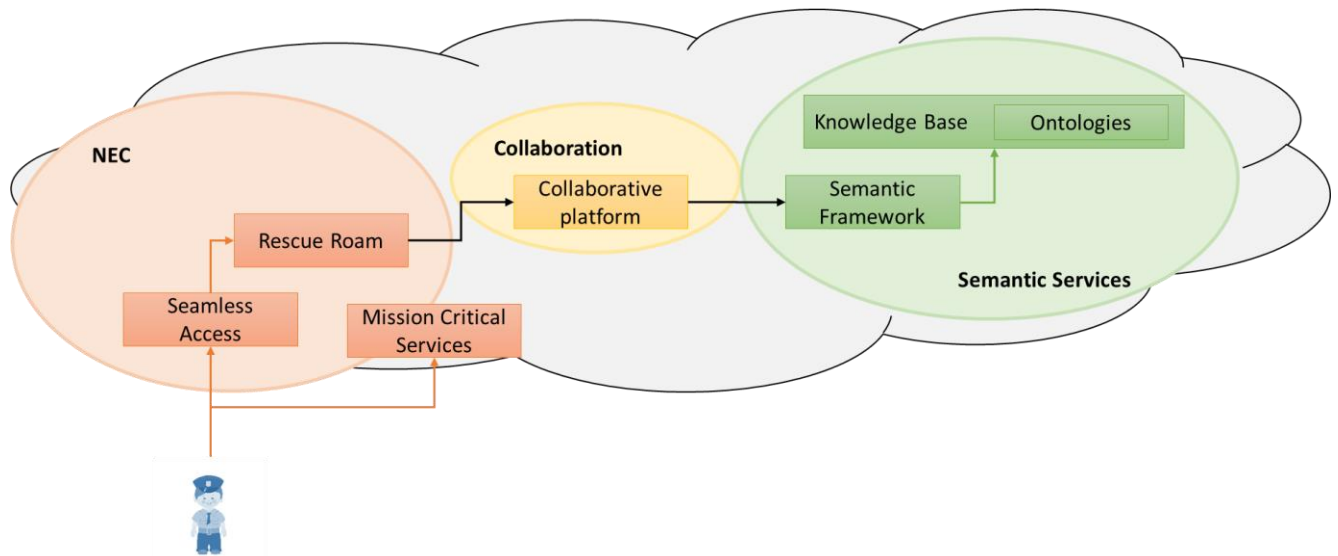


Figure 17 Component-based visualization approach [Sch17]

The last visualisation demonstrates the modular system architecture of all relevant elements and moreover highlights the combination and integration of reference implementation introduced in the original CIS concept of the SecInCoRe project. It will be used to address stakeholders in a proper way targeting directly their needs or requests to deepen knowledge about the SecInCoRe CIS concept.

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 cloud system is to use 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 such 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 integrates 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”.

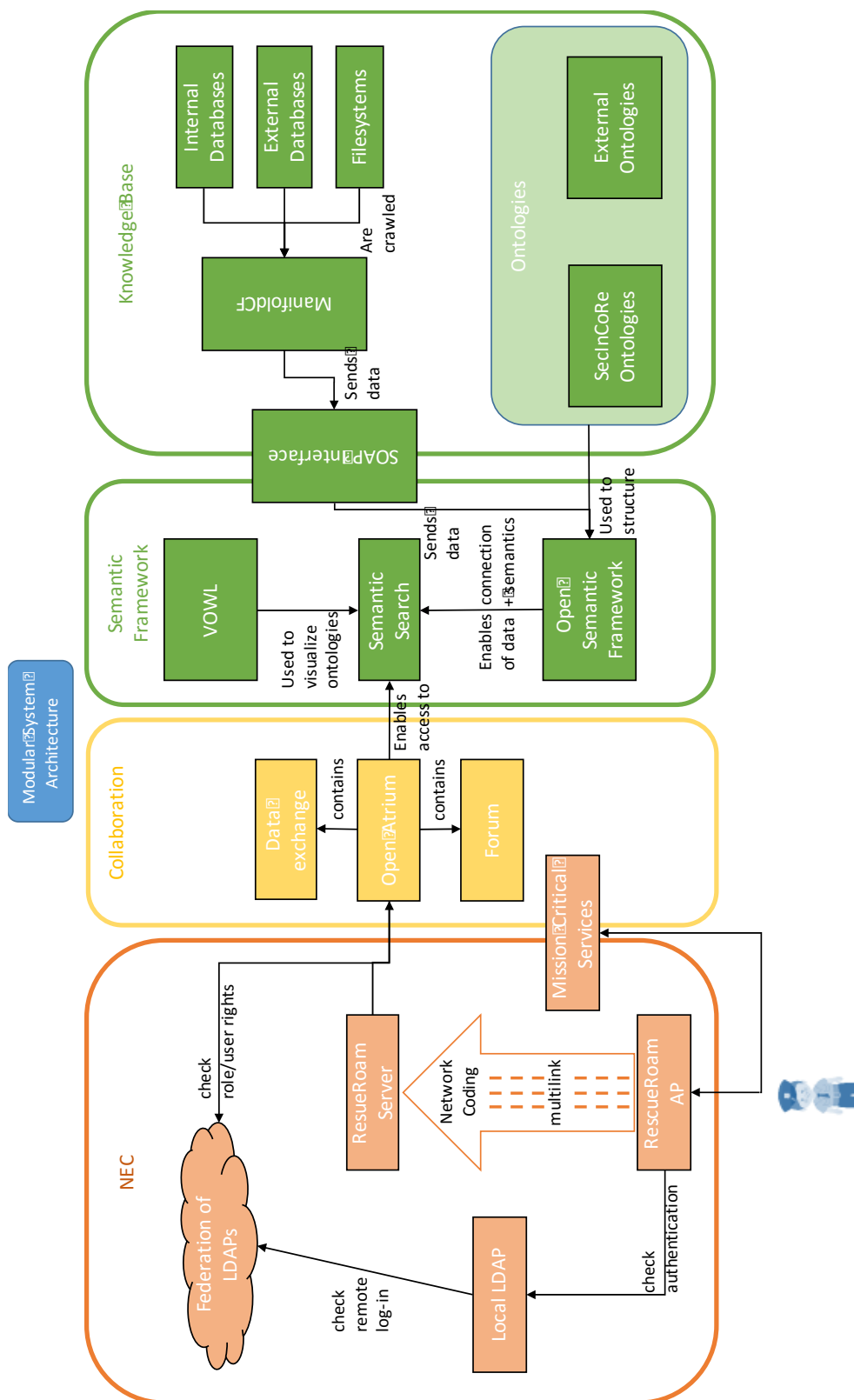


Figure 18 Modular system architecture visualisation [Sch17]

4 Seamless and secure communication system

The provisioning of a seamless and flexible communication platform as part of the Common Information Space is indispensable for ensuring a connection to the Cloud-based infrastructure and a key enabler for process-oriented local communication at incident scenes. The communication service should work in a transparent manner in two senses. On the one hand, and most of the time, it should 'just work' and make the complex processes that are necessary 'invisible' to the user. On the other, it should enable users and developers to, where necessary, open the 'black box' and inspect the logics and processes. The very text and diagrams in this document and their availability on the SecinCoRe Demonstrator Platform are designed to enable the second kind of transparency.

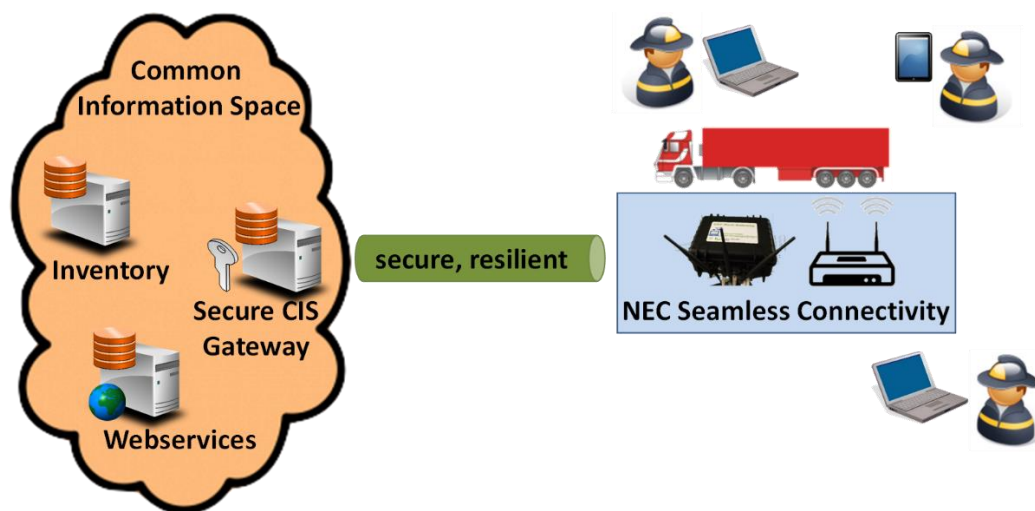


Figure 19 Seamless communication in SecInCoRe

In SecInCoRe, seamless communication is provided on two different levels as depicted in Figure 19. First level is the seamless connectivity for the users. The RescueRoam system as provided in section 4.2 provides this capability. The second level is access to the cloud in a secure and resilient manner. Cloud security aspects are presented in chapter 5, network communication methodologies are presented in section 4.1.

Additionally, AIRBUS is contributing to Mission Critical Services at 3GPP Working Groups SA1, SA6, SA3 and CT1.

4.1 Seamless communication platform

Seamless communication is strongly connected to a dynamic and reliable network and communication link management combined with intelligent failover mechanisms and network monitoring tools.

One way to improve the reliability of the communication access is the usage of multiple communication technologies and paths. Mobile communication technologies like IEEE 802.11 or cellular radio networks like LTE can be combined to improve performance and reliability. The challenge is to manage the different links and decide on best scheduling strategies to exploit the capacity in best way possible. The **Fehler! Verweisquelle konnte nicht gefunden werden.** provides an overview of different technologies to



provide such management features. Multipath TCP, Stream Control Transmission Protocol and Mobile IP are known methodologies. The HetLib is developed at TU Dortmund to make wide range applications feasible.

	HetLib	Multipath TCP	Stream Control Transmission Protocol	Mobile IP
Packet duplication	+	+	+	-
Throughput gain	+	+	+	-
TCP and UDP	+	-	-	-
Interface to application	+	-	-	+/-
Standardized	-	+	+	+
Cross-platform	+	-	+	+
Cellular networks	+	+	+	-

Table 1 Comparison of multipath communication strategies

Figure 20 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. In the following sections, the different components will be introduced in more detail.

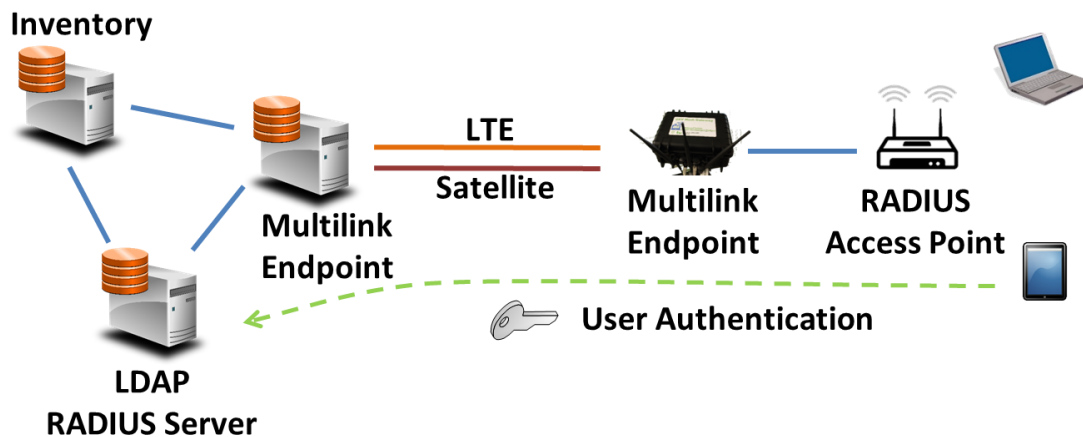


Figure 20 Network Enabled Communication architecture

A first step to enable the parallel use of Internet Protocol (IP) based and cellular networks is to provide seamless handover capabilities. Several solutions for this seamless handover at various layers exist; the most discussed ones are depicted in Figure 21 and discussed in [Zek12].

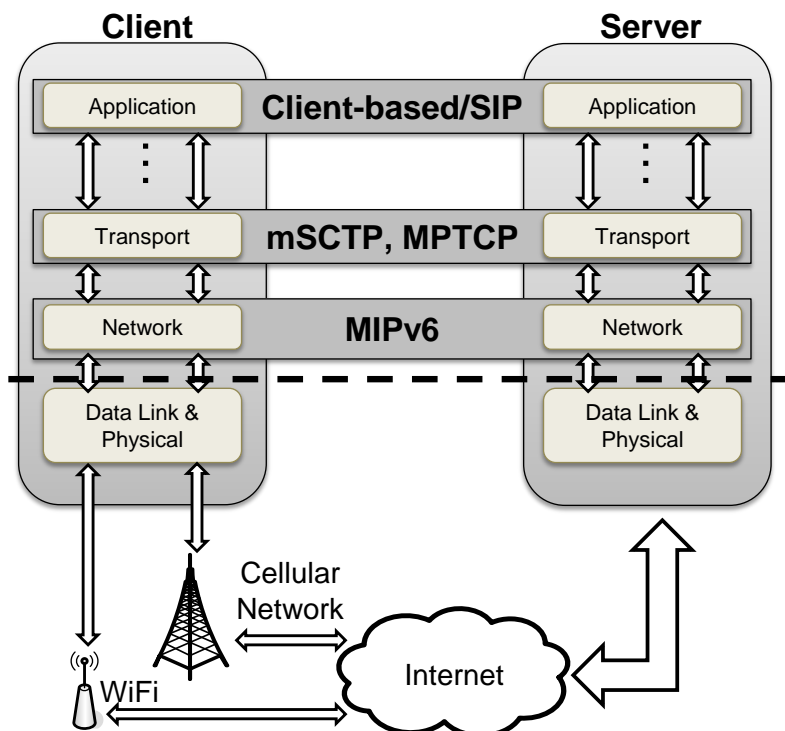


Figure 21 Mobility management and handover solutions at different layers

MIPv6 [Mag11], [AIH09], [Dev05]: Mobile IP assigns a permanent IP address to the mobile terminal by the use of home and foreign agents. This network layer based approach currently lacks in distribution caused by higher cost for network providers by the additional home agent component.

mSCTP [Ste07], [Rie07]: mobile Stream Control Transmission Protocol copes with the problem of various interfaces to the Internet, called multi-homed host. It enables an SCTP stack to associate IP addresses dynamically, supporting vertical handover during active sessions by dynamic address resolution. However, the adaptations have to be made to the network stack allow a wide spread of this solution.

Client based solutions, like the CSH-MU Solution proposed by Tran et. al [Tra14] are working without any central knowledge and are easy to integrate in nowadays smartphones by installing an application. For evaluation of client-based metrics and algorithms this solution is the easiest way to set up prototypes for evaluation in laboratory and real environments [Kuh14].

To sum up, current solutions can cope with the problem of seamless handover execution, therefore we will not focus on the handover solution in the rest of the project. Further, Mobile Controlled Handover (MCHO) solutions reduces the overall complexity in the network (e.g., signalling overhead, handover latency) and active switching will enhance the network experience. In the following section, we will present two approaches to facilitate the parallel use of multiple communication technologies in order to increase the gained throughput and reliability.

Multilink connection management

In order to enable the usage of multiple communication links, several technologies have been used and analysed in SecInCoRe.

During the 2nd project year, the transfer protocol Multipath TCP (MPTCP [Gon13], [Kha14]) was used extensively. MPTCP is an extension of TCP, using multiple TCP flows for transmission. One master flow is divided in several sub flows that are handled

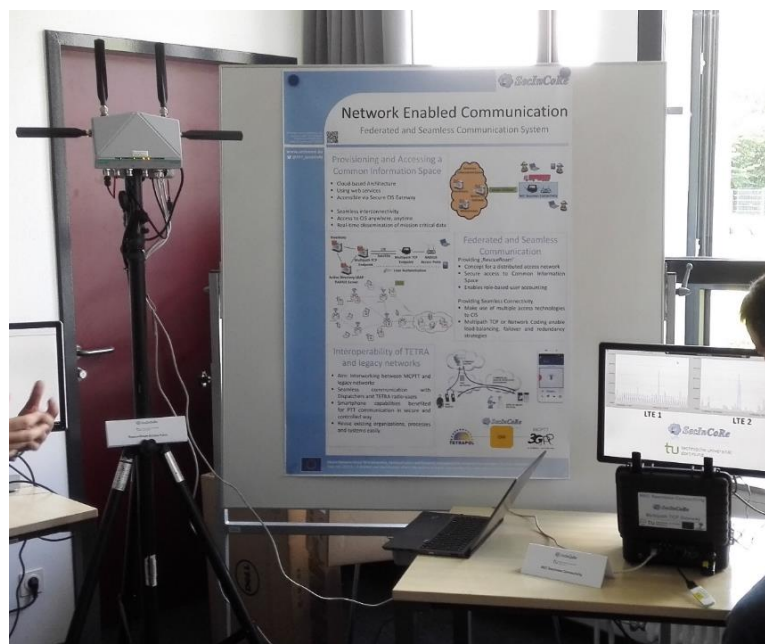


Figure 22 RescueRoam & Multipath TCP demonstration during 2nd review meeting

dynamically and are using various wireless interfaces. Currently, some network parts could block signalling traffic, because of missing MPTCP features.

Figure 22 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.

On the 2nd day of the review meeting, a comparable setup was used in the laboratory at the TU Dortmund. Figure 24 visualises the demonstration architecture. Instead of public cellular networks, lab components were used to realise a WiFi and a LTE connection. The advantage in this setup lays in the control and management of the connections. They can be disturbed in purpose to analyse the behaviour of MPTPC in such extreme conditions.

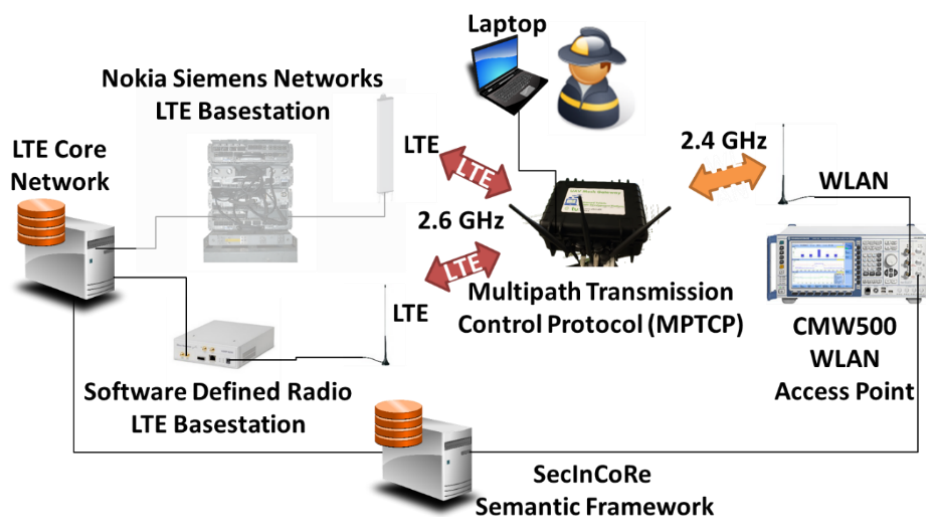


Figure 24 MPTCP Laboratory setup



Figure 23 MPTCP Laboratory demonstration during 2nd review meeting



During the 3rd project year a different methodology was analysed to realise multiple connections: Network Coding [Kat08].

In Figure 25, the main idea of the usage of Network Coding is presented. When a document is requested from the inventory, 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 analysed 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 reliability packets. If the buffer is filled with 16 packets, an additional 17th packet might be added to the data stream. In that case each of the 17 packets contains some redundant information with the aim that all information can be restored even if one packet is lost during transmission.

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, decoding process is started at the gained information is forwarded to the application layer. Each successful decoded generation is acknowledged to the sender by a message containing the generation id. The sender is waiting a pre-defined time for this message, if it is not received, the sender creates an additional packet for this generation and transmits it to the receiver. With this methodology, a data completion rate of 100% can be guaranteed.

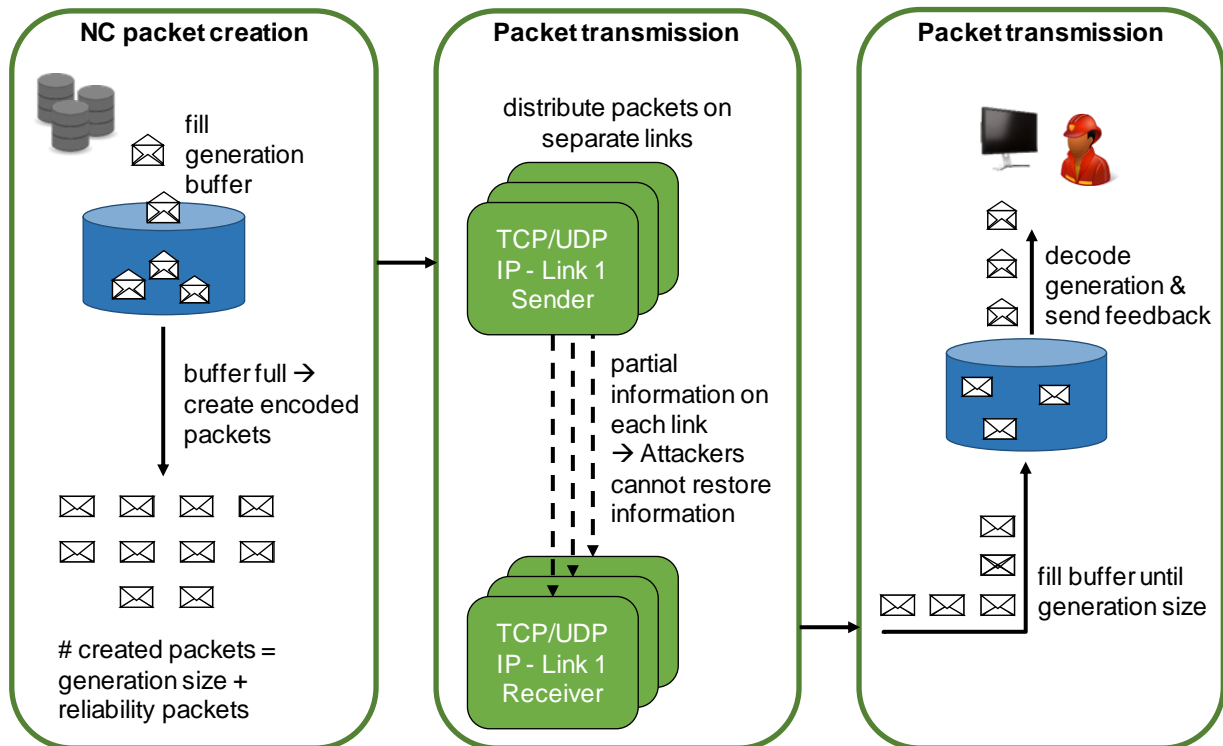


Figure 25 Network Coding in SecInCoRe [Sch17]

During the 3rd Advisory Board Meeting, a Network Coding demonstration was presented (Figure 26). 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.



Figure 26 Network Coding setup during 3rd Advisory Board Meeting



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 [kodo17] library was used. During the experiment, a data file with a size of 448 MB was transferred. Without Network Coding, a packet error rate (PER) of 10% results in a corrupt file



transmission. With Network Coding the PER can be compensated and the file is transferred successfully.

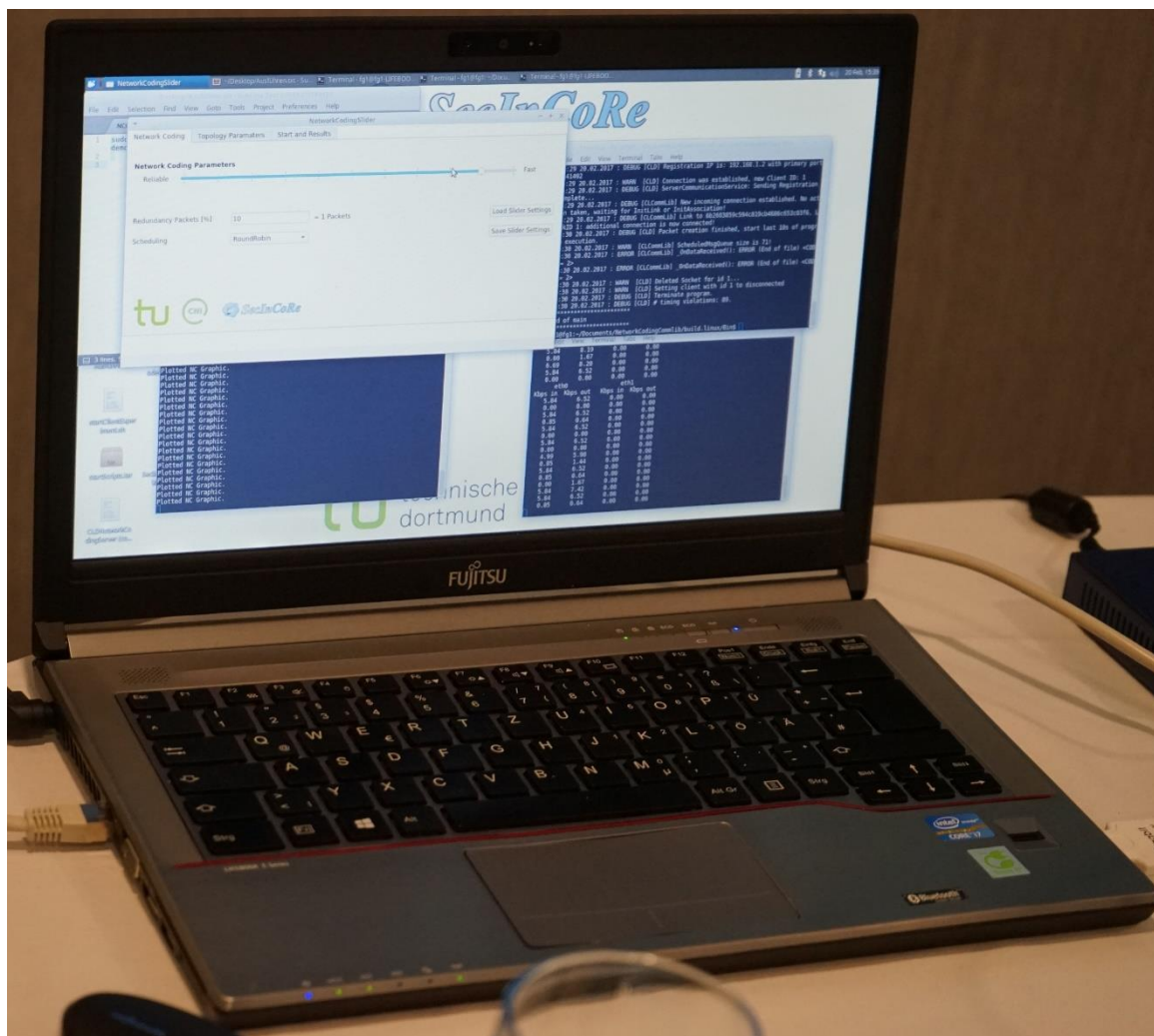


Figure 27 Parameterization of Network Coding

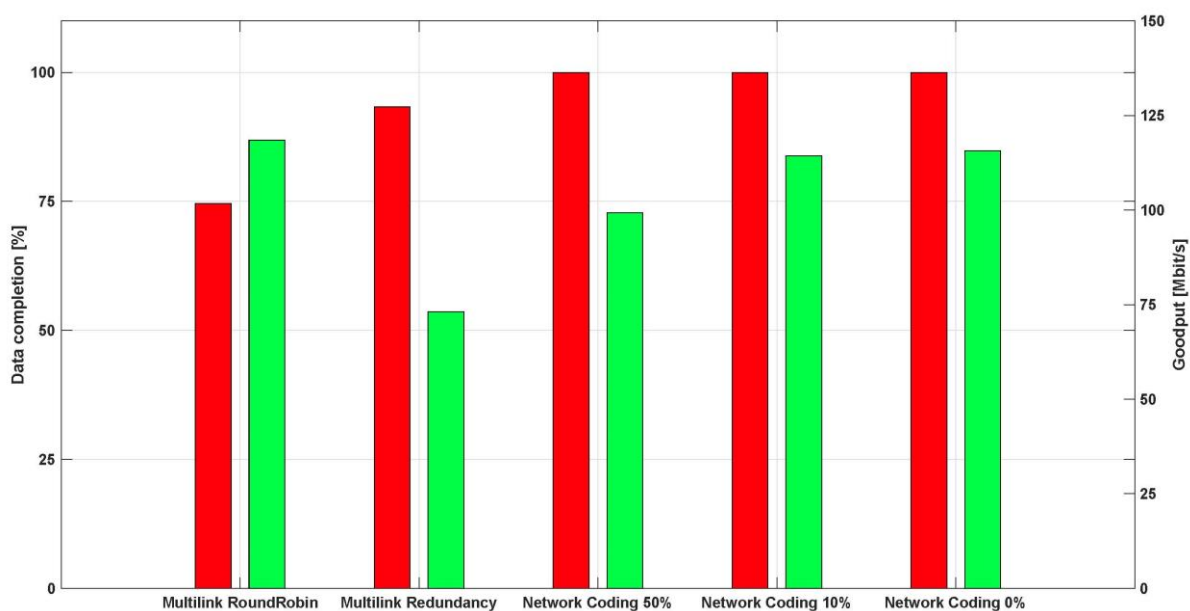


Figure 28 Data transmission via two channels with 25% packet error rate

In Figure 28 the results from experiments with two communication channels with a packet error rate of 25% are presented. Without Network Coding the data transferred is incomplete, with Network Coding the whole information is received successfully with a comparable data rate.

4.2 RescueRoam Architecture

The RescueRoam provides a common network space that can be shared by all parties involved in an emergency event. It includes mobile access points situated on sight of an emergency, secure WLAN connectivity that provides access to the full SecInCore functionality, personal Single Sign-On credentials that can be used to access other SecInCoRe components.

The initial entry point of the RescueRoam are the mobile access points that would be provided on the emergency sites. They will be configured to use a SecInCore LDAP server. This server is installed with OpenLDAP and freeRADIUS, which provide the authentication layer of RescueRoam. RADIUS is a network protocol - a system that defines rules and conventions for communication between network devices – for remote user authentication and accounting.

It serves three primary functions:

- Authenticates users or devices before allowing them access to a network
- Authorizes those users or devices for specific network services
- Accounts for and tracks the usage of those services

In the context of RescueRoam, this means that the RADIUS instance is flexible in terms of configuration and can be further tailored to any security requirements. The main use of the SecInCore LDAP instance is to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP



server to validate users. One of these application is the freeRADIUS instance, which uses LDAP to authenticate users. LDAP is well established as one of the most commonly used methods of user validation, thus it is widely supported in application and development libraries.

4.3 Single Sign-On using OpenLDAP under Linux

The Single Sign-On was implemented on a virtual machine within CloudSigma's Zurich cloud network. Having observed stability issues with the previous deployment of Active Directory on Windows 10, it was decided to use Linux as the underlying operating system. An Ubuntu 14.04 server was used and strict secure guidelines were followed when installing and configuring the required services. OpenLDAP and freeRADIUS were installed and configured on the server. Additionally, the management tool myphpldapadmin was installed for a graphical user interface to the OpenLDAP. This would ease the creation and management of users. An OpenVPN server was also installed along with LDAP integration, which could potentially be used for secure access to other components. On the other end a router using the DD-WRT software is configured to use the IP of the LDAP server. The authentication is delegated to the LDAP server. Once the user is authenticated, their device is connected to a WLAN.

4.4 MCPTT & MCS

As a follow-up of the description done in D4.3 regarding the NEC evolution related to Mission Critical Services interoperability, this section documents the status of this topic at the time this report is released (December 2016).

The Mission Critical Services interoperability is addressed by the 3GPP, the ETSI TCCE but also by Airbus as part of the SecInCoRe project.

3GPP MCS Status

The focus of the 3GPP R13 related to Mission Critical Services was on MCPTT service definition. MCPTT specifications have been approved in March 2016. However a lot of Change Requests (several hundreds) have been submitted and approved all along 2016 both at stage 2 (SA6, SA3) but also, and mainly at CT1 level. Only corrections are now taken into account in R13.

The main focus of the 3GPP R14 related to Mission Critical Services was split in two categories:

Work items:

- MCPTT improvements (due to the fact that the work was not completed in R13)
- MCVideo definition
- MCDData definition

Study Items:

- Study on Multimedia Broadcast and Multicast Service (MBMS) usage for mission critical communication services
- Study into interconnect and migration between MCPTT systems

- Feasibility Study on Mission Critical Communication Interworking between LTE and non-LTE LMR systems

As a result of guidance provided by SA#73 (September 2016), prioritisation was applied to MCData and MCVideo by the end of 2016. As a consequence, study items (except MBMS) had low priority and could not be completed in R14 whereas the other items have been almost completed.

More precisely, SA6 has estimated that the work progress is the following for these two study items:

- Study into interconnect and migration between MCPTT systems: 48%
 - Key issues list is completed
 - Solutions to key issues needs to be defined
- Feasibility Study on Mission Critical Communication Interworking between LTE and non-LTE LMR systems : 22%
 - Key issues list is not completed
 - Solution to key issues still to be defined

ETSI TCCE Status

In parallel of the 3GPP MCS specifications, the ETSI TCCE is also working on specifications in order to ensure that the MCS implementations are compatible with end-user organisations needs and existing deployments.

As an exemple of this focus, the ETSI TCCE WG4 is currently working on a TR (Technical Report) dealing with the Tetra-MCS interworking:

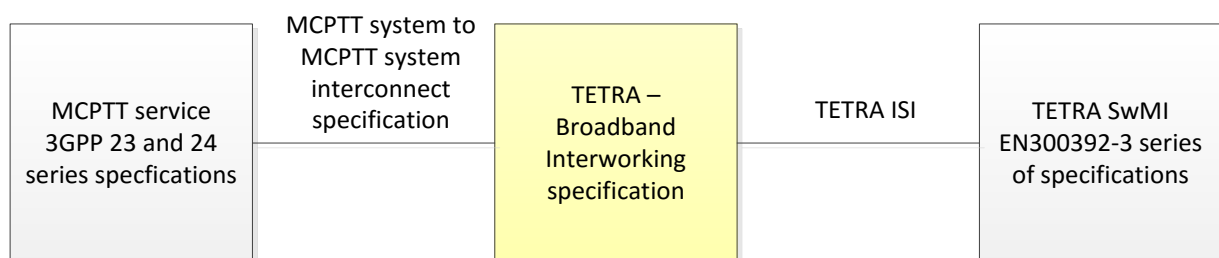


Figure 29 ETSI TCCE MCS-Tetra Interworking

The 3GPP MCS specifications cover the left part of the figure, but the interworking specification is handled by ETSI TCCE in addition to the right part of the figure.

ETSI TCCE WG4 expects to complete a Technical Report by in mid-2017.

Then an ETSI TCCE WG4 Technical Specification is expected in 2018.

Airbus is a key contributor on this topic at ETSI TCCE WG4. Airbus objective is to drive and ensure that the definition of these solutions fulfils the organisation requirements including at borders.



Airbus activities status

Even if the 3GPP and ETSI TCCE have a slower progress than expected on the MCS and legacy networks interworking definition, Airbus is still actively working on the definition and the prototyping of such gateways in advance of the standardisation works.

As part of the SecInCoRe project, a first demo of the MCS-TetraPol gateway is available in the Airbus lab.



5 Cloud Security

One of the main objectives of the SecInCoRe project is to research and develop suitable security and authentication technologies to ensure secure and auditable access to cloud-based services to emergency response services, researchers, public administration, as well as members of the public. A strong emphasis is placed on the integration of diverse data sets, their secure storage and transmission, as well as authenticated access to these data sets. Secure Single Sign-On and two-factor authorisation implementations are part of this ongoing research.

In D4.3, we briefly described the best practices relating to cloud security such as SSH-only access to infrastructure, firewall functionality, hypervisor-level isolation of VMs and Access Control Lists as well as exploring the use of containers, with particular focus on Docker, to facilitate the running of modular components over a framework based on the concept of microservices. We also hinted at the possibility of exploring cutting edge technologies such as Intel's Software Guard Extensions (SGX) to facilitate the secure processing of workloads within encrypted areas of the CPU referred to as enclaves. We will expand on each aspect in the following section. CloudSigma as the representative cloud provider on the project also offer first-hand insight into the various processes and mechanisms employed to secure their commercial cloud.

5.1 Secure Cloud Architecture

SSH Keys

SSH (Secure Socket Shell) is a network protocol that provides a more secure way of logging into a virtual private server opposed to using a password alone. SSH keys are more difficult to decipher. Generating a key pair creates two long character strings including a public and a private key. The public key can be placed on a server and unlocked by connecting via a client that already has the private key. When both keys match, the system unlocks without requiring a password. The private key can be protected further by applying a passphrase.

CloudSigma offers access to individual virtual machines by SSH keys allowing a user to run commands on a machine's command prompt without being physically present near the machine. It also allows a user to establish a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. SSH key creation covers the following scenarios:

- Customers can generate the SSH keys themselves and upload only the public key in their CloudSigma account. In this scenario customers take the responsibility for the protection and access of the private key. This option is provided for customers that are especially concerned about security in the cloud.
- Customers can generate the SSH keys themselves and upload both SSH keys in the CloudSigma account. Currently, this scenario doesn't provide additional benefits, but in the near future an SSH console (similar to the VNC console today) will be opened automatically in the Webapp. This option will be only available for customers that have uploaded both their public and private SSH keys to their CloudSigma accounts.



Access Control Lists

Access control lists (ACLs) work to segment account control rights and access to the different operational aspects. With this feature, the account administrators can allow access to different resources or a group of resources across the account. The account administrator delegates permissions to each account and lets each user log in to the web console with their own user credentials. Examples of delegated abilities:

- Provide accounting with access to billing, but not to edit any server/networking resources.
- Give junior sysadmins access to start/stop servers, but not to create or delete anything.
- Provide senior sysadmins access to fully manage the architecture, but not being able to access billing.
- Provide the operations team with access to firewall policies and networking, but not to servers.
- Provide a team with full access to their servers (using server tagging), but not any of the other resources.

The ACLs enable a very granular control over the account's permissions and budget, resulting in higher levels of transparency and security. In a distributed and federated infrastructure like the one advised here, it has to be plain for each participating organisations which account rights are given to whom. For each module, it is possible to delegate either read-only or read-write permission. It is also possible to delegate permission on individual resources, for example a server or set of drives.

Firewall Policy

Due to isolation and abstraction from the hardware, virtual machines by nature provide additional security over their traditional counterparts. An attack on a VM should not affect any other VMs running on the same server or the host OS. Virtual machines do have security vulnerabilities but the negative impacts from an attack can be mitigated using similar methods as applied to physical systems. The real security concern should be at the hypervisor level. If an unauthorized user were to gain access to the hypervisor and ultimately the host OS and hardware, they can take advantage of all the VMs being automatically generated on the same system. CloudSigma's hypervisor level firewalls ensure network protection below the level of the virtual machine without relying on the virtual machine operating system and which is resilient even to the compromise of that virtual machine. This feature allows customers to create, manage and apply enterprise-grade and other fine-grained networking policies appropriate in a disaster risk management context in relation to their cloud infrastructure in a fully integrated way. The users can configure and constrain both inbound and outbound traffic through the Web interface or directly over the API including by traffic type. Network policies also allow black and whitelisting by IP address. Management is achieved via policies which are applied to single or groups of infrastructure allowing each management and application across both small and large scale infrastructure in a convenient way. The policies range from a single rule that blocks all external public IP traffic, to complex schemes that only



allow connections to certain ports from a set of IPs. Network policies are saved and then applied to one or more virtual servers as required. Furthermore, network policies can be reconfigured and re-applied to running servers without service disruption.

Vulnerability Scans

Vulnerability scanners can be used to automate security auditing and can play a crucial role in securing cloud-based systems by exposing potential security risks. Most vulnerability scanners will generate a prioritized list of vulnerabilities and provide the recommended steps required to mitigate them, while some will even automate the patching process.

CloudSigma offers a network monitoring system called Multi Router Traffic Grapher (MRTG). MRTG is used to provide live data on all network infrastructure. The tool is used to obtain throughput data at an extremely granular level to alert for anomalies. A patented network discovery and vulnerability analysis technology - Passive Vulnerability Scanner (PSV) - is also utilized. It uniquely delivers continuous, real-time monitoring and network profiling in a non-intrusive manner. PVS monitors IPv4, IPv6, and mixed network traffic at the packet layer to determine topology, services, and vulnerabilities. Besides the above measures, CloudSigma's operations team conducts manual vulnerability checks on a regular basis.

Network Intrusion Detection Systems

Intrusion detection system (IDS) monitor the network for malicious activity including policy violations. Essentially, there are two types of Network IDS, Signature Detection and Anomaly Detection. While both are generally deployed in the same manner, there are some fundamental differences in the way they work. Signature-based detection references patterns relating to known malicious traffic, generating an alert when a signature is matched, while anomaly-based detection looks for unusual activity that deviates from statistical averages based on historical activities.

CloudSigma's cloud infrastructure, core routers and hosts are all monitored with IDS and DDoS monitoring and mitigation tools, monitored 24x7 by their Network Operations Center (NOC). With regard to alerts, the NOC interacts instantly and initiates further escalation to managers and C-level executives. Customers are updated on any issues affecting service whether or not they were directly affected.

Distributed Denial-of-Service (DDoS) Protection

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. CloudSigma implements a holistic approach to protection against DDOS attacks and other activities that can threaten the stability and availability of services to customers. This includes both remedial measures in relation to incidents and preventative measures that reduce the risk of CloudSigma being targeted.



- additional rules for fraud payment prevention (preventing fraudulent use of the cloud is the single most effective measure in reducing the incidents of attack and other issues)
- traffic shaping (put a policy in terms of number of packets and throughput), upon request that policy is editable to meet a particular client requirement
- automatic block-hole routing of problem IP addresses over the API across all upstream connectivity providers
- maintenance of a multi 10Gbps spare capacity to absorb malicious traffic incidents
- firewall measures both at the edge and internally
- obfuscation of public IP connectivity from cloud infrastructure where possible
- externally hosted cloud status page allowing status updates even during a potential total outage
- using IP proxies on core services (via CloudFlare) and other measures that can't be shared publicly
- automatic blocking of DDOS attacks

SSL Certificate

Secure Sockets Layer (SSL) Certificates are small data files that digitally bind a cryptographic key to a customer's account. SSL is mainly used to secure credit card transactions, data transfer and logins. CloudSigma supports SSL connections using individually generated private keys and a high encryption level. Two-factor authentication is offered as an additional option as well as security features that allow customers to white list only certain IPs for system access and other such access related security features. It is important that the customer retains sole root/administrative access to their cloud servers. Encryption is available to customers for their data on CloudSigma's cloud. Physical storage media is disposed of securely. Additionally, customers can choose to encrypt their data within their virtual machines at the boot level using an in-operating system encryption. Networking traffic can be encrypted between virtual machines at the customer's discretion again using in-operating system tools to achieve this.

Private Networking Interfaces

The CloudSigma cloud supports the ability for end-users to attach one or more private networking interfaces to their virtual machines. These networks are exposed as network card interfaces to the operating system of the virtual machine. By placing multiple virtual machines in the same private network, traffic can be passed securely between them. These private networks offer a 'virtual wire' implementation supporting all kinds of networking traffic including broadcast and multicast traffic which most cloud stacks do not support. Private networking traffic is passed over dual 10Gbps networking within the cloud.



Traffic separation

One of the key challenges of the cloud and Infrastructure-as-a-Service in particular is maintaining separation between different users on common infrastructure. This is the networking challenge in a multi-tenant environment as it is vitally important inhibit one user from viewing the internet traffic of another user. As a principal, different user networking traffic should be separated at the lowest level possible to provide the highest integrity separation. In CloudSigma's cloud the traffic is separated at the hypervisor level. CloudSigma also distinguishes between private and public network traffic. All traffic going between public IP addresses is routed over one set of hardware and networking devices with private networking traffic routed over an entirely separate physical network. This physical separation allows data within customer VLANs to benefit from full physical separation whilst in transit as well as hypervisor separation from other private networking traffic. Cloud servers can have multiple private networks and these VLANs can be connected to private lines instead of the shared Internet connectivity. Cloud servers can be configured to run only on private networks without a public IP interface. Private networks provide a 'virtual wire' between cloud servers supporting all traffic types including multicast and broadcast. As a public cloud operator, CloudSigma exclusively runs in Tier 3 and 4 data-centres which offer physical security to the highest standards with 4 to 5 layers of physical security:

- monitored and guarded perimeter
- entry man trap to inner secure perimeter
- biometric security with man trap for access to actual data center
- locked down cage in data center
- locked down rack in cage

5.2 Secure Cloud Access

On the authentication server, an openVPN instance is set up. It is configured as an access point and is using LDAP, therefore it is configured to use the same Single Sign-On scheme. It can be used to securely access all the related infrastructure.

6 Pan-European Information Exchange

One important aspect of implementing and establishing a pan-European information management system is the usage of a common exchange language as basis for the information sharing and collaboration.

Figure 30 presents the ideas of information providing and accessing information in cloud-based system like SecInCoRe. The intention is to provide an easy-to-use system to make feasible the integration into existing workflows.

Many organizations are using exchange languages; many projects have addressed the issue to define a standard for joint usage. References to existing approaches are given as the focus of the project is to leverage existing approaches but not provide a definition of a novel data exchange language.

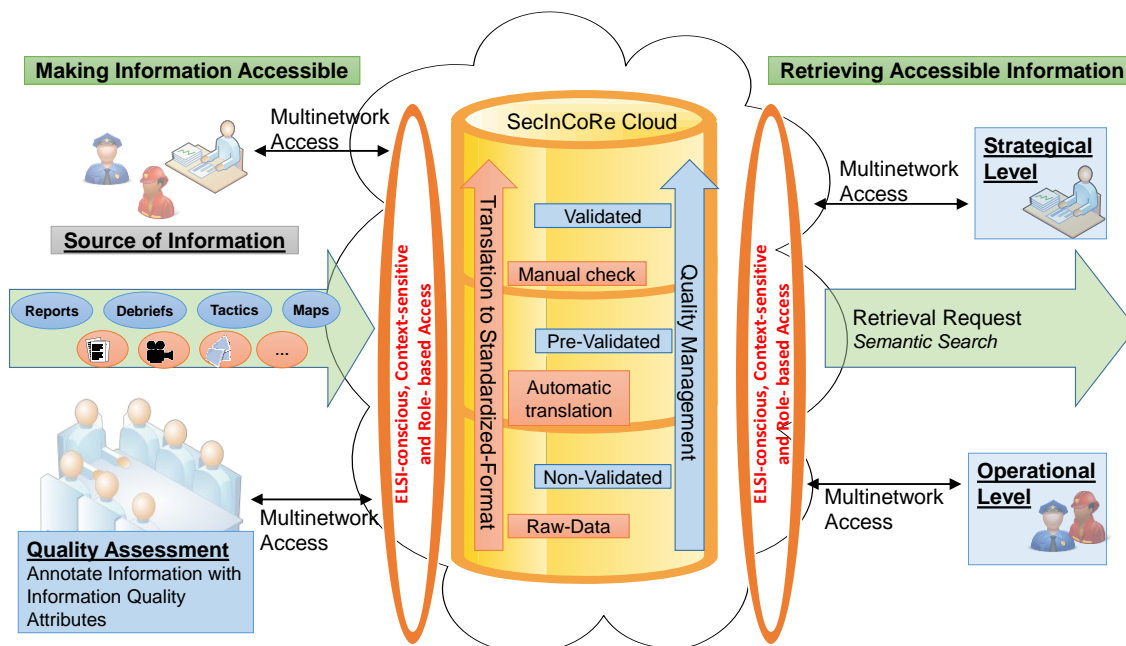


Figure 30 Information exchange using a cloud-based system

6.1 Protection and Rescue Markup Language (PRML)

The **Protection and Rescue Markup Language (PRML)** [prml] has been developed in the project SPIDER to enable the communication and information exchange for rescue forces in large incident scenarios. The intention was to support the coordination of rescue actions between all contributing actors. Hence, PRML should fulfil the following aims:

- transparent information exchange
- satisfy all regulations regarding data privacy and data protection
- identify and define interfaces connecting all integrated IT systems

PRML is defining information that will be exchanged digitally between organizations during a large-scale incident. For the definition of this exchange language XML has been chosen as conceptual language. Due to the addressed use case defined scripts include information regarding hospitals, e.g. capacity, patients, mission data, data used in simulations regarding traffic flow etc.

xmlns	http://www.w3.org/2001/XMLSchema
xmlns:tns	http://spider-federation.org/prml/1.0
targetNamespace	http://spider-federation.org/prml/1.0
elementFormDef...	qualified
include	schemaLocation=prmlAllgemeineTypen.xsd
include	schemaLocation=prmlPersonenDenaustauschTypen.xsd
include	schemaLocation=prmlEinsatzLeitsystemTypen.xsd
include	schemaLocation=prmlGebaeudemanagementTypen.xsd
include	schemaLocation=prmlSimulationTypen.xsd
include	schemaLocation=prmlKrankenhausTypen.xsd
include	schemaLocation=prmlListenTypen.xsd
element	
name	SPIDERDenaustausch
type	tns:SPIDERDenaustauschTyp
annotation	
documentation	Das Element dient zum Austausch schadensereignisbezogener Daten, wie Personendaten, Einsatzinformationen. Die Daten werden immer in einem definierten Rahmen uebertragen.
element	name=AnforderungKarten type=tns:DokumentTyp
element	name=AnforderungDokumentarten type=tns:DokumentArtenTyp
element	name=AnforderungScreeningFragen type=tns:PSNVFragenTyp
element	name=RollenAustausch type=tns:RollenTyp
complexType	name=SPIDERDenaustauschTyp

Figure 31 First layer of PRML structure (PRML.xsd)

PRML is defined using XSD-scheme files. Using these schemes Unified Modeling Language (UML) figures are generated. These figures support the technical description of structures. They include descriptions of individual elements and types. In Figure 31 an example of the structure is shown.

6.2 xHelp and DIN Spec 91287

The **xHelp** [xhelp] standardization approach was created in the German project LAGE by UPB. xHelp is a powerful tool which was transferred to **DIN Spec 91287**, a DIN specification for the information exchange between emergency response organisations. The standardization process implied significant reduction of complexity; therefore, SecInCoRe takes into account also the original xHelp source. According to Figure 32, xHelp consists of three core elements. All of them are based on an analysis of directives and guidelines as well as a multi-organisational interview study in Germany (Fire Department, Police, Federal Police, Red Cross, Technical Relief Agency, Deutsche Bahn, etc.):

- A semantic model describing all kinds of messages sent between actors in large scale emergencies. It covers messages bound to a certain format and free messages (like in conversations).
- A process model representing information flow in operations intra- and inter-organisational. The model is implemented in eEPC.
- A data format allowing to transfer the semantic models and the process model into a practical tool for IT supported information exchange. Existing IT standards like EDXL and TSO as well as generic frameworks like XÖV were analysed (for instance, in terms of field-by-field comparisons). Practical standards in terms of paper based forms (about 30 different types of message standards) were compared.

The resulting data format is prepared to support both IT supported information exchange as well as to derive paper based forms that simplify inter-organisational information exchange.

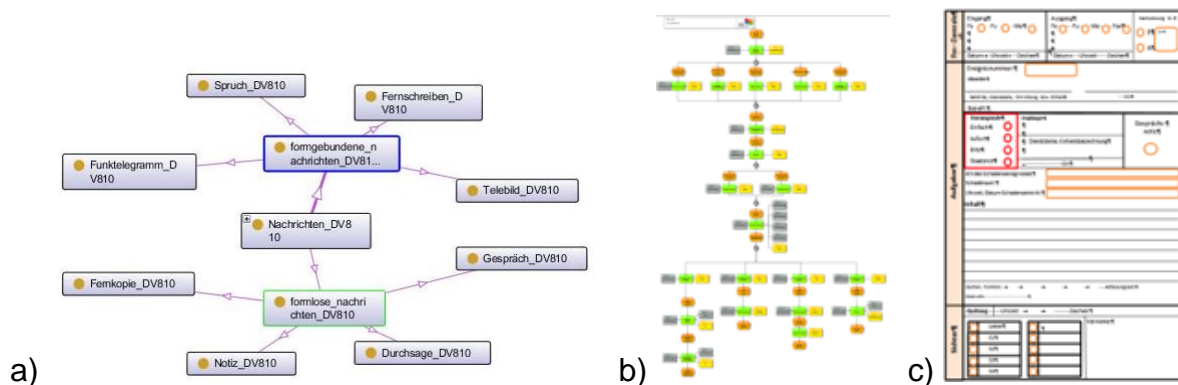


Figure 32 Three core elements of xHelp: a) Ontology, b) Process model, c) data format

For DIN Spec 91287, sample clients were implemented which help to adopt the standard specification and allow simple setup of messaging clients (see Figure 33).

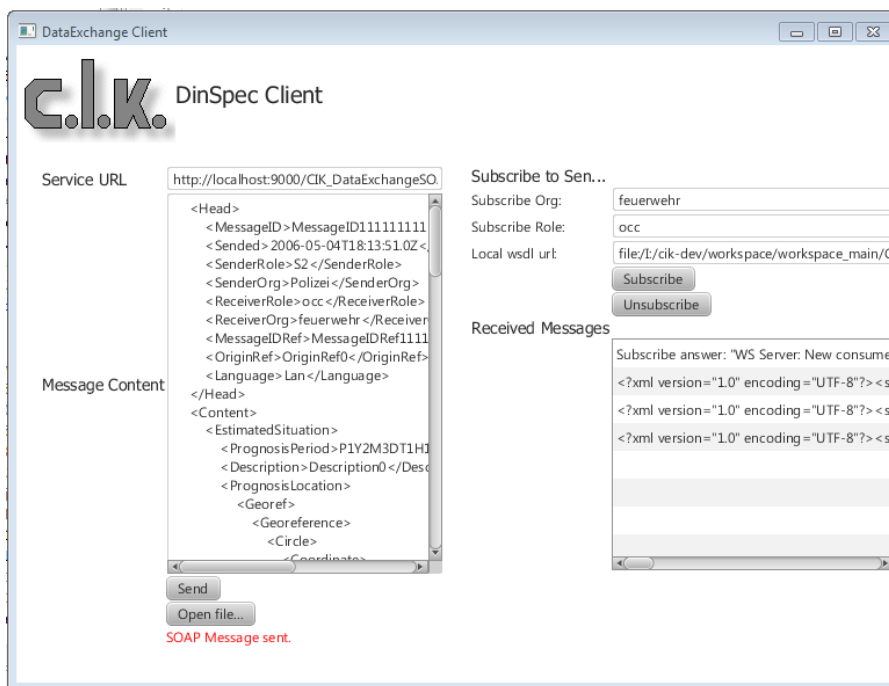


Figure 33 Reference implementation for DIN Spec 91287

6.3 Further approaches

Existing approaches	Description	Strong-and-weak-points of the approach
Unified Incident Command and Decision Support (UICDS)	Middleware framework for enabling information exchange in emergency situations. UICDS uses i.e. National Information Exchange Model (NIEM) Format or EDXL for exchanging data.	<ul style="list-style-type: none"> + Information system providers write UICDS adapters for their applications in order to connect to UICDS standards + UICDS is well established
Emergency Data Exchange Language (EDXL)	Support communication in emergency situations by defining a data exchange format.	



IEEE Incident Management Working Group 1512 (IEEE 1512/1512.2)	IEEE 1512/1512.2 provides a data exchange standard regarding traffic accidents.	
Tactical Situation Object (TSO)	TSO aims sharing a common operating picture (COP) by describing relevant aspects of a situation.	



7 Conclusion

The aim of the work package 4 in SecInCoRe is the conceptual design of a Common Information Space. Hence, it builds on the results of WP 3, on the one hand to integrate and derive a taxonomy and on the other hand, to make accessible and searchable the inventory results.

Starting with the requirement analysis in D4.1, the system views and concept of operations has been derived for D4.2. Whereas D4.3 and D4.4 highlight the different aspects of the conceptual design for Network Enabled Communication, secure cloud services and the semantic framework.

Therefore, this deliverable D4.4 finalises the work on different aspects of the design process. The designs are transferred to reference implementations and demonstration cases in WP 5.

- The taxonomy/ontology and subsequent semantic services offer novel ways to find documents for specific domains of interest;
- The RescueRoam provides a secure access to the cloud services for emergency organisations;
- Seamless communication methodologies like Network Coding or Multipath TCP increases the efficiency and reliability of data transmissions using multiple communication links and technologies;
- Mission Critical Services facilitate the introduction of new data applications and smart devices into TETRA and TETRAPOL networks.



8 Literature index

- [AlH09] A.-A. Al-Helali, A. Mahmoud, T. Al-Kharobi, T. Sheltami, "Characterization of Vertical Handoff Delay for Mobile IP Based 3G/WLAN Integrated Networks," in IEEE 69th Vehicular Technology Conference, 2009.
- [Dev05] V. Devarapalli, et al, "Network Mobility (NEMO) Basic Support Protocol" in Request for Comments (Draft Standard) 3963, Internet Engineering Task Force, 2005.
- [EhSt04] "QOM – Quick Ontology Mapping".
- [ELBB+04] "D2.2.3: State of the art on ontology alignment".
- [Gon13] M. A. Patino Gonzalez, T. Higashino, M. Okada, "Radio access considerations for data offloading with multipath TCP in cellular/WiFi networks," in IEEE International Conference on Information Networking (ICOIN), IEEE 2013.
- [Kat08] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "Xors in the air: Practical wireless network coding," in IEEE/ACM Transactions on Networking, vol. 16, no. 3, pp. 497–510, June 2008.
- [Kha14] Y. Khadraoui, X. Lagrange, A. Gravey, "A Survey of Available Features for Mobile Traffic Offload," in 20th European Wireless Conference; Proceedings of. VDE, 2014.
- [kodo17] Kodo Network Coding library. <http://steinwurf.com/products/kodo.html> (2017-02-21).
- [Kuh14] M. Kuhnert, C. Wietfeld, "Performance Evaluation of an Advanced Energy-aware Client-based Handover Solution in Heterogeneous LTE and WiFi Networks," in IEEE VTC Spring, 2014.
- [Mag11] L. Magagula, "Handover approaches for seamless mobility management in next generation wireless networks," in Wireless Communications and Mobile Computing, Wiley, pp. 1414-1428, January 2011.
- [prml] PRML documentation, <http://spider.kn.e-technik.tu-dortmund.de/de/prml.html> (2017-02-21).
- [Rie07] M. Riegel, M. Tuexen, "Mobile SCTP". Internet-Draft, version 9, IETF, 2007.
- [Sch17] C. Schäfer, T. Sauerland, J. Pottebaum, R. Marterer, D. Behnke, C. Wietfeld, P. Gray, B. Despotov, "Cloud-based Semantic Services for Pan-European Emergency Preparation and Planning," accepted for presentation on 11th IEEE International Systems Conference 2017.
- [Ste07] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration," RFC5061, IETF, 2007.
- [Su02] X. Su, "A text categorization perspective for ontology mapping".
- [Tra14] T. Tran, M. Kuhnert, C. Wietfeld, "Cloud voice service as over-the-top solution for seamless voice call continuity in a heterogeneous network environment", In Journal of Network and Computer Applications, Academic Press, vol. 41, pp. 250–262, 2014.



- [www1] https://en.wikipedia.org/wiki/Hyponymy_and_hyponymy (2017-02-21).
- [xhelp] DIN SPEC 91287:2012-07, Data interchange between information systems in civil hazard prevention, <https://www.beuth.de/en/technical-rule/din-spec-91287/152988042> (2017-02-21).
- [Zek12] M. Zekri, B. Jouaber, D. Zeghlache, "A review on mobility management and vertical handover solutions over heterogeneous wireless networks," Computer Communications, Elsevier B. V., 35(17), 2055-2068, 2012.