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

Deliverable 4.3 **Network Enabled Communication system concept and Common Information Space artefacts**

Olivier Paterour[1], Christina Schäfer[2], Alexandre Georgiev[3]

[1]Airbus Defence and Space, [2]University of Paderborn, [3]Cloud Sigma

April, 2016

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	30/04/2016
Sent to coordinator	17/05/2016
No. of document	D4.3
Name	*Network Enabled Communication system concept and Common information Space artefacts*
Type	*Report*
Status & Version	*1.0*
No. of pages	*103*
Work package	*4*
Responsible	*Airbus Defence and Space (ADS)*
Further contributors	*UPB* *CS*
Keywords	*Taxonomy, System Definition, Architecture, Network Enabled Communication (NEC), Secure cloud services*

History	Version	Date	Author	Comment
	V0.1	28/09/2015	ADS	Table of content
	V0.2	30/10/2015	ADS	Draft Content for sections related to taxonomy , NEC and cloud services
	V0.3	29/03/2015	ADS	Taxonomy (UPB) and NEC (ADS) sections updated
	V0.4	07/04/2016	ADS	First draft with the full content from UPB, CS and ADS
	V0.5	18/04/2016	ADS	Document ready for review and Q&A
	V0.6	02/05/2016	ADS	Document ready for monitoring
	V0.7	16/05/2016	ADS	Document ready for submission
	V1.0	31/05/2016	UPB	Finalisation for submission

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

Editor

Airbus Defence and Space

Olivier Paterour
Email: Olivier.Paterour@airbus.com

Authors

Airbus Defence and Space

Olivier Paterour
Email: Olivier.Paterour@airbus.com

University of Paderborn
C.I.K.

Jens Pottebaum
Email: pottebaum@cik.upb.de

Christina Schäfer
Email: c.schaefer@cik.upb.de

Torben Sauerland
Email: sauerland@cik.upb.de

Christoph Amelunxen
Email: amelunxen@cik.upb.de

Marc Bertram
Email: marc087@mail.uni-paderborn.de

CloudSigma

Alexandre Georgiev

Email : alexander.georgiev@cloudsigma.com

Reviewers

University of Paderborn
C.I.K.

Jens Pottebaum
Email: pottebaum@cik.upb.de

Christina Schäfer
Email: c.schaefer@cik.upb.de

Center for Security Studies
(KEMEA)
P.Kanellopoulou 4
1101 77 Athens
Greece

Giorgos Leventakis
Email: gleventakis@kemea.gr

ELSI Monitor

Centre for Mobilities
Research
Department of Sociology
Lancaster University
LA1 4YD
UK

Monika Buscher
Email: m.buscher@lancaster.ac.uk

Executive summary

This report gathers three topics which are key contributors to define the whole SecInCoRe concept:

- Taxonomy of used data sets, processes, information systems and ELSI
- Network Enabled Communication system concept
- Secure Cloud services

Chapter 2 provides a description of the taxonomy of used data sets, processes and information systems. SecInCoRe distinguishes the development of a taxonomy and an ontology. Moreover chapter 2 of this deliverable elaborate the work to 1) structure the PPDR domain with focus on processes, information systems, data sets and ELSI and 2) the process of choosing existing semantic approaches to be included in the ontology. Based on the results of the inventory of semantic approaches, the ontology will provide support regarding easy to use search functionality. The aforementioned work is founded on the grounds of the WP2 and WP3 output.

A first draft of the taxonomy is presented in this document and the possibilities for connecting existing semantic approaches with SecInCoRe's developments are reported in the deliverable.

Chapter 3 provides a description of the Networks Enabled Communications system concepts. This section starts by describing the general requirements for meeting interoperability and cross border communications and also reminds the legacy PMR services architecture concerns. Then two system architecture options are described:

- Option 1 : Interoperability with PMR services based on an extension of the legacy PMR services
- Option 2 : Interoperability with PMR services based on 3GPP standard solution (MCPTT/MCData/MCVideo)

A conclusion sums up and explains the pros and cons of the two options: both architectures may exist across European countries for many years since many of the public safety operators today are committed to sustain services on their legacy networks until 2025 (and even until 2030 in some cases). However, it is more than likely that a solution based on the definition elaborated by the 3GPP for Mission Critical Services will be the solution on which all the public safety operators across the Europe will converge and deploy.

Chapter 4 provides a detailed overview of the cloud service provisioning landscape by identifying best-in-breed virtualisation technologies and the support structures that exist today to automate their deployment, load balancing and auto-scaling capability, all the while ensuring security and privacy are maintained.

An overview of Hypervisor-based ecosystems and support services is presented, moving onto Containers and the frameworks and support structures these also facilitate. These two current best practices for service cloudification are then compared and contrasted, with strategies for the migration of legacy applications put forward.

Having described in detail what cloud today represents and the means by which services can be composed, Cloud Security principles and Cloud Security Services using the cloud paradigm are presented, moving onto the state-of-the art and future opportunities presented by 'edge' and 'fog' cloud, which will extend these best practices.

Finally, an overview of how SecInCoRe services are cloudified by using a combination of these technologies is described, including the SecInCoRe UI within containers and the Semantic Framework within VMs.

This section then goes into further detail to describe the Semantic Framework deployment and each comprising service's logical functionality.

Furthermore, work in WP4, specific technical solutions for supporting this system’s architecture are investigated (T4.5, T4.6).

Table of contents

1 Introduction

SecInCoRe's innovation relies on a Common Information Space (CIS) concept, dividing between the description of the specification of the CIS, related reference implementations and an ongoing refinement of demonstrations and demonstrator implementations to evaluate and proof the aforementioned concept. The CIS specification separates and distinguishes the socio-technical elements of the concept and the Cloud Emergency Information System (CEIS) concept from each other. The result of the combination is a co-designed socio-technical system to enhance interoperability of resources, communication and information management. The detailed structure of the concept is illustrated in Figure 1.

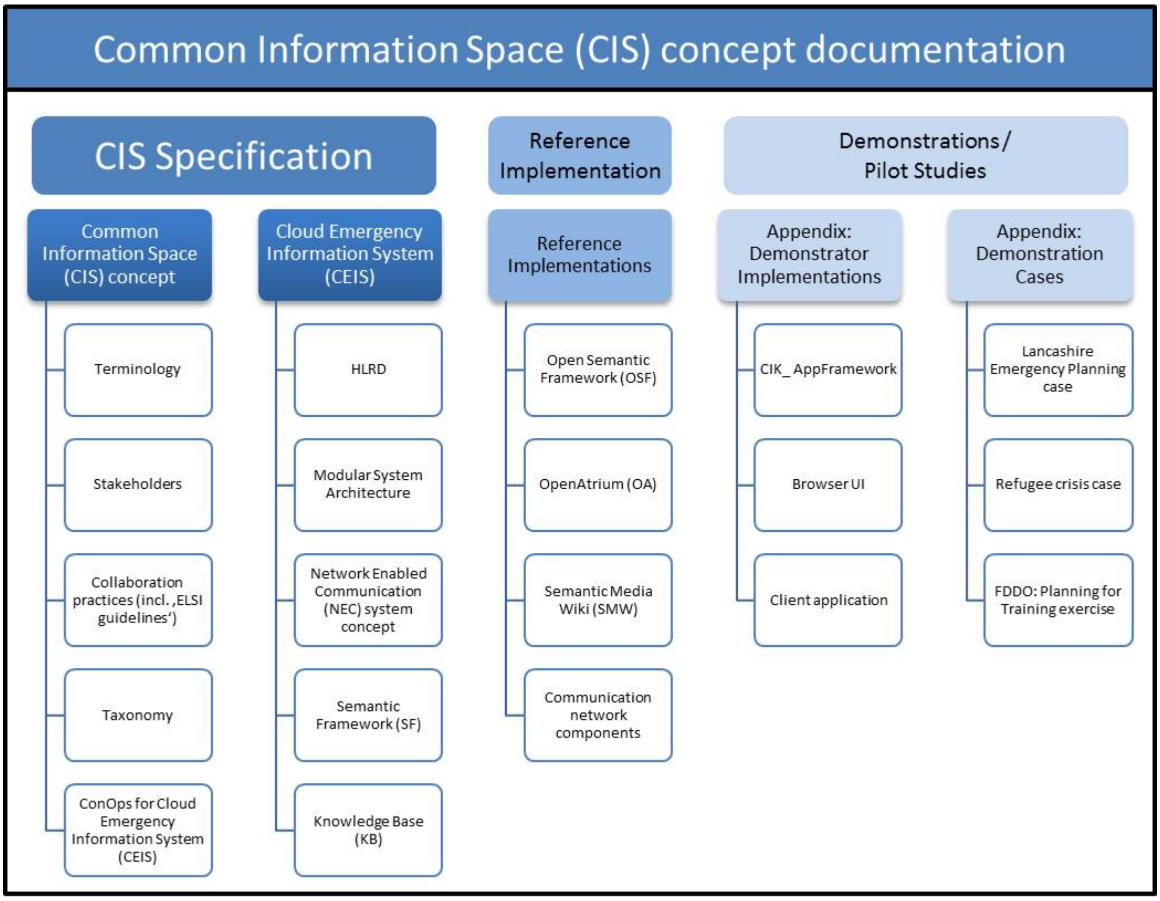

Common Information Space (CIS) concept documentation
CIS Specification
Reference Implementation
Demonstrations / Pilot Studies
Common Information Space (CIS) concept
Cloud Emergency Information System (CEIS)
Reference Implementations
Appendix: Demonstrator Implementations
Appendix: Demonstration Cases
Terminology
Stakeholders
Collaboration practices (incl. ‚ELSI guidelines')
Taxonomy
ConOps for Cloud Emergency Information System (CEIS)
HLRD
Modular System Architecture
Network Enabled Communication (NEC) system concept
Semantic Framework (SF)
Knowledge Base (KB)
Open Semantic Framework (OSF)
OpenAtrium (OA)
Semantic Media Wiki (SMW)
Communication network components
CIK_AppFramework
Browser UI
Client application
Lancashire Emergency Planning case
Refugee crisis case
FDDO: Planning for Training exercise

Figure 1 SecInCoRe CIS Concept (see D4.2)

1.1 Purpose of this document

The purpose of this D4.3 report is to describe the proposed approaches for:

- Taxonomy – based on combined approaches taken the CIS concept elements Terminology, Taxonomy, Semantic Framework, Knowledge Base and Collaboration practices into account. Overall the current status of a taxonomy and ontology covering the categories data sets, processes, information systems and ELSI is provided in this deliverable.

- Network Enabled Communication system concept – including parts from the modular system architecture and the NEC system concept from the CIS specification
- Secure Cloud services – this part provide insights regarding possibilities about the modular system architecture of the SecInCoRe project also considering the impact on the concrete reference implementations of the project.

1.2 Validity of this document

This document depicts the status of the work done by the SecInCoRe team related to the following concepts of the project:

- Taxonomy of used data sets, processes, information systems and ELSI
- Network Enabled Communication system concept
- Secure Cloud services

This deliverable represents a current state of work. Due to a collaborative workflow, an agile development process and moreover an agile dealing with requirements, changes may arise, but with a confident handling of risks, high scientific results will be ensured.

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] D2.1 Overview of disaster events
[5] D2.2 ELSI guidelines for collaborative design and database of representative emergency and disaster events in Europe
[6] D2.3 Report on performance, goals and needs and first draft of new crisis management models and ethical, legal and social issue
[7] Domain Analysis: Baseline and emergent future practices
[8] D3.1 Inventory Framework
[9] D3.2 First publication of inventory results
[10] D3.3 Second publication of inventory results
[11] D4.1 Requirement Report
[12] D4.2 System Views and Concept of Operations
[13] D5.1 Common information space for internal use
[14] D5.2 Early setup of evaluation model for internal use cases
[15] D5.3 Validation strategy and first functional 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 (including the implementation of the demonstrator) and are therefore related to the following documents directly:

[16] D4.4 Report on Interoperability Aspects

[17] D5.4 Validation report and final evaluation model of communication system concept

[18] D2.7 ELSI in crisis management through the Secure Dynamic Cloud

1.4 Contribution of this document

This document supports the conceptual design and realisation of the CIS. Therefore the work from several work packages will contribute to this deliverable. The development of a taxonomy and ontology gather the work from WP3, to define a model taken data sets, processes and information systems into account and results from WP2 to integrate ELSI in the semantic approach of SecInCoRe. Insights regarding the NEC system concept, and secure cloud services are based on the work of WP4.

1.5 Target audience

D 4.3 main target is the audience in the SecInCoRe project consortium as almost all the partners are engaged in standardisation.

Another potential target audience is the European Commission which may be interested in understanding how the SecInCoRe project intends to guarantee a long term use of the project results.

1.6 Glossary

Abbreviation	Expression
3GPP	3rd Generation Partnership Project
CEIS	Cloud Emergency Information Systems
CIS	Common Information Space
DoW	Description of Work
ETSI	European Telecommuncations Standards Institute
ICT	Information and Communication Technologies

Abbreviation	Expression
IT	Information Technology
KB	Knowledge Base
LTE	Long Term Evolution (of 3GPP)
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MCVideo	Mission Critical Video
NEC	Network Enabled Communication
OMA	Open Mobile Alliance
PEI	Pan-European Inventory
PMR	Private(Professional) Mobile Radiocommunications
WG	Working Group

1.7 List of figures

1.8 List of tables

2 Taxonomy of used data sets, processes, information systems

The overall aim of the creation of a taxonomy is to provide a combined classification scheme taking the inventory categories data sets, processes, information systems and ELSI into account (based on WP 3 and WP 2) (s. **Fehler! Verweisquelle konnte nicht gefunden werden.**). The application of the taxonomy is twofold: 1) the defined structure of the taxonomy enables a common understanding in the domain of PPDR and reflects the opportunity to standardize vocabulary and 2) the taxonomy will build the main structure for deriving an ontology, integrated in the SecInCoRe search functionality which make inventory content easily retrievable (see chapter 4.3, D3.3 and D5.3). This enhances the understanding and clarifies the differences between taxonomy and ontology defined for the SecInCoRe project. The taxonomy is a non-technical representation of gathered inventory content and the ontology will be available in a technical format. The following Figure deatils the differences and the distinct foundations the taxonomy and the ontology are built upon.

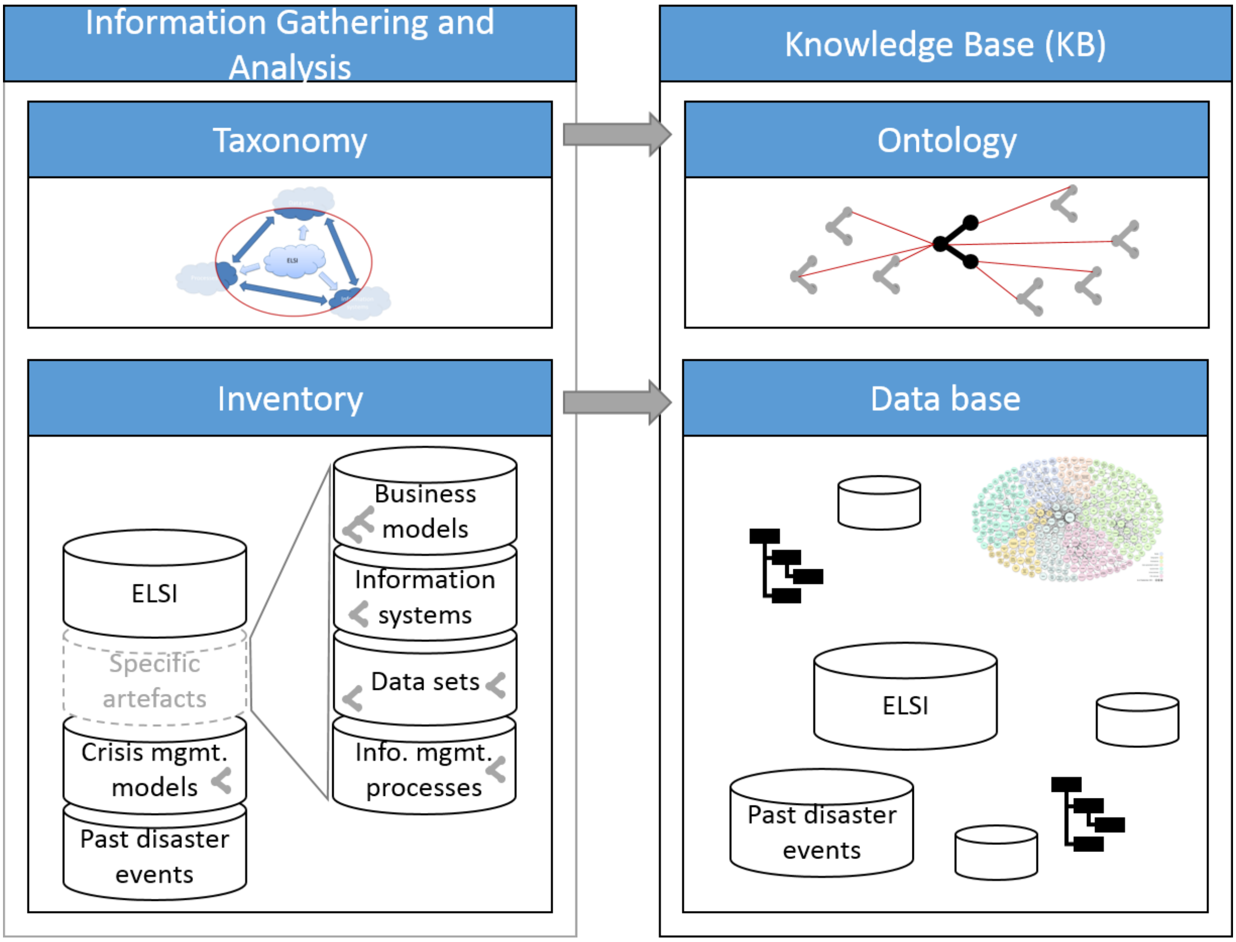


Figure 2 Differences between taxonomy and ontology in the scope of SecInCoRe

But of course taxonomy and ontology are cross-linked to each other, as is shown in the following Figure 3.

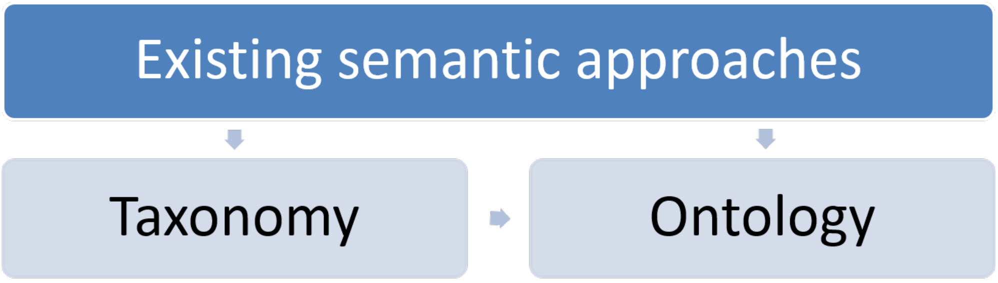


Figure 3 Connection between existing approaches, taxonomy and ontology

The development of a methodology as well as a work flow for designing new information and resource management services by merging new information with existing ones is also included in T4.1.

As described in the DOW [T4.1], D3.1, D3.2 and D3.3 the SecInCoRe taxonomy will cover four interlinked categories within the PPDR domain; namely these are the Information Systems, Processes, Data sets and ELSI reaching a comprehensive domain coverage (**Fehler! Verweisquelle konnte nicht gefunden werden.**). These categories will be used to classify the different approaches in the next steps. The aim of the SecInCoRe taxonomy is not to recreate new taxonomies for all of the categories, but rather to analyze the different existing approaches, find gaps and draw a connection between the different approaches. As a result, there should be the decision for the best fitting approach(es) for each topic, an extension of these approaches through our own work and a connection between the different categories.

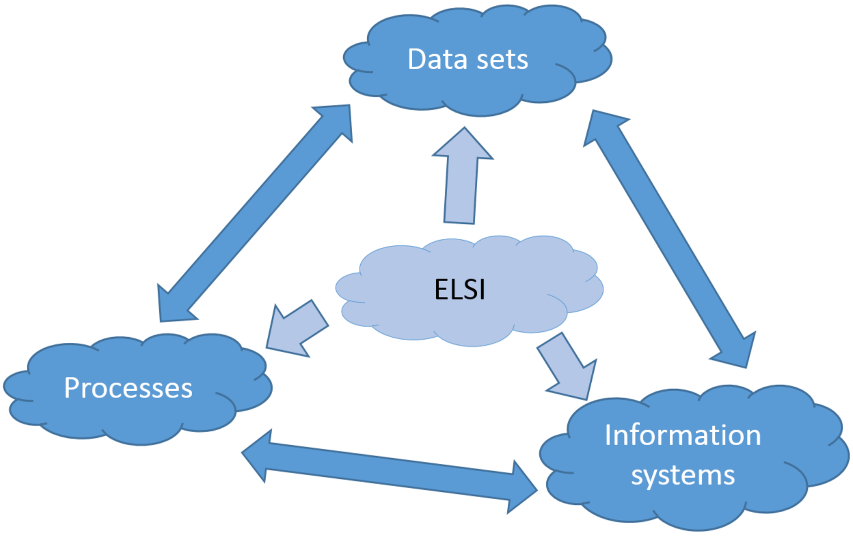


Figure 4 Categories to be covered by the taxonomy

In order to achieve the aim of creating a taxonomy and furthermore of an ontology, the following work flow is defined.

1. **Identify semantic approaches**

In a first step, relevant semantic approaches are identified. Currently there are no ways (or too many ways) for the categorisation of data sets, process models, information systems and ELSI. One major objective of SecInCoRe is an ongoing definition and classification of these issues (s. [DOW, Obj 2.1]). WP 3 and WP 2 support the work of the identification of relevant semantic approaches in order to build the basis for subsequent analysis and structure of identified information.

2. **Analyse existing approaches**
   Based on existing research a detailed analysis and a common understanding concerning existing approaches is essential. For that reason, the results of the inventory in WP3 and a review and analysis of existing approaches (see below) are taken into account, and good approaches and gaps are identified. Further smart requirements for the semantic approaches will be elaborated, in line with the defined High Level Requirements (see D4.2).
3. **Process existing / create new semantic approaches**
   Depending on the results of step two, either existing approaches are used as they are, existing approaches are combined with other or totally new approaches are created.
4. **Integrate into the SecInCoRe taxonomy**
   Methods for combining and integrating existing approaches with new developments are chosen and analysed. And in the end by the application of the identified methods a common taxonomy and ontology will be derived.

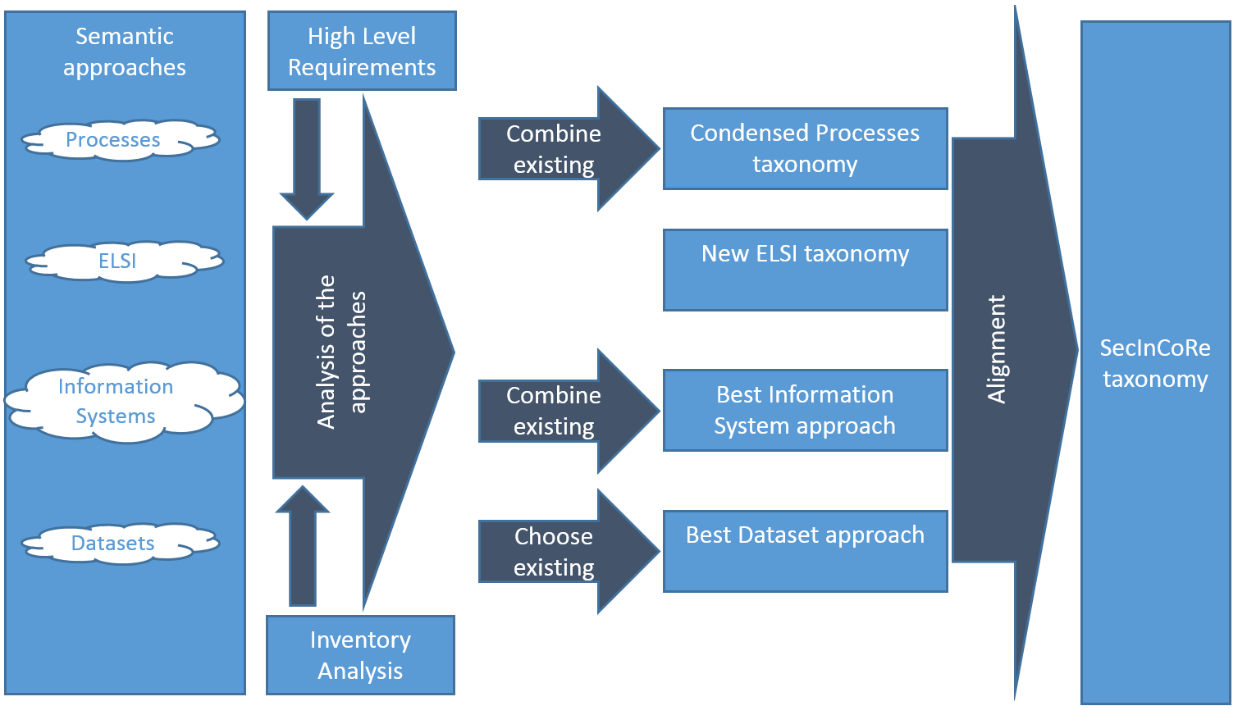


Figure 5 Workflow for deriving a taxonomy and an ontology

2.1 *Identification of existing semantic approaches in the Public Protection and Disaster Response domain*

A taxonomy is a "*system for naming and organizing things […] into groups which share similar qualities*" [www1]. Further in relation to the "Special Interest Group of the American Society for Indexing" Garshol describes taxonomies with regard to a so-called "*controlled vocabulary"* which is a *"closed list of named subjects, which can be used for classification"* [Gars04, p. 381]. The relationship between taxonomies and ontologies in the SecInCoRe context is described above. Garshol's definition is used in SecInCoRe to describe a taxonomy.

A brief overview of the already existing taxonomies and ontologies will be reported prior to the introduction of the SecInCoRe methodologies for the creation of taxonomies. There are several different definitions available concerning different categories of semantic approaches [FrMu00]. To simplify the use of the different words, the items in the following list are used as equivalents. The only distinction that is made concerns the difference between conceptual and technical elements as described above and therefore influencing, more the derivation of taxonomy or ontology.

- Glossaries and vocabularies
- Taxonomies
- Topic/Concept Maps
- Ontologies
- Object oriented schemas
- Data exchange formats

The taxonomy in SecInCoRe represents a categorization or a classification scheme which is based on the needs of stakeholders involved in PPDR and risk governance. In the context of SecInCoRe Use cases, perspectives and needs can vary per stakeholders (described in [D5.2, p. 35ff. and D2.4, Chapter 5]) or phase of the crisis management cycle (D2.4 Chapter 3). In addition, the perspectives with background to ELSI and to economic aspects can lead to several taxonomies. SecInCoRe aims at a taxonomy comprising the perspectives illustrated in Figure 4. The overall taxonomy includes all of these as it includes links between those specific sub-taxonomies.

Regarding the different needs of stakeholders, a subset of existing approaches are selected for covering most aspects of the SecInCoRe issues as described in **Fehler! Verweisquelle konnte nicht gefunden werden.**. In Table 1 an overview of existing semantic approaches in the different categories is shown. The table is based on [LiBr13] and beyond additional detailed investigation of existing sematic approaches. After that the connection to the SecInCoRe taxonomy is explained. In addition to existing approaches regarding taxonomies, data exchange formats with respect to emergency management will also be considered.

Table 1 Relation between existing approaches and SecInCoRe taxonomy

Inventory artefact	**Existing approach**	**Relevance for SecInCoRe**
Information systems	ISO 22745	The ISO 22745 is a standard for defining and exchanging master data based on the NATO Codification System (NCS) The standard also includes an identification guide which means a statement of requirements describing what data is needed about an item. This will be a basis regarding the work to deviate taxonomy for information systems.
	ISyCri	ISyCri is a French project that aims on improving information systems interoperability and coordination in crisis situations. For that purpose a Mediation Information System is provided to support involved organisations (e.g. medical units, police) with the possibility of exchanging information quickly and merging it into a global system of systems.
	BRIDGE	The BRIDGE project developed an architecture for the assembly of a system of systems of information systems and ICT applications. It includes standards for data exchange and aggregation (Zimmerman et al 2013, Ahlsén and Kool 2014) .
	STACCATO [WWW11]	The STACCATO project provide a taxonomy considering following aspects: Technologies and Components, Equipment and Sub Systems, Systems-Services Functions, Design-Manufacturing, Integrated Platforms and Systems and Human Factors, Missions Capabilities, Policy and Support.

Inventory artefact	**Existing approach**	**Relevance for SecInCoRe**
Data sets	TSO	While data sets mean all used or available data which have relevance before, in and after an incident, many different approaches will be taken into account. TSO provides a comprehensive vocabulary regarding emergency, while the MOAC ontology gathers information for crisis management activities in 70 classes and 30 properties. Furthermore HXL defines a set of vocabularies to describe populations affected by an emergency - deaths, injured, missing, displaced and non-displaced populations, refugees and asylum seekers. EMDat gives a classification of disasters, dividing them into groups and subgroups, such as geophysical, meteorological, hydrological, climatological and biological disasters. Different types of disasters are allocated into these subgroups and filled with data about occurred disasters (number of people injured, homeless and deaths). Similar to EMDat, the Canadian Disaster Database and the Australian Government Attorney-General's Department Disaster Database make past disaster events available. NIEM—the National Information Exchange Model—is a community-driven, standards-based approach to exchanging information developed in the US with several modular domain extensions. For covering more aspects GeoNames,
	Ontology of Information [GaWo11]	
	HXL	
	EMDat [WWW05]	
	Canadian Disaster Database [GoCa13]	
	Australian Government Attorney-General's Department Disaster Database	
	NIEM	

Inventory artefact	Existing approach	Relevance for SecInCoRe
	GeoNames [GeoN12]	Ordnance Survey Hydrology Ontology, USGS CEGIS and NNEW weather ontology are added, i.e. USGS CEGIS capturing topographical concepts and the NNEW ontology provides a formal conceptual model of the weather domain including 8 modules: humidity, lightning, measurement, precipitation, pressure, storm, visibility and wind. Inside of ISyCri a crisis ontology is provided, which consists of the studied system (e.g. people, natural sites, goods) and the crisis characterization (e.g. type, gravity and trigger). The ontology of information concerned the overall structure of information sharing in an emergency regarding information entity, bearer, event, instrument and agent. Next the above mentioned ontologies and databases various glossaries are considered to build basis vocabulary for emergency management, e.g. the Glossary of Humanitarian Terms and the Glossary and Acronyms of Emergency Management Terms. The EMERGEL core ontology is an ongoing work based on results from the DISASTER project. It contains knowledge and concepts related to emergencies and the stakeholders involved in a crisis situation.
	Ordnance Survey Hydrology Ontology	
	USGS CEGIS	
	NNEW weather	
	MOAC	
	ISyCri	
	Australian Emergency Management Glossary [WWW03]	

Inventory artefact	Existing approach	Relevance for SecInCoRe
	Emergency Preparedness Glossary [WWW04]	
	ICDRM/GWU Emergency Management Glossary of Terms [GWIC10]	
	IRDR Peril Classification and Hazard Glossary	
	Emergel [WWW12]	
Processes	ISO22320	For defining a sub-taxonomy regarding processes in the context of SecInCoRe with regard to all stakeholder needs, several existing approach will be taken into account. SOKNOS focuses on defining a hierarchical structure of material resource & human resource. Further FOAF provides terms for describing characteristics of people and can be used regarding the definition of stakeholder in the process. IntelLEO and Organisation Ontology both implement core base concepts the foaf:organization concept. The ontologies formalizes basic concepts for defining the organizational structure (organisation ontology does not provide category structures for organisation type, organisation purpose or roles).
	SOKNOS [Lim12]	
	FOAF [BrMi14]	
	GeoNames [GeoN12]	
	IntelLEO [JoSi11]	

Inventory artefact	Existing approach	Relevance for SecInCoRe
	Organisation Ontology [Rey10]	Moreover TSO builds a basis for different organization types, units and roles. GeoNames is a Linked Data approach for representing various locations in the world and can be useful for precise process definitions. SIADEX is an integrated planning framework for crisis action planning. It helps decision makers in crisis situations by designing firefighting plans and consists of two independent modules, the planning algorithm and the knowledge representation named BACAREX, which contains the information about the planning objects in firefighting scenarios (e.g. resources, places, facilities, task forces).
	TSO	
	SIADEX/BACAREX	
	NIEM	
ELSI	ISO/TC 233	There are no existing taxonomies on ELSI, but related endeavours that are useful for the production of ELSI inventory and guidelines include ISO/TC233, which develops international standards to increase societal security, and ISO/TC292, which focuses on standardisation in the security field to enhance safety and resilience with working groups on Emergency Management (WG3), Authenticity, integrity and trust (WG4) and Community Resilience (WG5). Standardisation Mandate 530, in particular Joint Working Group JWG8, which explores how to address and manage privacy and personal data protection issues during the design and development of security technologies and services.
	ISO/TC292	
	Standardisation Mandate 530/JWG 8	
	GDACS Guidelines	

Inventory artefact	Existing approach	Relevance for SecInCoRe
	JESIP	GDACS Guidelines on finding and providing disaster information and the Virtual OSOCC, a kind of common information space. JESIP, UK Joint Doctrine interoperability framework, containing categorisations and terms of multi-agency collaboration. Project ATHENA and its Framework for legal and ethical issues for the use of social media and ICT systems in crisis (D.2.8). IFRC (2013). Professional standards for Protection Work, especially Ch. 6 'Managing sensitive protection information'.
	Project ATHENA	
	IFRC	
Misc	WB-OS	The semantic concepts mentioned in this category are not taken into account for the SecInCoRe taxonomy. There are different reasons, why the approaches are not included in the above described categories: The first reason is, that the approaches are not available publicly. After that, all approaches, which don't fit into the categories are mentioned here. Lastly all approaches with a very special focus are added here, because they are not applicable to give a domain overview.
	BIO	
	ERO-M	
	BBK [WWW01]	
	UNEP-DITE [WWW02]	
	Glossary of Humanitarian Terms [RWP08]	
	Glossary and Acronyms of Emergency Management Terms [TRAD99]	
	English-French Emergency Management Glossary	

Inventory artefact	Existing approach	Relevance for SecInCoRe
	of Terms [OMCS11]	
	PSCAD	
	EPANET	
	THREVI	
	OTN [LoOh+05]	
	Ordnance Survey Buildings and Places Ontology	
	E-response Building Pathology Ontology	
	E-response Building Internal Layout Ontology	
	AktiveSA (multi-domain)	
	Hazard Ontology	

Besides the review of existing approaches of taxonomies, glossaries and ontologies, as well as related standards and codes of conduct, a number of other research projects, that may create useful data sets, processes or information systems for SecInCoRe, will be considered. A list is given in table 3.

Table 2 Research projects with useful aims regarding SecInCoRe

Research Project	Status	Description
INDYCO	Completed (2012-2015)	The INDYCO project (Integrated Dynamic Decision Support System Component for Disaster Management Systems) is a German project that aims on supporting relief forces in disaster management. Part of the

Research Project	**Status**	**Description**
		decision support system is a continuous situation assessment, which recognizes hazardous situations prematurely and gives alerts to help allocating resources. The main applications are flood situations and alpine avalanches.
MOVE	Completed (2007-2011)	The goal of MOVE (Methods for the improvement of Vulnerability Assessment in Europe) is to analyse the vulnerability to physical, technical, environmental, economic, social, cultural and institutional hazards in Europe. Therefore methods, frameworks and knowledge is created.
INACHUS	Active (2015-2018)	INACHUS supports urban search-and-rescue teams in cases of structural failures by increasing efficiency. It provides simulation tools to locate potential survival spaces depending on structure types and building material. Moreover decision and planning modules are implemented to assess damages and casualties by considering various information sources, such as laser scans, image data, mobile phones and different sensors.
REDIRNET	Active (2014-2016)	REDIRNET is a project to improve the communication between first responders of different agencies across the EU. A decentralized interoperability framework that is based on a public meta-gateway is created to overcome various business and cultural inhibitors, e.g. different doctrines, budgetary pressures and trust and security concerns between agencies and countries.
CRISMA	Completed (2012-2015)	The CRISMA project (Modelling crisis management for improved action and preparedness) provides, similar to INDYCO, a decision support system that helps modelling and simulating large dimensioned crisis scenarios of human, societal, structural and economic nature. A better understanding of the crisis evolution and the implications of the decisions to make by

Research Project	Status	Description
		considering simulated and real events is significant in cases where a prioritisation of actions concerning human lives and property is needed or response forces impend to lose control over the situation.
SECTOR	Active (2014-2017)	SECTOR deals with four main points that are learning from past events, cooperation, coordination and information exchange within the scope of trans-border collaborative crisis management to support first responders and police authorities. For that purpose a common information space is developed that provides an updated overview on the crisis evolution and information about available plans, resources and processes. Moreover it guaranties communication interoperability and enables activity coordination.
EPISECC	Active (2014-2017)	The project EPISECC (Establish a Pan-European Information Space to Enhance security of Citizens), similar to SECTOR, targets to create a common information space for an improved pan-European communication system, providing physical interoperability. A taxonomy and ontology model is developed that ensures semantic and syntactical interoperability.
IDIRA	Completed (2011-2015)	IDIRA (Interoperability of data and procedures in large-scale multinational disaster response actions) tried to improve multi-national and multi-organisational response actions in large-scale disasters by developing a technological framework. [WWW06]
SECRICOM	Completed (2008-2012)	SECRICOM (Seamless Communication for Crisis Management) developed a secure infrastructure for the communication of organisations in the field of public safety. [WWW07]
FREESIC	Completed (2012-2014)	FREESIC (Free Secure Interoperable Communications) developed possibilities to improve the communication and interoperability between

Research Project	Status	Description
		different organisations across Europe. [WWW08]
CRISP	Active (2014-2017)	CRISP (Evaluation and Certification Schemes for Security Products) aims to enable a level playing field for the European security industry by developing a robust methodology for security product certification. [WWW10]
DISASTER	Completed (2012-2015)	Aim of the project was to develop a common and modular ontology to gather all stakeholder knowledge in a flexible way. One result is the Emergel – framework.

2.2 *Methodology for bridging between concepts and building taxonomy or ontology*

In this section, the methodologies for the derivation of new taxonomies are defined, linking and extending existing approaches with SecInCoRe's research.

2.2.1 Methodology for derivation of new taxonomy or ontologies

In SecInCoRe the taxonomy to be developed is based on hierarchical classifications but does not necessarily include a tree structure between all characteristics.

There are mainly two different ways to build taxonomies according to [Niso05]; the bottom up approach takes the most used words and groups them to build a hierarchy. The other approach, the top down identifies the broadest terms first and then defines more specific terms, generating a hierarchy through this process. The two approaches are not opposites but highly compatible. Using them in tandem can improve results significantly.

In the following figure, a bottom-up approach is presented which is suitable for SecInCoRe since it allows a continuous extension and adjustment and is thus usable in an ongoing process.

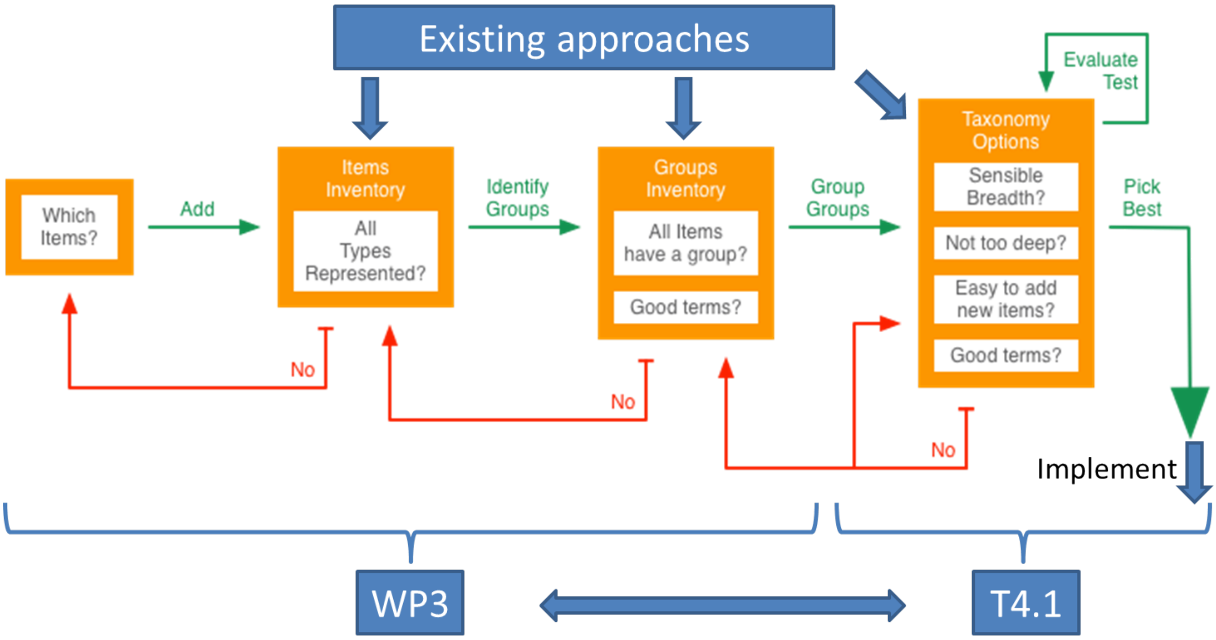


Figure 6 Process of deriving a taxonomy

Source: Adjusted illustration of [www2]

For this approach used in SecInCoRe, an initial vocabulary has to be defined, including several items. This is in accordance with the coherences described by McCreary [McCr06] (cp. Figure 2). In order to consider existing approaches, knowledge encapsulated in glossaries, data specifications and standards, ontologies and domain specific tools (like tactical symbol catalogues) has to be synthesised. Additionally the derivation of a taxonomy must include an analysis and synthesis of existing and well-established taxonomies.

In addition, the research on the four categories, undertaken in work package 3, is taken into account and provides further items. In the next step a categorisation will be derived by grouping those items and proof it against existing categories. Items can have an identical meaning or complement each other and belong to the same cluster groups. These groups will be merged to higher-level groups. For the categorization, card sorting techniques (cp. [McGr09]) can be used to develop a hierarchical model. All these activities lead to the definition of different hierarchies. These will be evaluated, tested and refined until the best one is chosen. Thereby a few things have to be considered:

- Broad or deep hierarchy: A broad hierarchy (many categories on the same level) makes a selection between many options necessary, a deep hierarchy (many levels) causes many selection steps
- Sequence: For a taxonomy one main questions is whether the order of levels is sensible or should be changed.
- Multiple appearances: This issue addresses the question whether an item should appear in more than one category.

- Single entries: There should be no single entry in one category. If there is a group with one item either it should be removed or other items should be added.

2.2.2 Connection of existing good approaches

There are several ways to draw a connection between different semantic approaches. The best-known methods are explained below, according to [NSH06]. Further [BEEF05] describe three different dimensions of heterogeneity in ontologies, which implies deviating effort to combine these approaches.

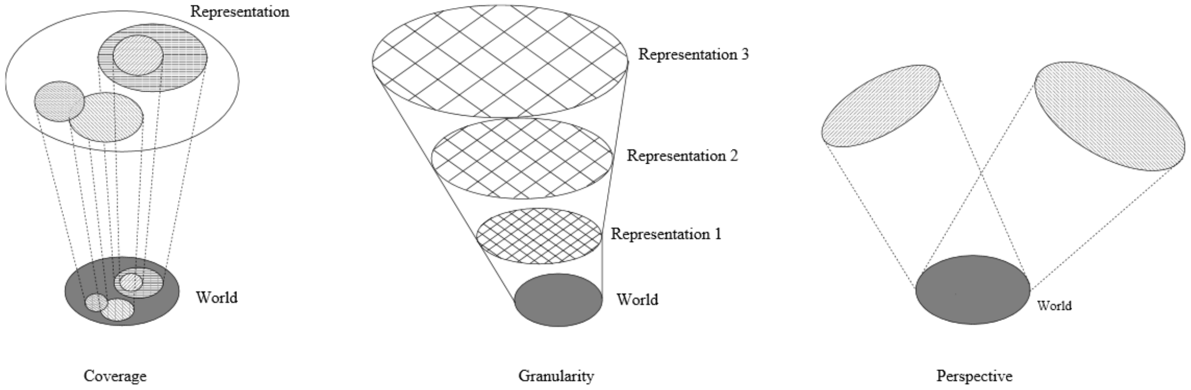


Figure 7 different dimensions of ontologies based on [BEEF05, S. 8]

- **Coverage:** Ontologies can cover different, same or overlapping contents of the world or domain.
- **Granularity:** Ontologies can cover the same, a lower or a higher level of detail for the same entity.
- **Perspective:** Ontologies can represent the same or a different view on the domain or world.

(Regarding further explanation see [BEEF05])

Based on the chosen approaches, different methodologies can be used to build connections between the approaches. 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]).

In detail the methods “Ontology Alignment” and “Ontology Merging” will be taken into account. But in particular the effort and complexity is growing in general from the “Ontology Alignment” to the “Ontology Merging”.

- **Ontology Alignment** aims to connect different ontologies by drawing connections between the concepts used in the different approaches.
- **Ontology Integration** aims to combine different ontologies addressing different topics into one single ontology (see [KHK05, S. 1])
- **Ontology Merging** aims to create one single ontology from different ontologies, which cover the same topic. (see [KHK05, S. 1])

2.2.2.1 Support regarding alignment or merging based on existing tools

There are several tools which offer functionalities for ontology alignment and merging. The range starts with simple tools which offer a visualisation to help doing a manual alignment and ends with scientific approaches which could enable an automatic merging. To find the best tools to enhance the building process of the SecInCoRe taxonomy, functional and stable tools are analysed and listed below. The tools will be tested with parts of the SecInCoRe-in-progress taxonomy, NIEM (ISO 3166) and MOAC. There are several steps necessary to enable an ontology mapping.

Vine (http://mmisw.org/orr/)

The online-tool Vine provides a Web interface with an integrated ontology repository. After selecting from the repository or uploading two ontologies, a mapping between the ontologies can be created manually by assigning one of the following operators to a pair of concepts: exactMatch, closeMatch, hasBroaderConcept, hasNarrowerConcept, relatedMatch. A new ontology is created as a result, which contains the two matched ontologies with additional skos[1]-annotations defining the matches. Besides the requirement to sign up for the tool, the permission to make the ontologies publicly accessible must be given.

Alignment API (http://alignapi.gforge.inria.fr/)

The Alignment API provides a programming interface that automatically creates a mapping between two ontologies and can be executed within a Java environment, with a web interface or via command line. The created mappings are stored in a RDF/XML file.

Agreement Maker Light (http://somer.fc.ul.pt/aml.php)

Agreement Maker Light comes with a java based graphical user interface for matching ontologies. A source and a target ontology can be selected and matched automatically considering a certain threshold. For the matching process several matching steps can be taken into account, such as a word matcher, string matcher, structural matcher, property matcher or coherence filter. After the process the matches are listed and must be evaluated by marking them as correct or incorrect. Additionally, more matches can be defined manually by allocating two classes or properties with the operators equivalence, superclass, subclass, overlap or unknown.

Blooms (https://github.com/jainprateek/BLOOMS,)

Blooms is a bootstrapping-based linked open data ontology matching system. For the execution a number of programming interfaces are required. A Java environment, the Jena API, the Alignment API, the WordNet Java API and the Bing Websearch API must be installed.

[1] Simple Knowledge Organization System for linking ontologies.

CODI (https://code.google.com/p/codi-matcher)

CODI provides the possibility to align concepts, individuals and properties of two heterogeneous ontologies via word-based similarities and scheme information. The matching problem is solved as an optimization problem. Therefore, the Gurobi Solver and a MySQL Database are required. An overview of the system architecture is shown in figure 11, the match process can be seen in figure 12.

COMA 3.0 (http://dbs.uni-leipzig.de/Research/coma.html)

COMA 3.0 is a schema and ontology matching and merging tool that provides an infrastructure to solve large real-world match problems. It comes with a web interface, as well as a GUI that requires Java and a MySQL Database and supports different matchers and schema formats, such as XSD and OWL.

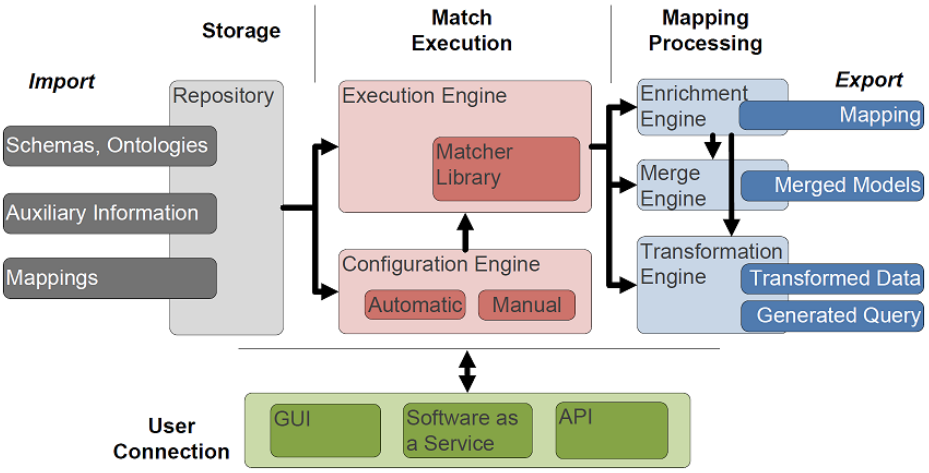


Figure 11 Overview of the COMA 3.0 architecture

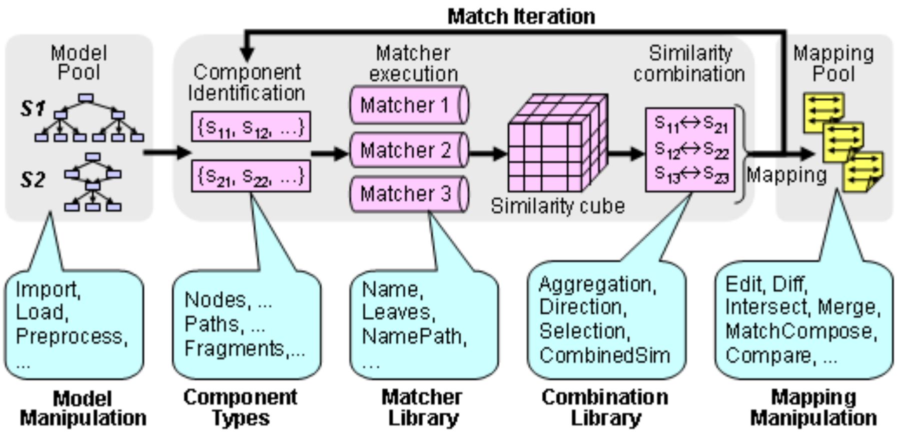


Figure 12 match processing in COMA 3.0

2.3 Definition of Requirements regarding semantic approaches

The argumentation for the decision of valuable approaches are based on criteria identified by literature research and the analysis of the High Level requirements (HLR) defined in the SecInCoRe project.

The following table describes the HLR considering the development of a taxonomy or ontology based on the status presented in D4.2 and the relation to the concrete work in conducting a taxonomy and ontology.

To define in detail steps and goals for the development of a taxonomy or ontology, a transformation into smarter requirements is necessary. A HLR is assigned to one or more components and outcomes of the SecInCoRe project. Therefore, the fulfillment of the requirement can only be ensured by a specification of all low level requirements (R1,..,R3 in the following Figure) for each component. The approach is shown in the Figure below.

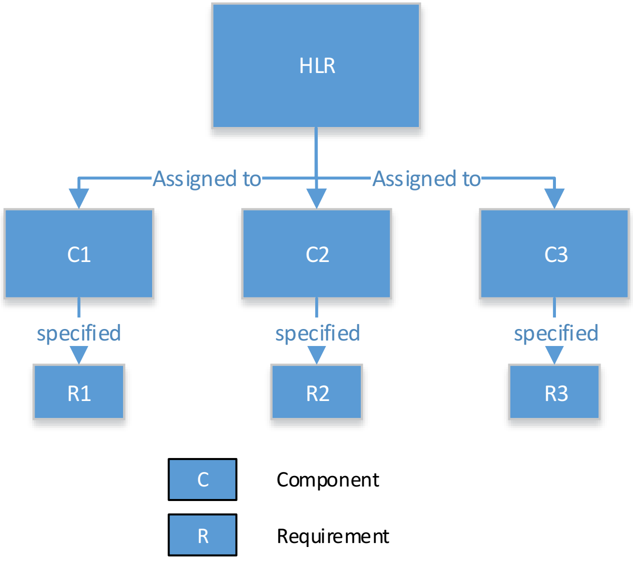


Figure 8 Connections between HLR and the different components

Table 3 requirements and respective transformation into SMART requirements

Number of requirement	**Description of requirement**	**Transformation**
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. This requirement also needs to be addressed by the CIS.

SICR-149	Information aggregation should be based on reliable sources of information	**The SecInCoRe-Ontology will be based on literature, existing sematic 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.
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.
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.
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.
SICR-114	Support inclusiveness through search	**The SecInCoRe-Ontology will be based on literature, existing sematic approaches and ontologies and will prompt references to ELSI guidelines.** The guidelines will help to identify missing voices in the current situation.
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’.
SICR-112	Alert users to danger of unlawful re-identification	**Rejected** - Not relevant at the level of taxonomy/ontology’
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..**
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.

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 FoI requests.
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.
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.
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.
SICR-103	Support users in respecting human rights	**The SecInCoRe-Ontology will include ELSI related concepts.**
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.**
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.**
SICR-88	Search based on location, type of disaster	**The SecInCoRe-Ontology will cover concepts 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.**
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.
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.**
SICR-61	Indicator of available resources	**The SecInCoRe-Ontology will integrate concepts regarding resources.**
SICR-59	Status of involved assets	**The SecInCoRe-Ontology will integrate concepts regarding assets.**
SICR-58	Status of engaged agencies	**The SecInCoRe-Ontology will integrate concepts regarding agencies.**
SICR-56	Advanced search capabilities	**The SecInCoRe-Ontology will integrate concepts regarding capabilities.**
SICR-54	Search Categories Options	**The SecInCoRe-Ontology will cover concepts 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.**
SICR-20	Classification of information	**The SecInCoRe-Ontology will classify inventory content in accordance to the definition of the included concepts.**

Based on the transformation from high level requirements to more smart requirements four main aims could be identified. These requirements are included in the decision for the use of existing approaches and part of the further work in the individual taxonomies / ontologies.

Overall, there are the following main issues, which should be addressed by the taxonomy.

1) To include ELSI in the ontology and therefore define taxonomies in this direction,
2) To document every concept based on literature or existing approaches,
3) To define concepts to describe different incident scenes and information needs in different level of detail and therefore also classify inventory content (including the date, resources, assets, agencies and capabilities).
4) To enable collaboration of first responders through a better understanding of connections of search results based on the ontology and it´s visualization.

2.4 Decision for existing semantic approaches

To elaborate the best fitting approaches, all the approaches mentioned above are analyzed with the value-benefit analysis. According to Zangemeister [Zang76], this method analyses complex action alternatives, to sort them according to the preferences of the decision maker, using multidimensional aims. The procedure of the value-benefit analysis is described [BiMR04] with the following steps:

1. Define criteria describing the aims
2. Weight the criteria
3. Rate every alternative
4. Calculate the value-benefit
5. Assess the benefit

These steps are processed in the following to find the best fitting semantic approaches. The steps one and two and the steps three and four are merged into one.

2.4.1 Define and weighing of criteria describing the aims

The criteria are defined based on the requirements discussed above regarding ontology and taxonomy approaches and further depending on general scientific values for working with semantic approaches.

First of all K.O.-criteria have to be clear and reduce quantity of possible sematic approaches. If these criteria are not matched, the approach is not taken into account. Here one aspect is of importance: the **availability of the approach**. I.e. some ontologies are discussed in research papers, but full source of the ontology is not available. These approaches are left out for further work in relation of identifying and combing valuable approaches. Hence the weight of this criterion is 0 or 1.

All other criteria are non K.O.-criteria but are also scored on a scale between 0 and 1. Overall all criteria will be weighted and provide an added value for the taxonomy or ontology. Both the condition to define the scale concerning the respective approach and the indication for the weight in relation to the importance are described in the ongoing section.

Power and depth of the approach and respective information are the next criteria to score all available sources. To conduct an objective rate, these higher level criteria are split up into more detailed variables:

- **The semantic type and richness.** Possible types that have been mentioned already: glossaries, databases, taxonomies, data exchange formats and ontologies. These different types describe more or less semantic relations of relevant topics of a domain. Simple glossaries will have the weight 0,2 where rich ontologies will have the weight 1. Other approaches are placed in between these before mentioned.

- **The number of concepts, columns or tables** (depending on the type of semantic approach). This criterion indicates the comprehensiveness and depth of the approach. The criterion will have a weight of 0,2 to include valuable approaches. The approaches will be scored as follows:

NUMBER OF CONCEPTS	SCORE
>1500	1
1000-1500	0.8
500-1000	0.6
100-500	0,4
10-100	0,2
<10	0.1

- **The domain-category coverage.** The domain coverage is divided into the main scopes of the taxonomy or ontology, data sets, processes, information systems and ELSI and scored in these relations. The requirement analysis forces concepts to describe incident scene and related artefacts. Therefore the domain-coverage is an important criterion in the SecInCoRe project. The weight will be 0,3. The approaches will be scored with 1, if the degree of coverage represents nearly the complete domain and 0,1, if the domain is only very partially covered.

Next the **up-to-dateness** will be taken into account to identify valuable and applicable semantic approaches for the SecInCoRe project and to ensure further development in the approach. The weight will be 0,1. The approaches are scored with 1, if they are from 2010 or newer and with 0, if they are older than 1990.

Especially based on the requirements definitions the importance of the **use of trustworthy sources** and standards becomes clear. Therefore the trustworthiness of the grassroots of the approaches will influence the score. The weight will be 0,1. If the approaches rely on governmental sources, they are scored with 1. Otherwise they are scored with 0.

The overall aim of SecInCoRe is to enable Pan-European collaboration between various first responder organisations. For that reason the consideration of a **European perspective** in the approach is a dedicated criterion. The weight will be 0,1. The approach will be rated with 1, if the approach has an origin in an European country, with 0,5, if the origin is not from within Europe, but could be applicable for Europe and 0, if it is not European and not applicable.

An additional indicator in relation with technical solutions are the syntactical correctness of the approach, most important for ontologies. With the use of existing tools correctness will be ensured or degraded the approach.

2.4.2 Rate every alternative and calculate the value benefit

All approaches identified in our research will be evaluated based on the criteria described above. In the following table the rating of approaches regarding data sets are presented to show the application of the methodology.

Table 4. Value-benefit analysis of semantic approaches

	Availability	Semantic type and richness	Number of concepts, columns or tables	Domain-category coverage	Up-to-dateness	Trustworthy source	European perspective	Total
weight	1	0,2	0,2	0,3	0,1	0,1	0,1	1
TSO	1	0,8	0,8	1	0,8	1	1	**0,9**
Ontology of Information	1	0,6	0,1	0,1	1	0	0,5	**0,32**
HXL	1	0,4	0,2	0,2	1	0	0,5	**0,33**
EMDat	1	0,4	0,2	0,8	1	1	1	**0,66**
Canadian Disaster Database	1	0,4	0,2	0,2	1	1	0	**0,38**
Australian Government Attorney-General's Department Disaster Database	0							**0**
NIEM	1	0,8	0,5	1	1	1	0,5	**0,81**
GeoNames	1	1	0,2	0,2	1	0	0,5	**0,45**
Ordnance Survey Hydrology Ontology	1	1	0,4	0,2	0,8	1	0,5	**0,57**
USGS CEGIS Geographic Information Ontology	1	1	0,3	0,2	1	1	0,5	**0,57**
NNEW weather ontology	0							**0**
MOAC	1	1	0,4	0,5	1	0	0,5	**0,58**
ISyCri	0							**0**
Australian Emergency Management Glossary	1	0,2	1	0,2	0,3	1	0,5	**0,48**
Emergency Preparedness Glossary	1	0,2	0,5	0,2	0,3	1	0,5	**0,38**
ICDRM/GWU Emergency Management Glossary of Terms	1	0,2	0,6	0,2	0,3	0	0,5	**0,3**
IRDR Peril Classification and Hazard Glossary	1	0,2	0,3	0,2	1	0	0,5	**0,31**
Emergel	1	1	0,8	0,6	1	1	1	**0,84**

The value-benefit analysis has some disadvantages. The synthesis of the single value-benefits into one aggregated value-benefit needs all criteria to be equally cardinally measurable. After that all criteria have to be independent from each other [Gabl15]. After that the value-benefit analysis is influenced by subjective aspects [GeLe14]. For that reasons, the value-benefit should be a strong indicator, but not a strict decision. It is a step to make the decision process more transparent and understandable [BlLü95].

2.4.3 Decision results

As the results have shown, there are many different values in the different categories:

In the processes category there are several different semantic approaches. The issue with these approaches is that the processes are not at all standardized across different countries. Partly they are even not standardized within countries. Therefore we decided to try to build a synthesized approach based on different available process descriptions, instead of choosing an existing one.

In the information system category no entirely sufficient approach was found. Therefore a combination of existing approaches and the results of WP3 should be used.

In the dataset category suitable approaches were identified. The best rated approaches are TSO (Tactical Situation Object), Emergel and NIEM. To choose the best fitting one of these three, the approaches were analysed in detail. NIEM is a broad approach from the US, which contains concepts from different domains, but is up-to-date and supported by communities. Nevertheless TSO vocabulary describe in more detail possible data sets which may occur in an incident scene. Therefore the taxonomy of data sets will base on TSO but both other (NIEM and Emergel) will be taken into account to ensure a comprehensive view.

In the ELSI category, there are no existing taxonomies, but a range of efforts to formulate best practices and codes of conduct in relation to networked collaboration and information exchange in PPDR and risk governance have been reviewed. The ELSI task force led by SecInCoRe pioneers production of an ELSI taxonomy for networked collaboration and information exchange in PPDR and risk governance. This integrates efforts from a range of projects, including BRIDGE, EPISECC, SECTOR and REDIRNET. We are constructing an inventory of ELSI and ELSI Guidelines, building on reviews of relevant existing initiatives (see Table 1).

2.5 Good value approaches and ongoing work in the taxonomy artefacts

This section describes the chosen semantic approaches and ongoing work for the taxonomies of Processes, Information Systems, Datasets and ELSI in detail.

2.5.1 Taxonomy of Processes

None of the approaches identified to describe processes and information management practices cover a holistic European perspective. For that reason based on the knowledge of the existence of these approaches and knowing the differences in the command and control systems in each European country a combined solution will be needed.

In a first step, a subset of existing command and control systems have been chosen, analysed and used to identify relevant class names and sub classes. The items of the different command and control systems will be compared, proofed for identical meaning and grouped into a new structure. This means in detail:

1) Identifying equal defined elements in all chosen command and control systems and define relations
2) Group more items from the command and control systems in the taxonomy

Regarding the first step, the SecInCoRe approach divides 4 different levels within the command and control systems:

- **First level „Command and Management“** – considering the task of the organisation especially during an incident
- **Second level „Command Post“** – considering mobile or stationary command posts during an incident, the measurement to efficiently overcome a critical situation and incident related information
- **Third level „Command System“** – taken the incident command, command process and moreover the command and control structure into account. In a next step the process to gain operational information will be listed.
- **Fourth level “Command process”** – considering the assessment of the situation and decision-making processes

The following Figure provides an overview about the reference command system.

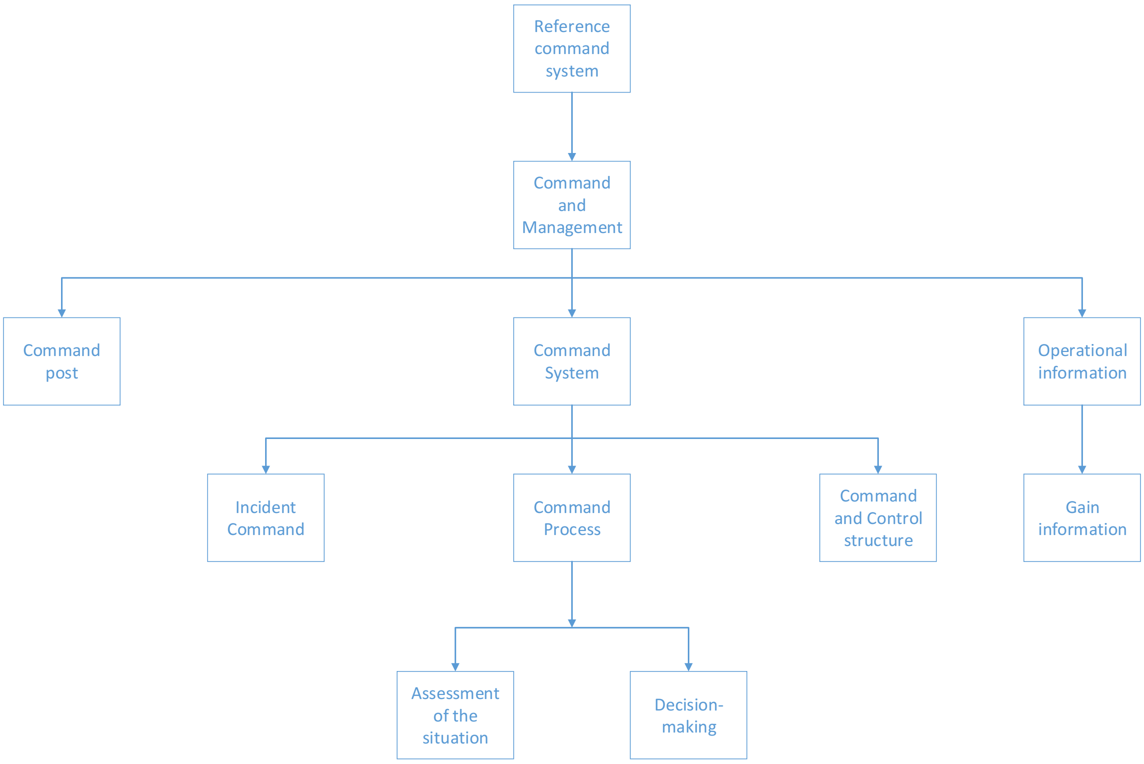


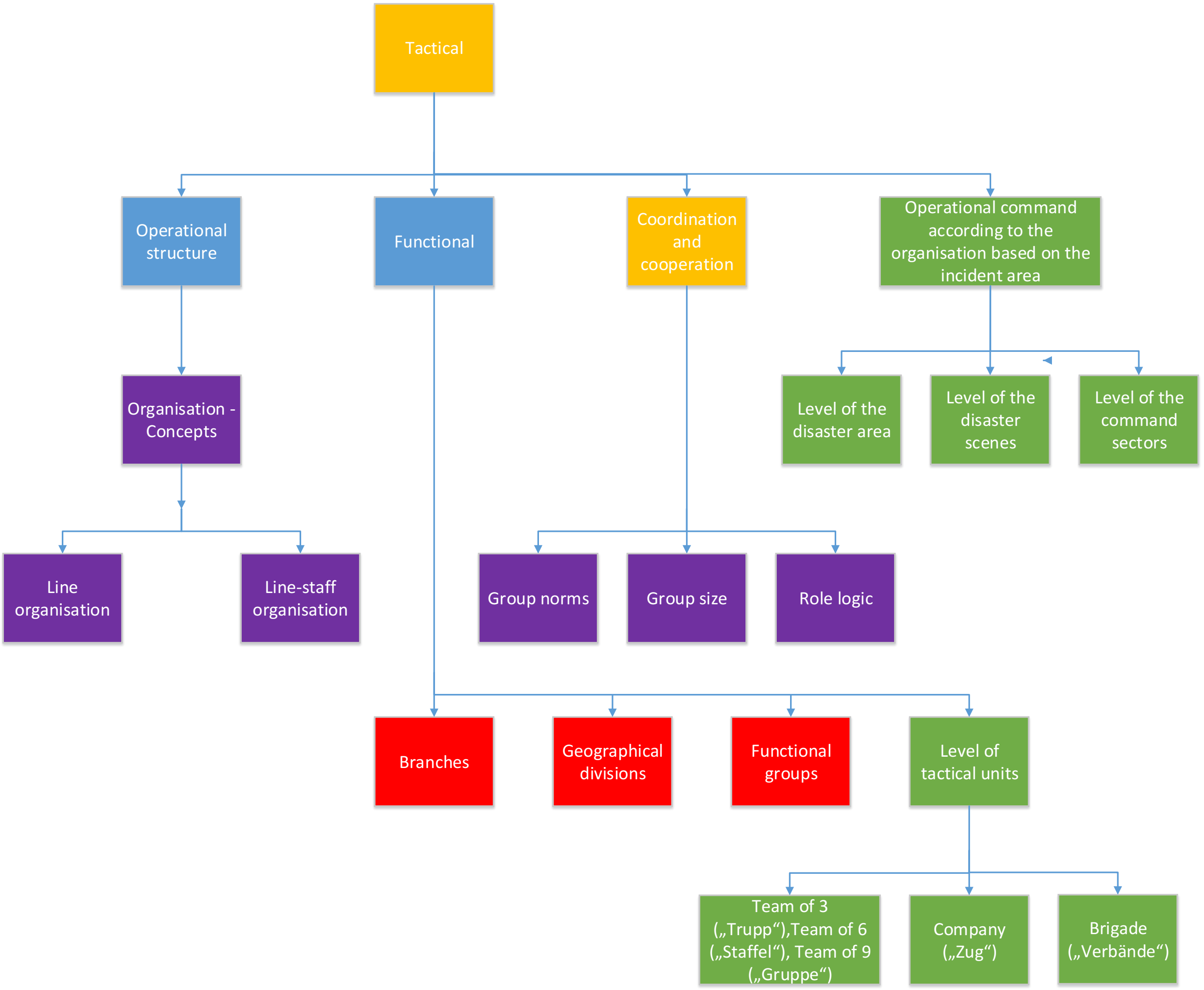
Figure 9 Common elements of 4 command and control systems

The different structures in the command and control processes complicate the design of a common process model.

2.5.1.1 *Combination of not equal elements in the command and control systems*

In this taxonomy approach, two European models are integrated, the ISO 22320 as an international standard and the NIMS as an outlook to a well know American system.

The following Figure illustrates a little part of the taxonomy (due to readability). The different color indicates the various sources of the defined items and shows possibilities for integration.


Tactical
Operational structure
Functional
Coordination and cooperation
Operational command according to the organisation based on the incident area
Organisation - Concepts
Level of the disaster area
Level of the disaster scenes
Level of the command sectors
Line organisation
Line-staff organisation
Group norms
Group size
Role logic
Branches
Geographical divisions
Functional groups
Level of tactical units
Team of 3 („Trupp“),Team of 6 („Staffel“), Team of 9 („Gruppe“)
Company („Zug“)
Brigade („Verbände“)

🟡	[ISO22320]	International Standard: „Societal security — Emergency management — Requirements for incident response“; ISO 22320: 2011
🟢	[FwDV100]	DV 100: „Leadership and Command in Emergency Operations“; 2007
🔴	[NIMS]	U.S. Department of Homeland Security: „National Incident Management System“; 2008
🟣	[SCMW]	Svensson, Stefan; Cedergårdh, Erik; Mårtensson, Ola; Winnberg, Thomas and the Swedish Civil Contingencies Agency: „Tactics, command, leadership“; 2005 (ISBN 978-91-7383-031-7)
🔵	added	

Figure 10 Part of the Process Taxonomy

The colours indicate the source of the respective item. But it is possible to compare and combine the different aspects in one taxonomy.

2.5.1.2 Documentation of items

To enable a common understanding of items in the taxonomy, a template was designed to ensure the validity of the respective item. In this structure the meaning and influence of the class of the taxonomy is documented and make a translation to an ontology possible.

Table 5 Template do document Taxonomy items

Language(s): The language used on the template relating to the respective term is specified at the top. The template of an element can be prepared several times by using different languages. In this case every available language is specified, so that someone can choose the preferred version.	
Terminology (Term): The terminology (Abbreviation: Term) consists of words and compound words or multi-word expressions that in specific contexts are given specific meanings. Every element is identified by its terminology in connection with the corresponding information source. The Terminology can be limited to one or more languages.	**Abbreviation:** The abbreviation is a shortened form of the words or multi-word expressions which are specified in the terminology. It consists of a group of letters taken from the terms. An included assumption is that only valid and accredited abbreviations are mentioned on the template.
Information source: The information source is a reference to a link or literature of an element that provides knowledge about it. The type of source is defined in the next step.	
Type of source: There are different types of information sources for the elements. This function should help to determine the information source by four given categories. The type of source are differentiated between norm, regulation and suggestion. If none of these three sources fit into the context, there is a possibility for the operator to add a different type of	**Level of validity:** The level of validity shows where the terminology of the specified source is valid. The validity could be cross-national (international), just in one country (national), in federal states of a country (federal states) or at a regional level (municipal). Afterwards the validity can be described in more detail during the description.

source.

- Norm
- Regulation (e.g. statute)
- Suggestion

- International
- National
- Federal States
- Municipal

Domain:

The domain determines the specific branch of the element, because every single element belongs to at least one domain. The central goal is a classification relating to the relevant domain and to separate the elements from other domains.

- Fire brigade / Fire department
- Police
- Emergency medical services (Abbr.EMS)
- Military
-

Domain specific synonym:

The domain specific synonyms are elements with a similar meaning like the given term on the sheet, but with the addition that the synonyms belong to another information source. There should be a reference to the templates of these elements, because the intention is to show commonalities between different elements and their relationship to each other. The synonyms should be specified in the same language and must belong to the same domain.

Element:

The terminology should be allocated to a specific kind of element. Therefore some choices are denoted:

- Process
- Object
- Institution (e.g. national institution)
- Location
- Basic model (Organisation/Structure)
- Position

If none of these elements fit to the term, there is a possibility to add a different kind of element. This possibility should ensure an accurate definition.

Description:

The description should specify the meaning of the given term. It represents characteristics and aspects of the element in detail with the aim of getting a first impression and understanding of it. The meanings may deviate from the meanings the same elements have in other contexts or other domains.

Wikipedia link:

If the content of the description can be found in an article of Wikipedia, the corresponding link is declared. Wikipedia is a public everyday reference system, and that this is counterbalance with more rigorously scientific and authoritative domain specific sources under the category ;Literature'

Hypernym:

The hyponym, also called subordinate, is a more specific element than the hypernym and its content is more detailed than the hypernym. It belongs to the category of the hypernym. There can be more than one single hypernym as superordinate for a hyponym if there exists more than one ordinary context or different hierarchies relating to the hyponyms.

Hyponym:

Every keyword or term that is associated with the element can be denoted. It helps to describe the element and allows it to be found again by searching. Also tags could reveal similarities with other elements.

Tags:

Every keyword or term that is associated with the element can be denoted. It helps to describe the element and allows it to be found again by searching. Also tags could reveal similarities with other elements.

Literature:

The indication of literature refers to the source of the description and includes the declaration of a connected link.

Weblinks:

Beside the indication of a link directly related to the description, there can be more weblinks. The weblinks refer to other sources on the internet with the same descriptions of the elements.

2.5.2 Taxonomy of Information Systems

Several works to classify or describe information systems in relation to emergency management and response already exist (see [LoKi14], [WWW09]). However this is not a holistic view considering a European perspective or including functions and mechanisms of the respective system. Other research projects have taken this into account e.g. CRISP but do not reach a comprehensive result. Moreover the NATO Classification Code provides an approach to classify and categorize technical equipment, first done for military logistics (see also ISO 22745).

These approaches will be used to cover the SecInCoRe taxonomy of information systems but a detailed decision about integration possibilities will follow soon. Therefore the process of the definition of a taxonomy / ontology to classify information systems in the domain of PPDR is ongoing.

SecInCoRe research is based on the activities of WP3 regarding the identification of functionality and distinguishing characteristics of information systems. It will complete the taxonomy of information systems. The work of WP3 explicated the structure of information systems according to various identified relevant metrics. The taxonomies below structure Information Systems on the one hand regarding functionalities in the first taxonomy and on the other hand in mobility (see Figure 12). Hence the taxonomy artefact “Information System” includes several sub-taxonomies which are connected based on the scheme of Figure 11 which was elaborated by the analysis of nearly 100 information systems in the PPDR domain. To elaborate the scheme, a semi-automatic approach was chosen (see D3.3) also taking the methodology described in this deliverable regarding conducting a new taxonomy into account.

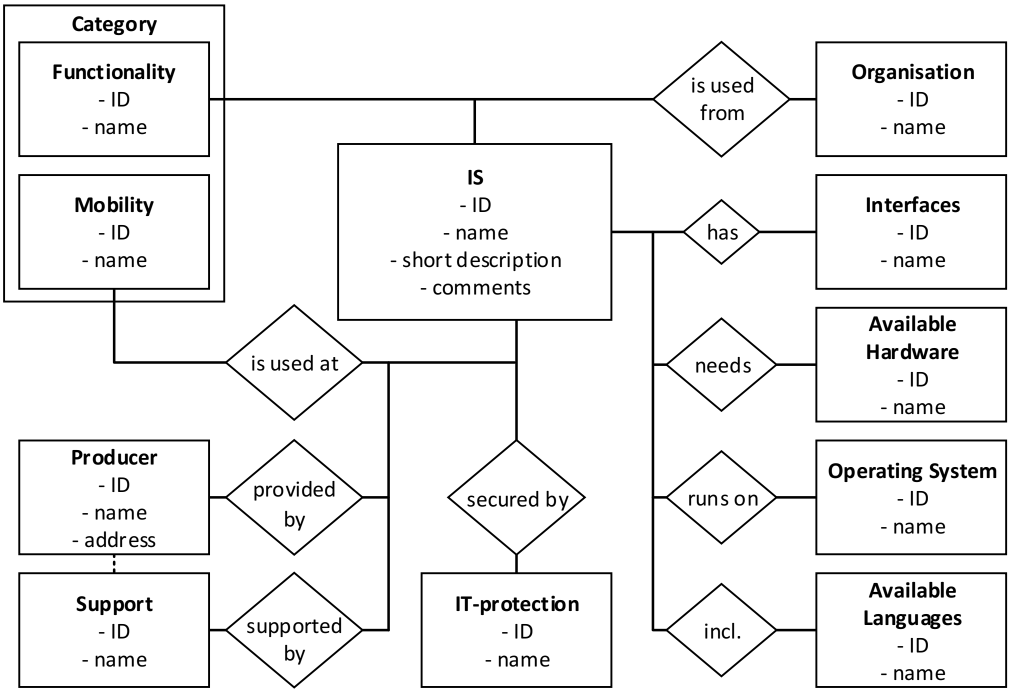


Figure 11 Structure scheme for information systems Source: [D3.3]

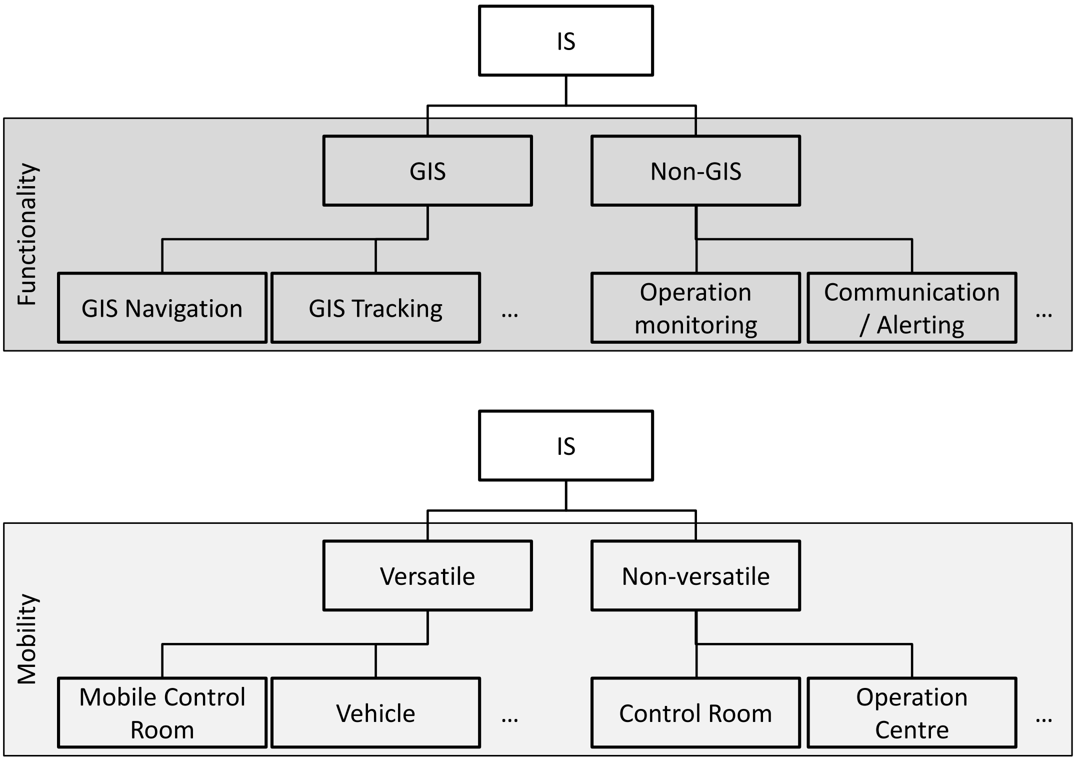


Figure 12 Two exemplary taxonomies for structuring information systems (IS)

Each metric identified in Figure 11 will be split up into small taxonomies based on SecInCoRe research or the use of existing sematic approaches.

I.e. in order to provide a taxonomy regarding the producer of information systems in the PPDR domain the work from EENA and BUCH will be the bases. Each category identified in the scheme mentioned will need the integration of other sources.

2.5.3 Taxonomy of Datasets

The taxonomy of data sets will be based on the vocabulary of the Tactical Situation Object (TSO). TSO is described in a twofold way:

1) the structure was defined in CWA-Part 1 "Disaster and emergency management - Shared situation awareness - Message structure" and
2) later on items considering end-user concepts identified, such as the type of the environment where the incident occurs were listed in CWA-Part 2 “Disaster and emergency management - Shared situation awareness - Codes for the message structure”. This is used for describing SecInCoRe data sets.

The approach of [CWA09] describes with the TSO an “information structure to record a view of a situation as seen by a particular observer at a particular time” [CWA09]. It is used for information exchange and a providing a common view of the situation, i.e. nearly 50 items are defined for describing the weather situation regarding an actual incident. The items are “expressed as a hierarchical structure subdivided into code elements. The code elements are separated by a slash” [CWA09]. Hereafter an example of the structure is given by [CWA09]:

MAT/VEH/ROADVE/FRFGTN/FRF

- MAT: material
    - /VEH: vehicle
        - /ROADVE: road vehicle
            - /FRFGTN: fire appliance
                - /FRF: fire engine truck

In the following Figure the document object model of TSO is illustrated and also shows the relations between describing an information exchange format and deriving a taxonomy.

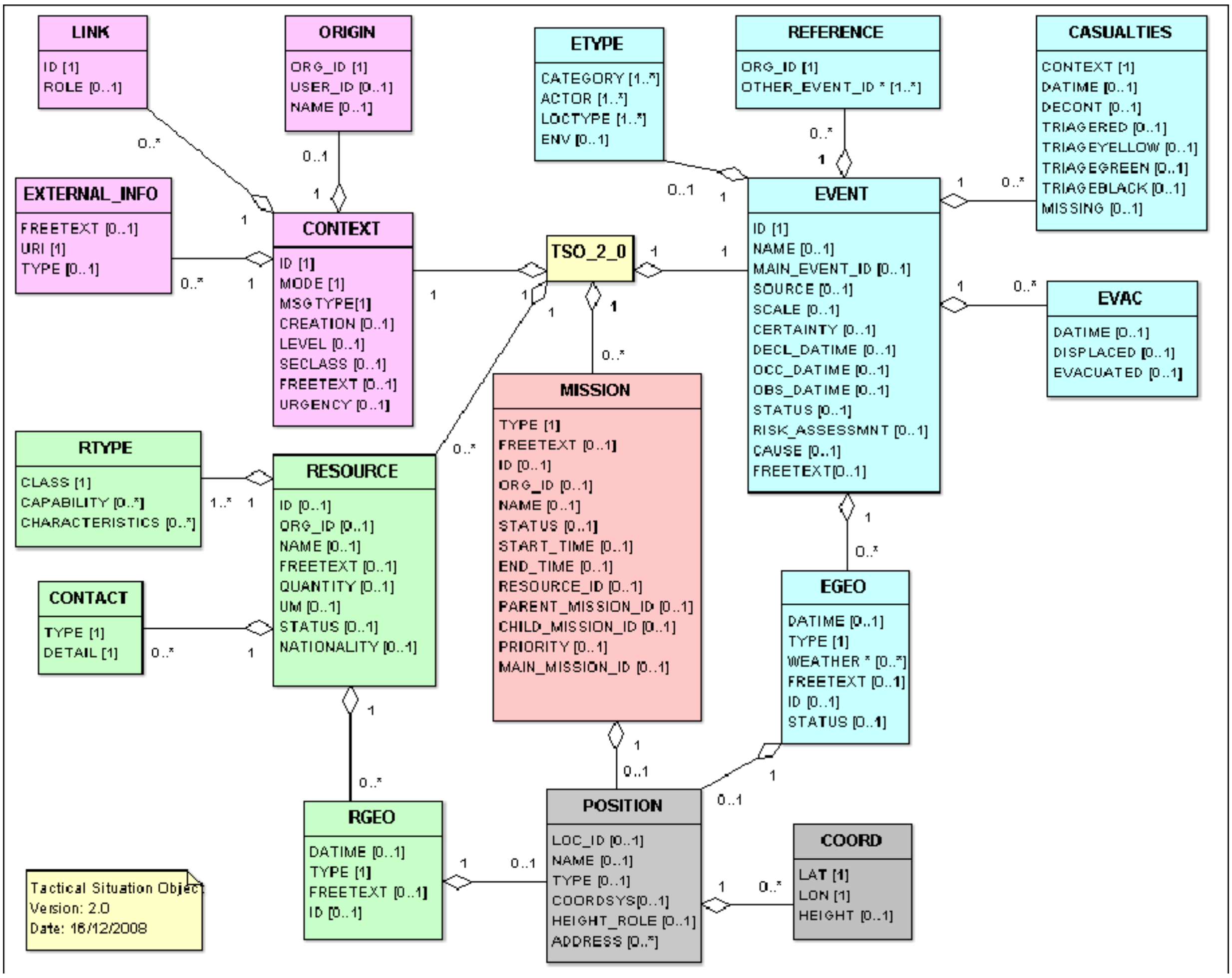


Figure 6 TSO document object model [CWA09]

TSO does not cover all aspects which have to be taken into account for the description of data sets. An extension providing a structure for lessons learned is necessary to consider advisors' and end-user feedback in several workshops. Moreover, a general classification of information is needed to be aware of new information and data. Here the integration of the Dublin Core could be an added value to TSO, by integration of a meta data classification scheme A diversification in relation to social media is possible.

The process of building the data sets taxonomy and ontology is ongoing and will be updated in the deliverable D4.4.

2.5.4 Taxonomy of ELSI

Concerning the ethical, legal and social issues in networked collaboration and information exchange in PPDR and risk governance, no sufficient semantic approach was found. Therefore a new taxonomy is being developed using the before mentioned methodology (see 0) based on the SecInCoRe ELSI guidelines (see http://185.12.5.114/elsi/elsi-guidelines-prototype) and other research (see D2.2, D2.3, D2.4). The following Figure demonstrate the flow of work to identify relevant artefacts to be integrated in the ELSI taxonomy.

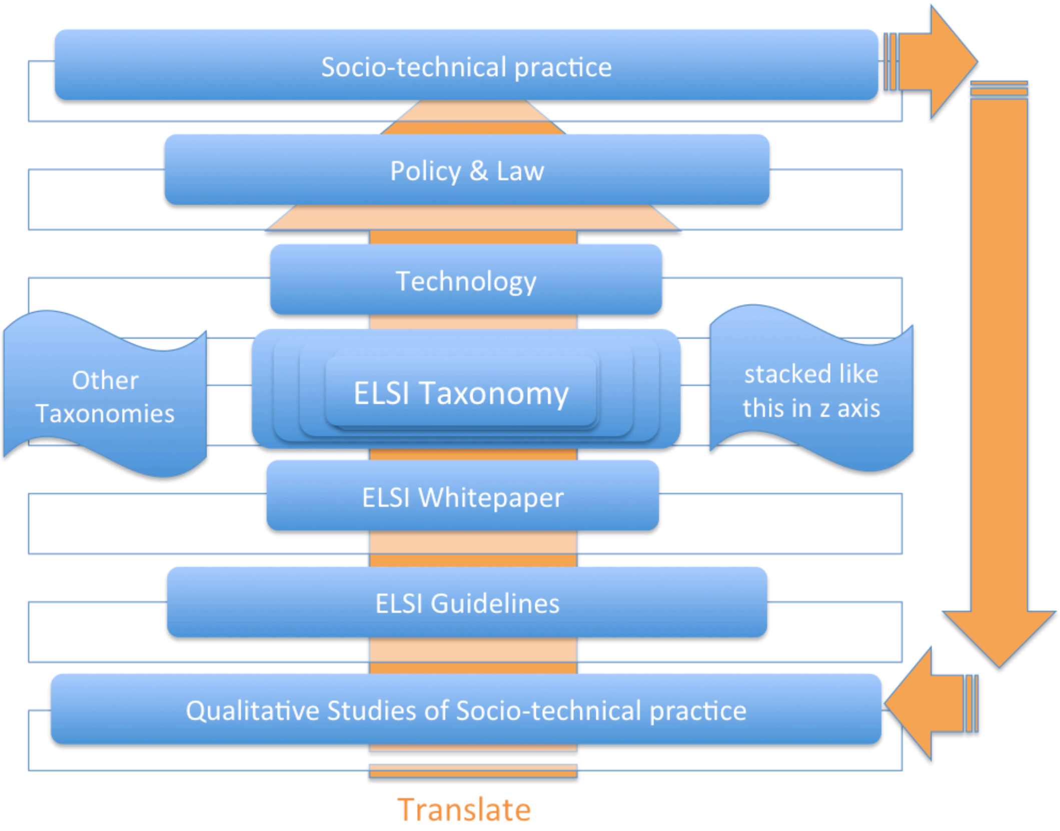


Figure 13 Context and flow of actions to identify relevant ELSI

The ELSI Taxonomy is nested within the other taxonomies (on processes, data sets, information systems). Like all taxonomies it is also nested within practice. It is an abstraction from qualitative studies of ELSI arising in socio-technical practice in risk governance, which are explored and summarised with a view to guiding ethically circumspect, lawful and socially responsible technologically augmented risk governance. The research undertaken in the SecInCoRe project and in collaboration with EPISECC, SECTOR, REDIRNET and BRIDGE has resulted in ELSI Guidelines which are motivated and explained in a concise manner in an ELSI Whitepaper (forthcoming D2.7, see also Buscher et al. 2016). The ELSI taxonomy underpins technology design and its categories and relations are materialised there as well as in innovation in policy and law (see Table 3).

Moreover, a methodology for concretely deriving the taxonomy was conducted based on the translation process (see Figure 13), which provides a twofold approach.

1) In a first step defining relevant classes and sub classes of the taxonomy in an iterative way
2) Describing relations between identified classes

The approach is illustrated in the following Figure.

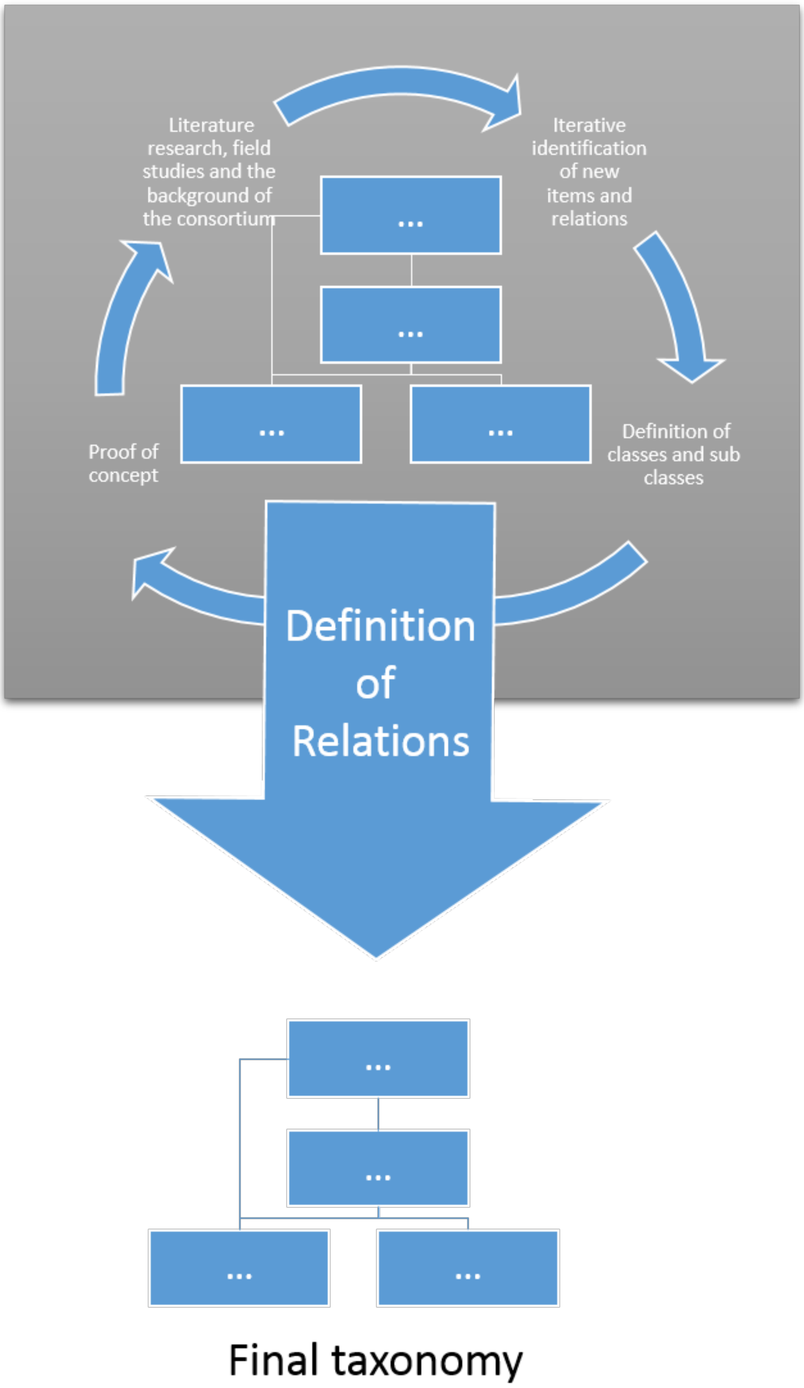

Literature research, field studies and the background of the consortium
Iterative identification of new items and relations
...
...
...
...
Proof of concept
Definition of classes and sub classes
Definition of Relations
...
...
...
...
Final taxonomy

Figure 14 Process of elaborating the Taxonomy of ELSI

In the development different aspects influence the structuring process of all relevant ELSI entries.

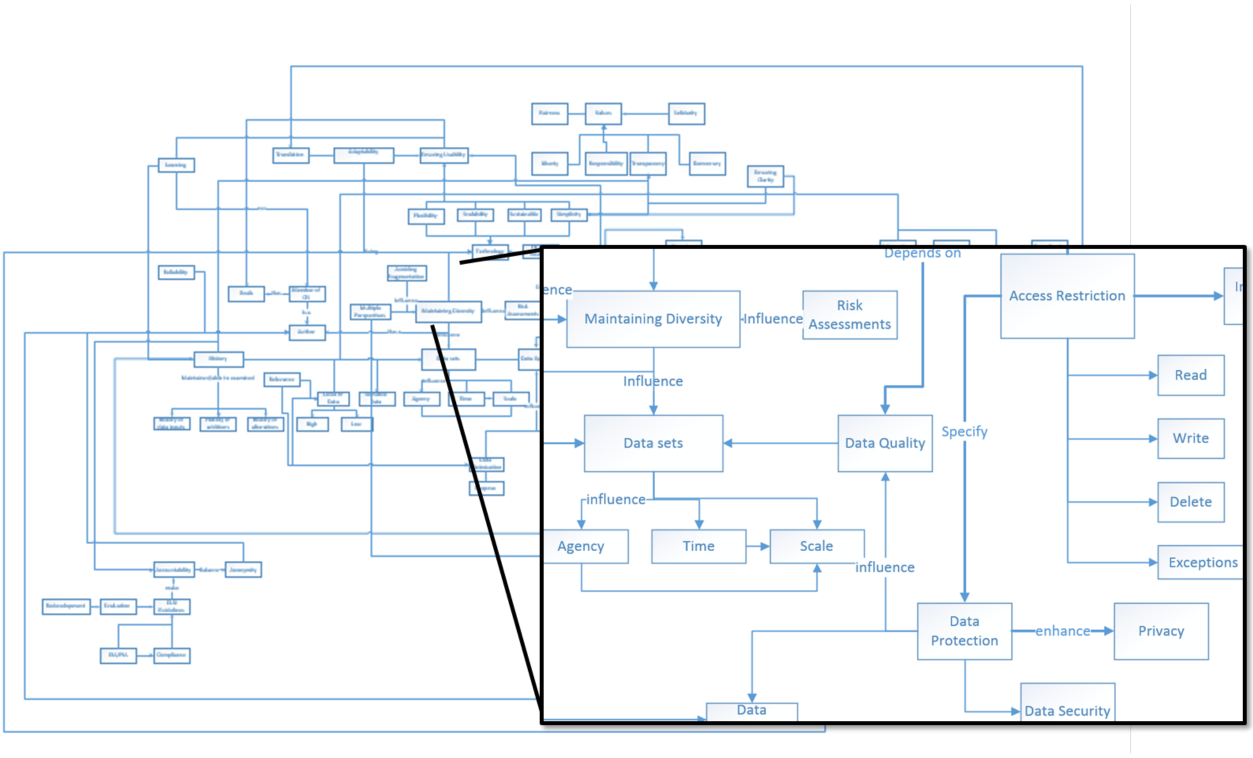


Figure 15 First draft of class definition

A first draft of the resulting taxonomy is shown in the Figure above, just to give an overview about early work. While proofing the items and also relations, the structure is growing and continuing to become a more adequate and useful formulation of values, rights and virtues as well as regulatory and legal aspects. This ‘capture’ recognises that these items and relations are experiencedin socio-technical practice. These practices are changing and this requires an ongoing cycle of studies, adaptation and experimentation.

The following Figures show the current status of the ELSI taxonomyof SecInCoRe. In the high level structure a cross connection between User / Design Goals, User / Design Practices, System Configuration and Governance was identified.

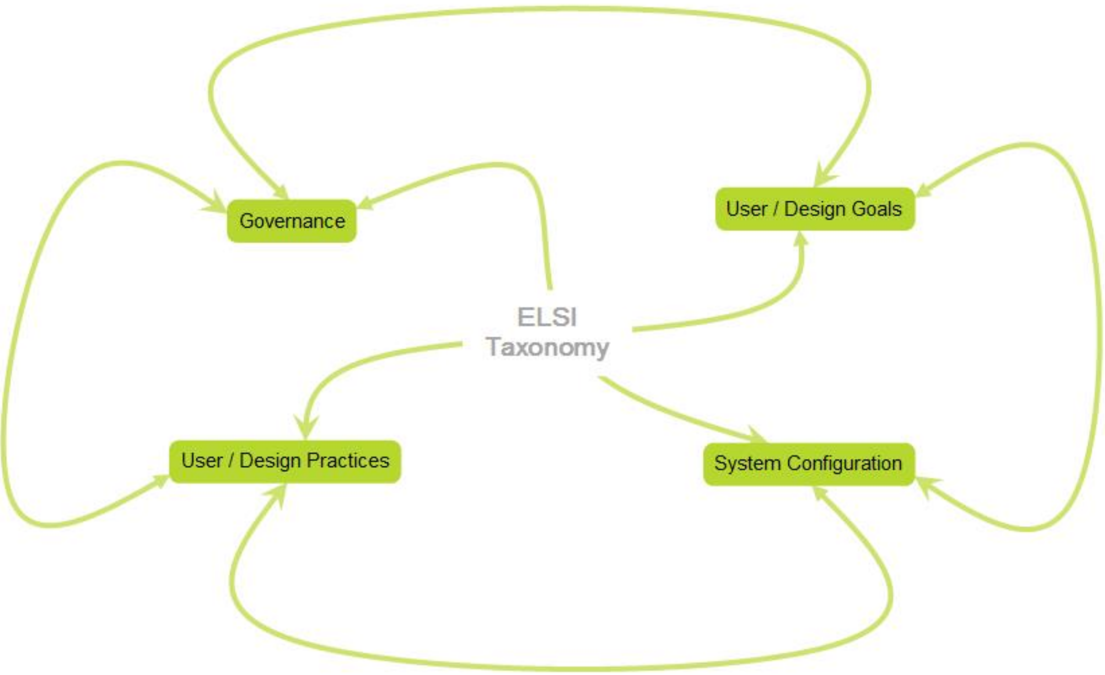


Figure 16 High level structure of the ELSI taxonomy

Based on this structure the taxonomy will be detailed in a continuing process of negotiation, experimentation and formative evaluation. The current status is presented in Figure 17The taxonomy part regarding Governance covers basic categories including values, laws and social aspects.

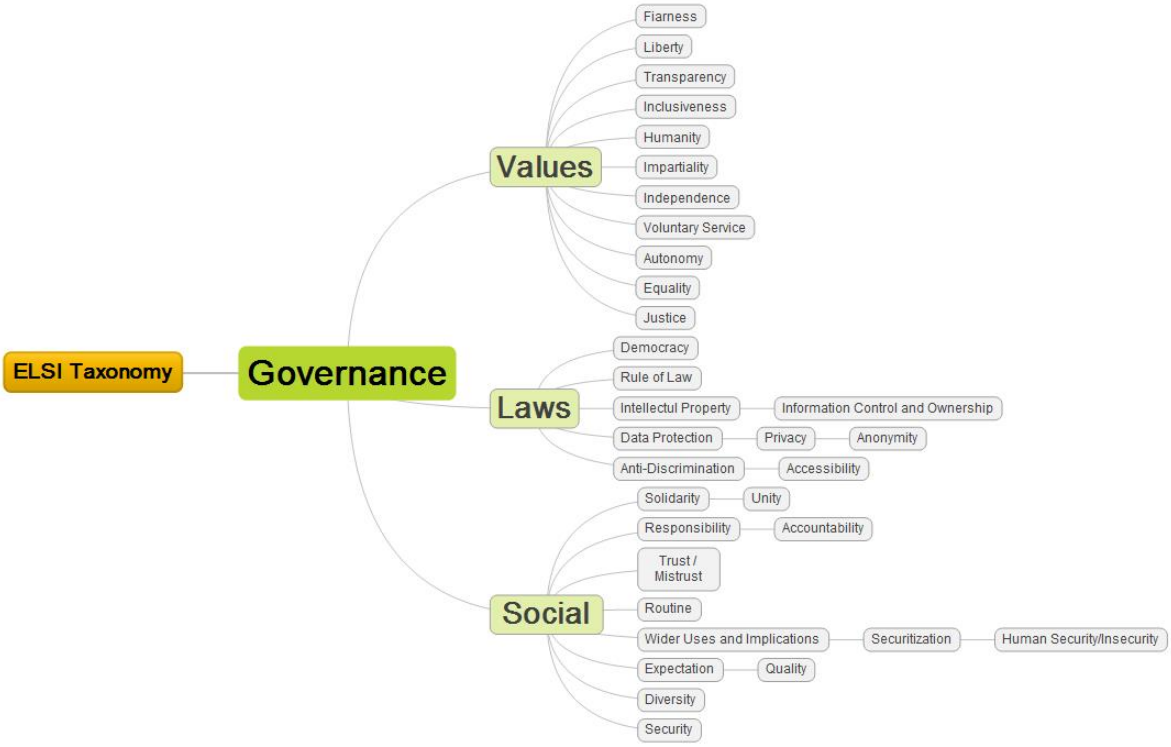


Figure 17 Elaboration of ELSI Taxonomy regarding Governance

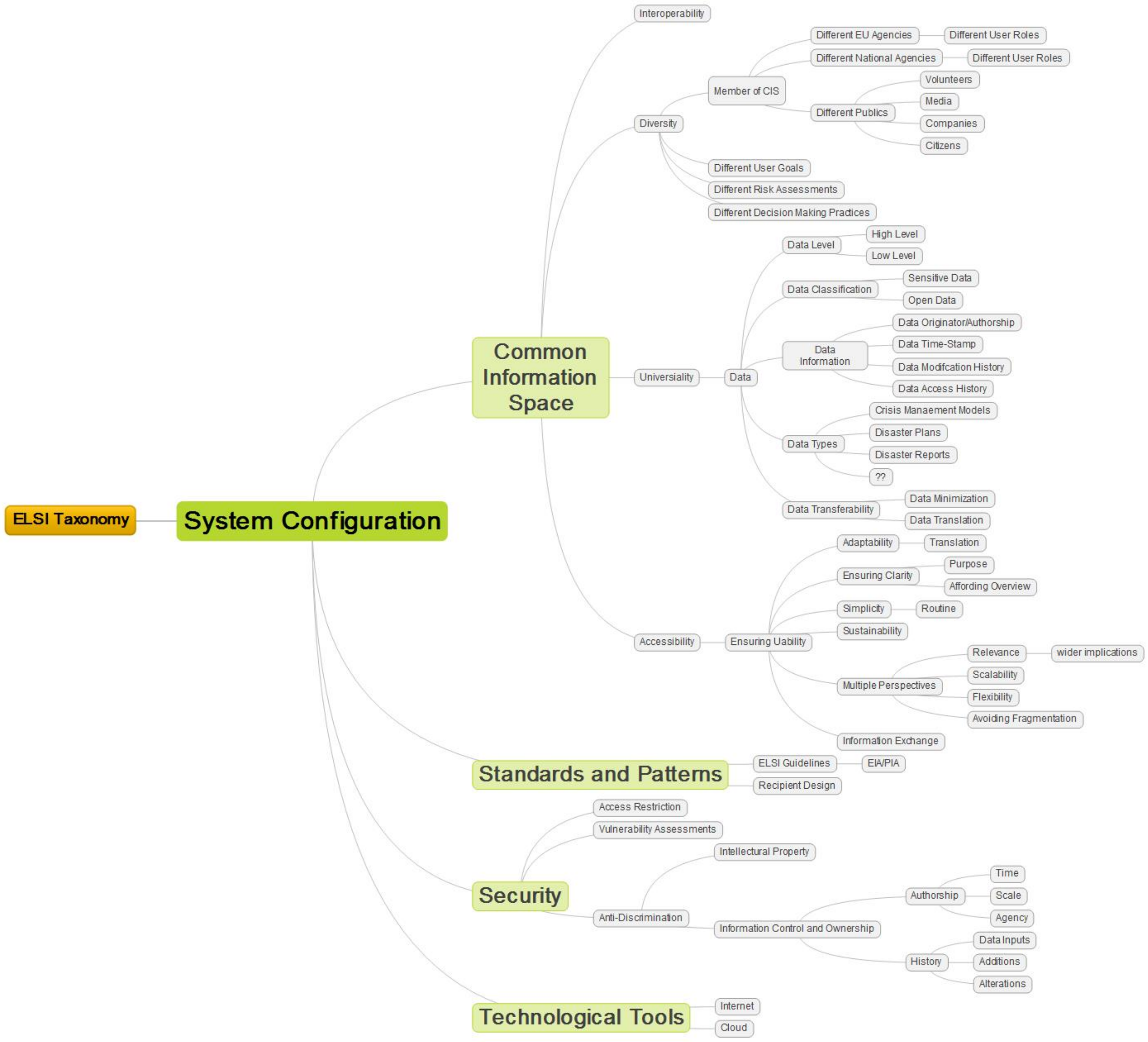


Figure 18 Elaboration of ELSI Taxonomy regarding System Configuration

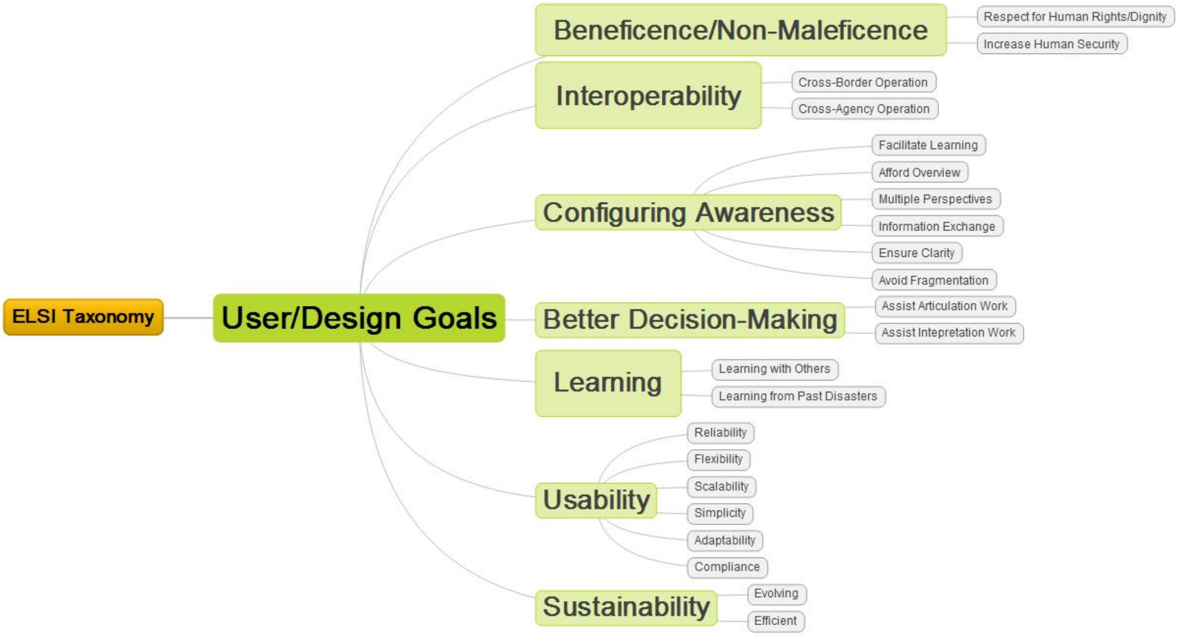


Figure 19 Elaboration of ELSI Taxonomy regarding User / Design Goals

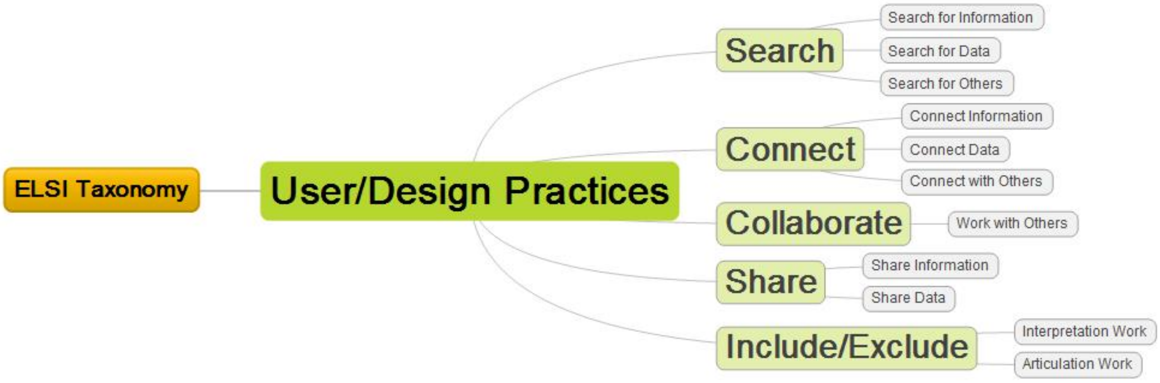


Figure 20 Elaboration of ELSI Taxonomy regarding User / Design Practices

2.6 Taxonomy conclusion and next steps

To sum up, the SecInCoRe taxonomy will consist of four single semantic approaches which are merged at least conceptually. At the moment, TSO vocabulary is chosen to represent the datasets. The other taxonomies processes, information systems and ELSI are under development. Once the single taxonomies are available in a first version, they will be combined either on taxonomy or on ontology level.

3 Network Enabled Communication system concept

3.1 Introduction on interoperability/cross-border communications

Interoperability and therefore cross-border communications between Public Safety organisations in the European countries have so far been very limited mainly due to incompatible communication systems in the countries. This has limited other countries' Public Safety forces to enter into neighbouring countries and gain access to neighbouring countries internal communication systems for Public Safety in order to collaborate and being part of the same CIS.

In addition, the complexities of the relevant legal framework and lack of common operational procedures have made cooperation between countries' Public Safety forces difficult and not offered the right support to obtain maximum results from operational cooperation between Public Safety forces in cross-border activities.

However, the subject Public Safety Cross-border communication and cooperation has been on the agenda throughout the world for years and the need is increasing, e.g. due to the following factors:

- Cross-border support during firefighting;
- Cross-border support during natural disasters and accidents close to a border or in coastal areas between countries;
- Cross-border support during / after terror attacks;
- International crime – drugs, human trafficking, smuggling etc.;
- Police pursuit of criminals cross-border(s);
- Transport of patients to hospitals between countries;
- VIP protection (e.g. EU ministry top).

One of the SecInCoRe project objectives is to design a system concept in due consideration to a universal architecture and regarding the stakeholder needs. Moreover, to ensure a high end-user acceptance of the project results, the services are developed in close alignment with specific end-user requirements.

Then the concept is transferred to a technical specification of a federated and seamless communication system concept incl. knowledge base and services utilising existing infrastructure.

3.2 NEC System concept

3.2.1 Overview

This section starts by describing the general requirements for meeting interoperability and cross-border communications and also reminds the legacy PMR services architecture is described.

Then two following system architecture options are described in details:

- Option 1 : Interoperability with PMR services based on an extension of the legacy PMR services
- Option 2 : Interoperability with PMR services based on 3GPP standard solution

At the end of section, a conclusion sums up and explains the pro and cons of the two options.

Other interoperability options exist.

The FP7 ISITEP (Inter System Interoperability for TEtra-tetraPol networks) project interconnects forces beyond national borders. For more details see : http://isitep.eu/. However, interconnections are only related to Tetra and TetraPol networks, currently deployed, but does not address evolution to broadband networks.

The FP7 SALUS (Security And InteroperabiLity in Next Generation PPDR CommUnication InfrastructureS) project leverages the control room interfaces to support different technology and provide an evolution to broadband data. For more details see: https://www.sec-salus.eu/. However, in order to address borders communications, it requires an agreement between the related countries in order to setup such control rooms. So far, this is not the envisaged path in Europe.

The FP7-HIT-GATE project developed a solution to communications interoperability between First-Responder networks, including those involving more than one nation. More specifically, an IMS platform has been created that links differnet TEtra, tetraPol networks, even with GSM/3G mobile phones. For more details see: http://www.hit-gate.eu. However, it has not been adopted by any county in the EU.

Main focus of this section is on the Network enabled Communication level (NEC) and services it provides including security. There is no detailed focus on cloud services since there is a dedicated section later in this document.

3.2.2 General requirements for meeting interoperability and cross-border communication

Harmonised conditions for mobile services or sectorial applications such as BroadBand Public Protection and Disaster Relief (BB-PPDR) is established when Mobile Terminals or UE (User Equipment) seamlessly maintain its connection when moving into a visited network (e.g. in other country), what is also called “roaming”.

To obtain this technically at least four aspects have to be fulfilled:

- Spectrum requirements have to be aligned so that radio terminals from the European country’s public safety radio networks are able to operate under other countries radio network coverage. Multi-band user equipment has to be used, interoperability can be achieved in case the bands used in each country are supported by the multi-band equipment even when countries choose different bands;

- Standardised network and radio terminal technologies supported by all user equipment without proprietary modifications by different vendors;
- Appropriate roaming agreements and technical interconnections between the connected networks have to be in place,
- The networks and radio terminals have to have (the standardised) appropriate roaming capability implemented.

BB-PPDR services could be provided by means of one of the following infrastructure implementation models:

1. Dedicated network infrastructure for BB-PPDR;

2. Commercial network(s) infrastructure providing broadband services to PPDR users;

3. Hybrid solutions with partly dedicated and partly commercial network infrastructure.

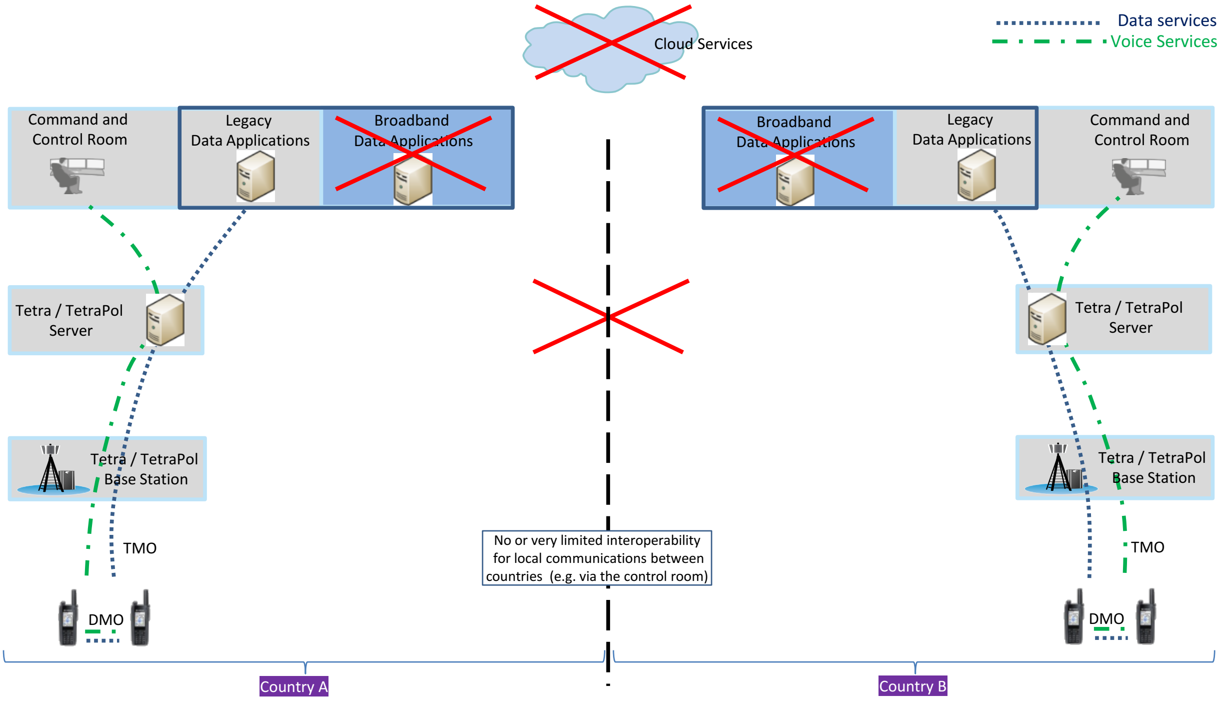
Fully commercial network implementation options will not require any PPDR specific spectrum, but spectrum for the dedicated network option and many of the hybrid network models would be required on a national level.

3.2.3 Legacy PMR services architecture

Public Safety networks based on TETRA or TETRAPOL technology have substantially improved the efficiency and mission safety of public safety operations, bringing a huge leap in security, as well as robustness of systems and richness of features.

Today, there are more than a thousand TETRA and TETRAPOL networks in over 120 countries, including public safety networks and those in industrial areas. Many users of these networks would welcome the introduction of new data applications and smart devices.

Although today’s dedicated digital networks can deliver extremely secure and reliable data services, the narrowband technology used in public safety networks does not have the capacity for new bandwidth-hungry apps.


Cloud Services
Data services
Voice Services
Command and Control Room
Legacy Data Applications
Broadband Data Applications
Tetra / TetraPol Server
Tetra / TetraPol Base Station
TMO
DMO
No or very limited interoperability for local communications between countries (e.g. via the control room)
Country A
Country B

A PMR network is typically composed of:

- Tetra/TetraPol based stations which provide radio coverage
- Tetra/TetraPol server mainly providing PTT services
- Legacy Data Applications (narrow band data applications e.g. database queries, automatic vehicle location etc)
- Command and Control Rooms systems (e.g. dispatchers, call taking positions)
- Tetra/TetraPol devices providing either TMO (Trunked Mode Operation) or DMO (Direct Mode Operation) PMR services.

As already mentioned, interoperability with other PMR systems is so far very limited mainly due to incompatible communication systems in the countries (e.g. between country A and country B in the figure).

Last point, the narrowband technology used in public safety networks does neither have the capacity to support broadband data applications nor cloud services (which host mainly broadband data applications).

3.2.4 Interoperability with PMR services based on an extension of the legacy PMR services (option 1)

3.2.4.1 Hybrid model complements public safety networks with mobile broadband

For many public safety authorities, empowering their operations with mobile broadband that is secure and matched to their needs is an appealing prospect. New capabilities enabled by fast access to data in the field promise innovative ways to maintain public safety and security, as well as helping organisations to improve the efficiency of their operations.

Although today's dedicated digital networks can deliver extremely secure and reliable data services, the narrowband technology used in public safety networks does not have the capacity for new bandwidth-hungry apps. The key is to get more data capacity for mobile applications, such as video, database queries and pictures, yet without losing the vital aspects of reliable voice, security and interoperability.

Mobile broadband will at first be used for data applications, with mission-critical voice communications continuing to be supported on the digital narrowband networks.

This is because today's commercial broadband networks simply do not have the standardization, group communication and other features needed. They cannot replace narrowband networks in mission-critical communications. Their availability and resilience need to be improved. In addition, it makes little sense to replace an existing well-serving public safety network with an alternative that does not meet the critical requirements.

An important question is coverage. To be used for mission-critical voice, broadband networks must provide comparable coverage to that of the existing public safety networks. In contrast to commercial networks, which measure coverage by the numbers of people they can reach, in mission critical communications the measure is the share of land area covered by the net-work. This is much more expensive to build up.

Although work is under way to make mission-critical voice available on broadband, standards-based products are still some years away. TETRA and TETRAPOL will be used well into and most probably beyond the next decade.

Hybrid model complements public safety networks with mobile broadband

Yet there are some options for public safety organisations seeking to implement mobile broadband services. One method is to use the services of regular mobile operators. However, this is not totally suitable because the standard mobile data services offered by commercial operators do not meet rigid mission-critical requirements. The opposite approach is to build a dedicated broadband network owned and operated by a user organisation.

Between these extremes is the Secure MVNO (Mobile Virtual Network Operator) approach, which uses the radio capacity of commercial mobile operators, while the public safety organisation remains in control of subscribers and security.

One very cost-effective approach is the hybrid network, where a public safety organisation can continue with a TETRA or TETRAPOL network for mission-critical voice and data and introduce mobile broadband services step-by-step. These services can be based on a dedicated broadband network, commercial services with Secure MVNO, or a combination of the two.

Using a hybrid network means investments can be made gradually as and when needed. Hybrid network investments add value today, but also offer long-term benefit by bridging existing narrowband networks and future solutions.

The broadband network can be developed in different ways depending on which applications are needed and the level of investment that can be supported.

One way of evolving towards broadband services is to start with a Secure MVNO service, using several mobile operators' services to achieve improved coverage and reliability. This is particularly suited to providing mobile office applications. Dedicated broadband capacity can be added as needed to improve the coverage, or when applications become more mission-critical.

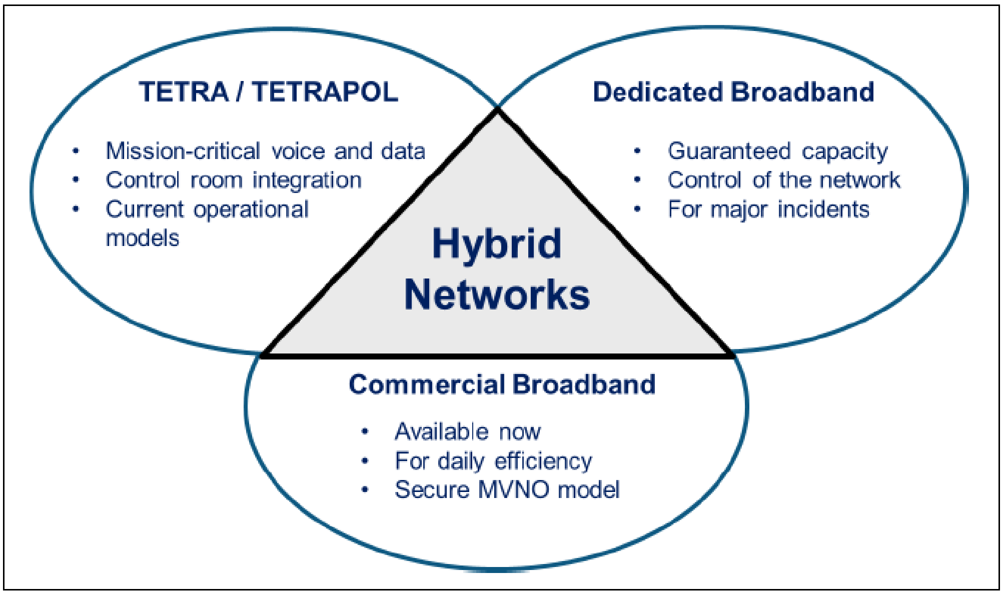


Figure 21 : Hybrid model complements public safety networks with mobile broadband

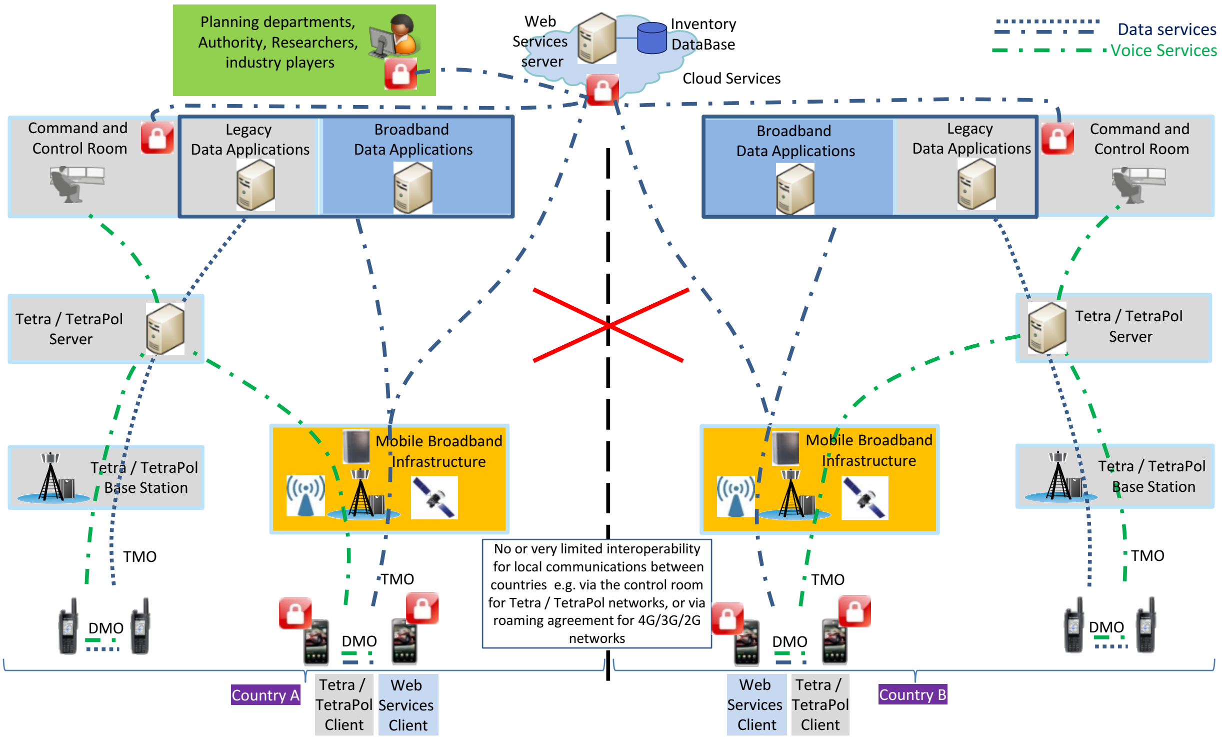
Mobile broadband for public safety is becoming a reality

Many public safety network operators in Europe are interested in adopting new data applications based on mobile broadband services. A good example is Finland's VIRVE, whose existing nationwide TETRA network will serve until 2030. A hybrid network with commercial and dedicated broadband will be used to complement existing services.

Another example of public safety operator in Europe proceeding with Secure MVNO is Astrid in Belgium. Astrid launched a service called Blue Light Mobile in 2014 for its public safety customers.

3.2.4.2 SecInCoRe System Architecture based on Option 1

The SecInCoRe system architecture is depicted here below leveraging the hybrid model which complements public safety with mobile broadband.


Planning departments, Authority, Researchers, industry players
Web Services server
Inventory DataBase
Cloud Services
Data services
Voice Services
Command and Control Room
Legacy Data Applications
Broadband Data Applications
Broadband Data Applications
Legacy Data Applications
Command and Control Room
Tetra / TetraPol Server
Tetra / TetraPol Server
Tetra / TetraPol Base Station
Mobile Broadband Infrastructure
Mobile Broadband Infrastructure
Tetra / TetraPol Base Station
TMO
TMO
TMO
TMO
No or very limited interoperability for local communications between countries e.g. via the control room for Tetra / TetraPol networks, or via roaming agreement for 4G/3G/2G networks
DMO
DMO
DMO
DMO
Country A
Tetra / TetraPol Client
Web Services Client
Web Services Client
Tetra / TetraPol Client
Country B

Mobile broadband services (orange part in the figure) could be provided by means of one of the following infrastructure implementation models:

- Dedicated network infrastructure for broadband PPDR;
- Commercial network(s) infrastructure providing broadband services to PPDR users;
- Hybrid solutions with partly dedicated and partly commercial network infrastructure.

Mobile Broadband services could rely on any IP Mobile technology such as:

- 4G (LTE), 3G, 2G
- WLAN
- Satellite

Mobile broadband services bring capacity for BB-PPDR users to access to legacy data applications but also to broadband Data applications (e.g. video, pictures, multimedia content). They also offer natively access to cloud services.

On the device side, PMR services are implemented in a client/server model leveraging the IP connectivity provided by the Mobile broadband services. Legacy PMR services are provided thanks to a Tetra / TetraPol Client and a Web services client is provided to access to data applications including those hosted by the cloud services offered by SecInCoRe. Some data applications may require a specific data application client.

Moreover, some PMR services can be also provided in DMO (Direct Mode Operation) leveraging some technologies:

- WLAN with Wifi-direct
- LTE with ProSe (started at 3GPP standardisation in R12)

In this architecture, interoperability with legacy PMR services is natively provided by the Tetra/TetraPol server which supports both the legacy Tetra/TetraPol devices and the broadband devices (e.g. smartphone).
Legacy PMR services supported by a broadband device are the same as the PMR services available on a Tetra/TetraPol device, but they could be offer in a different way.

If roaming agreement is in place between country A and country B, a BB-PPDR user from country A can access to PMR services leveraging Mobile broadband services from country B. Moreover, BB-PPDR users from country A and B could have access to the same cloud services and could therefore be able to share/exchange information.

However, since this solution relies on a proprietary implementation, interoperability with other PMR systems for local communications remains limited mainly due to communication incompatible communication systems in the countries (e.g. between country A and country B in the figure).

3.2.5 Interoperability with PMR services based on 3GPP standard solution (option 2)

3.2.5.1 Introduction

Long Term Evolution (LTE and its evolutions) is expected to be the dominant technology for mobile broadband communications for many years ahead. In order for BB-PPDR to benefit from the technical development and economies of scale from the commercial mobile broadband market, there is a common view that LTE will be the technology to meet future BB-PPDR needs. As the future evolution of mobile broadband is assumed to be based on an evolution of the current LTE technology, the adaptation of LTE for BB-PPDR services is seen as a very long-term solution.

LTE is a global mobile communications technology specified by 3GPP. 3GPP is a collaboration of several telecommunication standards bodies across the world supported by a wide range of organisations including equipment suppliers, network operators and government departments. In Europe, 3GPP specifications are published by European Telecommunications Standards Institute (ETSI).

The advantage to the police, fire and emergency services of having video and broadband data capabilities integrated into their communications devices is significant and widely sought around the world. European Telecommunications Standards Institute (ETSI) TETRA and Critical Communications Evolution (TCCE), OMA (Open Mobile Alliance) and TIA (Telecommunications Industry Association for P25) initiated each individually the work to create a MCPTT (Mission Critical PTT) capability based on broadband networks (namely LTE).

The industry converged in 2014 by agreeing to do a single set of work in 3GPP. It is the first Working Group to combine the expertise and influence of ETSI, OMA and 3GPP. The TCCA is represented both as a 3GPP Market Representation Partner, by its Members and by ETSI TC TCCE, which has the mandate to develop critical communications broadband standards as well as continuing the development and maintenance of TETRA standards.

3.2.5.2 Mission Critical Push-To-Talk over LTE (MCPTT) Overview

Work on Mission Critical Push-to-Talk (MCPTT) began in 2014 in 3GPP with the creation of a set of requirements by 3GPP SA1 (System Architecture working group 1) in TS (Technical Specification) 22.179. Work then expanded into 3GPP SA2 to begin to examine architectural needs.

In recognition of the importance of the work, and to manage its work load better, 3GPP decided to create a new working group, SA6, focused on Critical Applications. The work done in SA2 was transferred in January 2015 to SA6.

The goal of the MCPTT work in 3GPP Rel-13 is to create specifications for mission critical voice over LTE.

Support for:

- video services called MCVideo (Mission Critical Video) and
- data services called MCData (Mission Critical Data)

for public safety users are in the scope of the 3GPP Rel-14 work.

MCPTT group calls take advantage of both unicast and broadcast (eMBMS) bearers to distribute voice content to members of the group.

Integration of MCPTT over LTE with existing Land Mobile Radio (LMR) systems such as P25 and Terrestrial Trunked Radio (TETRA) will be required to provide a migration path to countries and jurisdictions from LMR systems to LTE-based public safety communications. The work will necessarily follow the work in 3GPP but it has been agreed that it will be out of the Rel-13 scope.

An aspect of MCPTT is the use of 3GPP Proximity Services (ProSe) defined by 3GPP in Rel-12 to allow two public safety devices to communicate directly with each other both in and out of regular LTE network coverage. The MCPTT application that operates over the lower layer ProSe capabilities is called MCPTT Off-Network vs MCPTT on-network application when leveraging the network infrastructure.

The MCPTT capabilities, based on the requirements in 3GPP TS 22.179, include group calls, person-to-person calls, prioritization of calls and of individuals, group management, user management, configuration management, security, operation in relay-to-network mode, operation in off-network mode and a number of other related features.

The work on group calls includes the basic abilities to push-to-talk and to have the voice content delivered to other members of the group, and includes special prioritization of calls to handle, for example, situations where public safety first responders encounter an emergency situation and push the “red button” on their device. Distribution of group call content makes use of normal unicast bearers to individual devices, and also makes use of eMBMS to deliver the same group content to multiple group members in one area.

Priority management in MCPTT includes recognition that individuals, particularly in public safety first responder situations, will have different roles and will need different abilities to access and even pre-empt other individuals. For example, the fire chief will need a higher priority than other fire personnel in order to be able to give the orders necessary to efficiently and safely contain and put out a fire. In addition, the need exists for individuals, regardless of the priority of their role, to be able to obtain immediate priority when an emergency situation arises. In this case, depending on system policy and configuration, the priority given by the system may allow the individual fireman to override the fire chief in order to alert others of a life threatening situation.

Group management involves the ability of the administrator to pre-configure groups of individuals for the purpose of group communications. For example, all police personnel in the North Police Station may be automatically included in a group “North Police”. Groups can also be formed dynamically by a dispatcher or by individuals to meet the needs of the situations encountered.

3GPP has completed the application level architecture for MCPTT in Rel-13 in march 2016. However, some work still remain to be addressed or improved and therefore the 3GPP will continue the discussion on MCPTT definition in Rel-14.

3.2.5.3 3GPP MCPTT specifications

SPECIFICATIONS

3GPP follows a three-stage methodology as defined in ITU-T Recommendation I.130:

- Stage 1 specifications define the service requirements from the user point of view

- Stage 2 specifications define an architecture to support the service requirements
- Stage 3 specifications define an implementation of the architecture by specifying protocols in details.

MCPTT specifications produced by the 3GPP for Rel-13 are listed here below:

N°	Title	Reference
R1	MCPTT over LTE (Stage 1)	22.179
R2	Functional Architecture and information flows to support MCPTT (Stage2)	23.179
R3	MCPTT call control protocol specification (Stage 3)	24.379
R4	MCPTT media plane control protocol specification (Stage 3)	24.380
R5	MCPTT group management protocol specification (Stage 3)	24.381
R6	MCPTT identity management protocol specification (Stage 3)	24.382
R7	MCPTT Management Object (MO) (Stage 3)	24.383
R8	MCPTT configuration management protocol specification (Stage 3)	24.384
R9	Codecs and Media Handling	26.179
R10	Security of MCPTT	33.179
R11	Study on application architecture to support Mission Critical Push To Talk over LTE (MCPTT) services	23.779
R12	Mission Critical Push To Talk (MCPTT); Media, codecs and Multimedia Broadcast/Multicast Service (MBMS) enhancements for MCPTT over LTE	26.879

The relationship between these specifications is the following:

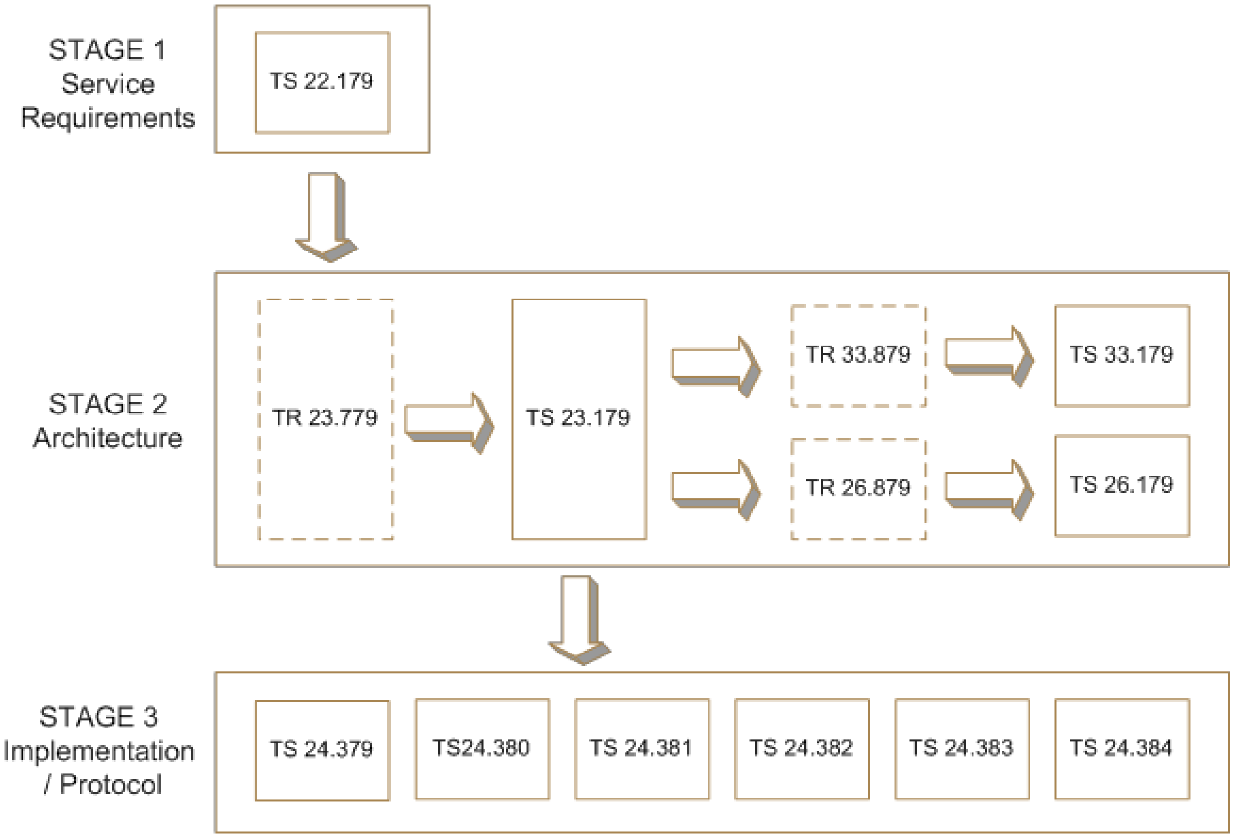


Figure 22 : 3GPP MCPTT documentation relationship

3.2.5.4 MCPTT functional models

3GPP TS 23.179 specifies the functional architecture, procedures and information flows needed to support the mission critical push to talk (MCPTT) service including the common services core architecture for identity management, group management, and configuration management required to support the MCPTT voice service. Support for both MCPTT group calls and MCPTT private calls operating in on-network and off-network modes of operation is specified.

The corresponding service requirements are defined in 3GPP TS 22.179.

The On-Network MCPTT functional model for the application plane in TS 23.179 is the following:

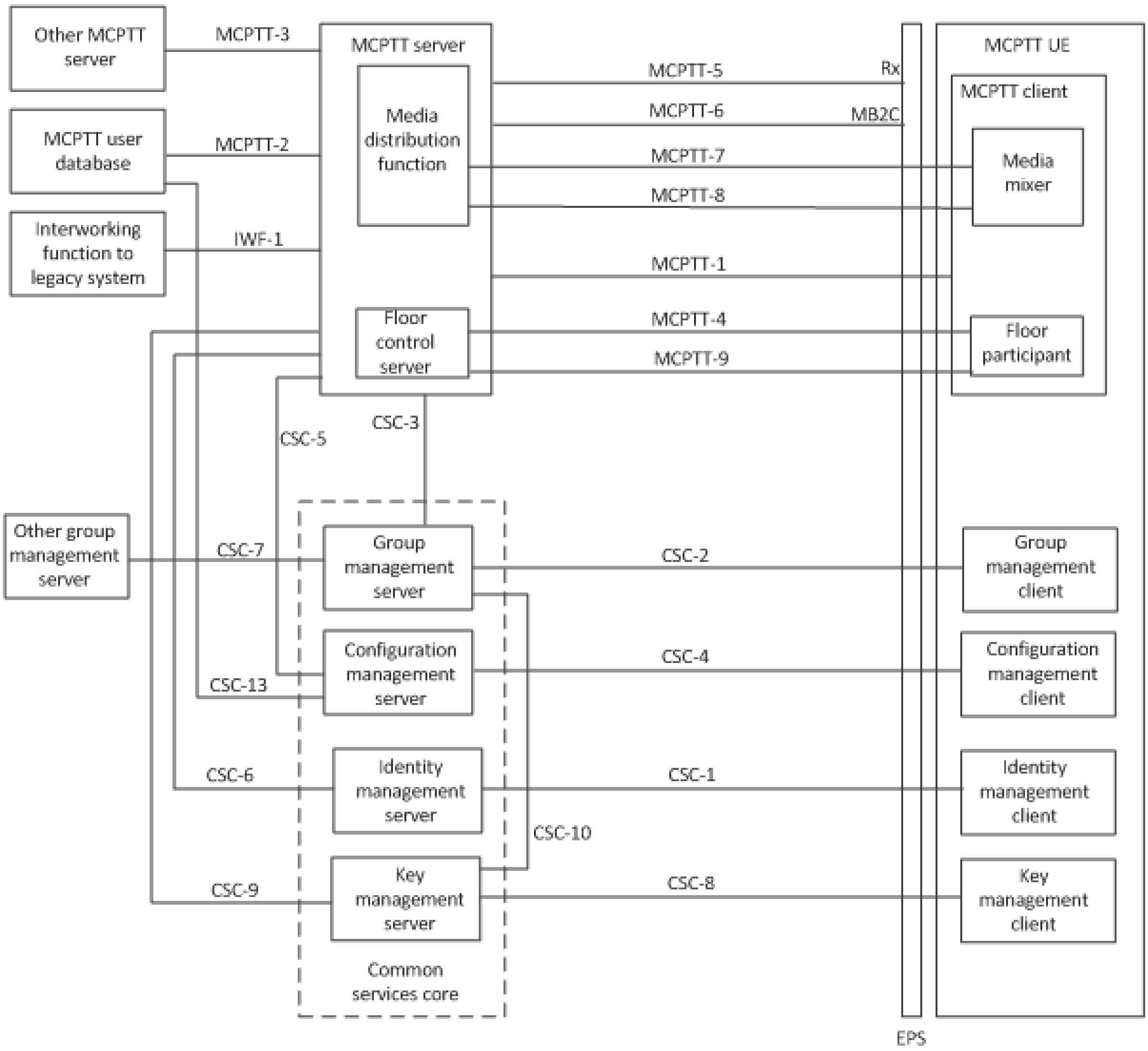
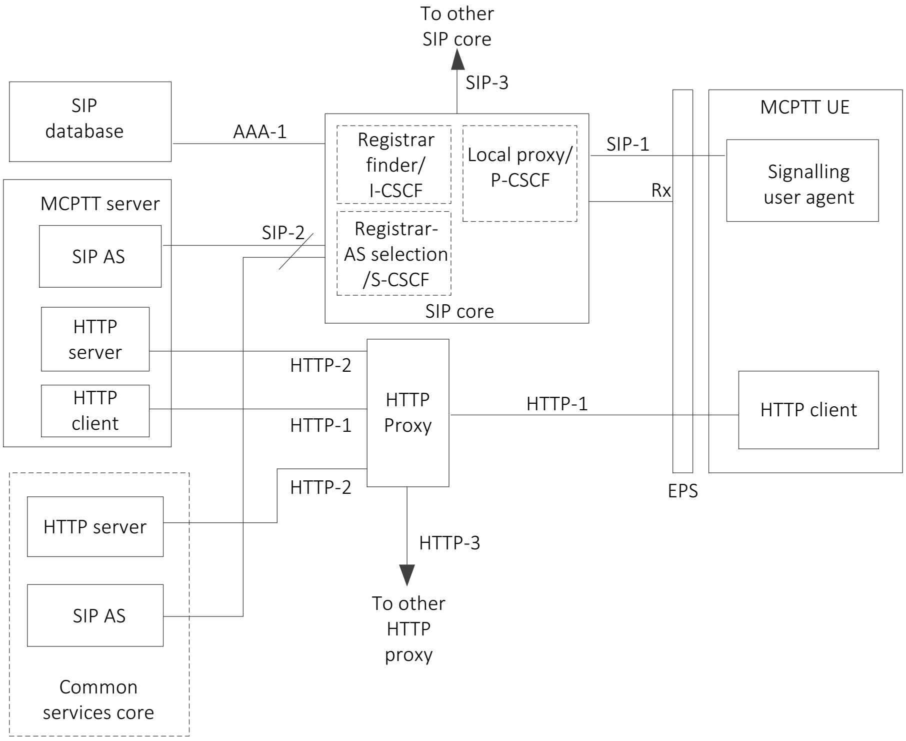


Figure 23 : On Network MCPTT Functional Model for Application Plane (from 3GPP TS 23.179)

A detailed description of this MCPTT functional model could be found in 3GPP TS 23.179.

The On-Network functional model, with reference points, for signalling control plane specified by the 3GPP in TS 23.179 is the following:



For details on this functional model, see TS 23.179.

The MCPTT functional model leverages aspects of:

- the SIP Core/ IMS architecture defined in 3GPP TS 23.228,
- the Group Communication System Enablers for LTE (GCSE_LTE) architecture defined in 3GPP TS 23.468
    - MCPTT group calls take advantage of both unicast and broadcast (eMBMS) bearers to distribute voice content to members of the group.
    - eMBMS access was made available in Rel-12 to applications by the creation of the MB2 interface. This work was primarily done to support MCPTT, but also, supports any application implementing the MB2 interface
- the Proximity-based Services (ProSe) architecture defined in 3GPP TS 23.303, for MCPTT Off-Network application (functional model not described here above).
    - In Rel-13, further enhancements to Proximity-based Services (ProSe) have been added in order to support the Public Safety and non-Public Safety use cases that could not be completed in Rel-12 and to fulfill the requirements of Mission Critical Push to Talk (MCPTT).

The MCPTT UE primarily obtains access to the MCPTT service via E-UTRAN, using the EPS architecture defined in 3GPP TS 23.401.

Specific MCPTT functions such as dispatch and administrative functions can be supported, using either MCPTT UEs in E-UTRAN or using MCPTT UEs via non-3GPP access networks. Moreover, dispatch consoles and devices used by MCPTT service administrators are considered MCPTT UEs in the MCPTT architecture.

MCPTT UEs that use non-3GPP access can only support a subset of the functionality specified in this specification that is supported by the non-3GPP access network.

3.2.5.5 MCData and MCVideo services

Extension of the mission critical communications services is part of 3GPP Rel-14, and SA1 requirements work has already begun and is planned to be approved in June 2016. In particular, extension to other media types (e.g., video and data) is important to public safety operations.

Two dedicated Work Items have been created Mission Critical Video (MCVideo) and Mission Critical Data (MCData).

MCData covers services such as messaging and file transfer.

MCVideo covers services such as Real time video ("see what I see") and video streaming.

It is anticipated that MCData and MCVideo will leverage some significant blocks of the MCPTT functional model, such as the Common Services Core (Identity management, configuration management, group management), but also a significant part of the participating role of the MCPTT server. Therefore, 3GPP Rel-14 is also revisiting the content of the MCPTT definition done in Rel-13 in order to separate:

- the common core services called MCCore (Mission Critical Core) and
- MCPTT services only

3.2.5.6 3GPP MCPTT Interoperability for SecInCoRe

In the SecInCore context, the interoperability is a key point.
In the On-network MCPTT functional model for application plane specified in 3GPP TS 23.179 (see it in the previous section), the service interoperability between organisations is supported via the following reference points:

- MCPTT-3: Reference point between an MCPTT server and MCPTT server
- CSC-7: reference point group management server and group management server
- IWK-1: Reference point between the MCPTT server and interworking function to legacy systems. It is not specified in the 3GPP R13 specification.

MCPTT-3 and CSC-7 are the reference points which are used for interoperability between two MCPTT systems.

These reference points are defined by the 3GPP.

MCPTT-3:

The MCPTT-3 reference point, which exists between the MCPTT server and the MCPTT server for MCPTT application signalling for establishing MCPTT sessions, shall use the SIP-2 reference point for transport and routing of signalling. If each MCPTT server is served by a different SIP core then the MCPTT-3 reference point shall also use the SIP-3 reference point for transport and routing of signalling. Floor control signalling and media are also transferred using the MCPTT-3 reference point.

CSC-7:

The CSC-7 reference point, which exists between group management servers, allows group management servers to handle group management related signalling in multiple MCPTT systems environment. The CSC-7 reference point shall use the HTTP-2, HTTP-3 and HTTP-4 reference points for transport and routing of non-subscription/notification related signalling. The CSC-7 reference point shall use SIP-2 and SIP-3 reference points for transport and routing of subscription/notification related signalling.

IWF-1:

The IWF-1 reference point between the MCPTT server and the interworking function to legacy systems is not specified in the 3GPP R13 specification.

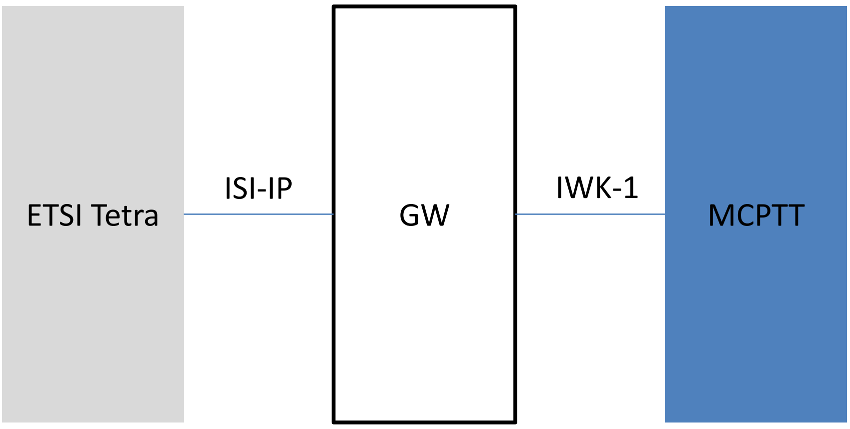
Note: a subset of the functionality provided by the existing MCPTT reference points could be used to interconnect with legacy systems.

At the time this report is written, it is a hot topic both at the ETSI and ATIS in order to provide contributions to 3GPP in April 2016.

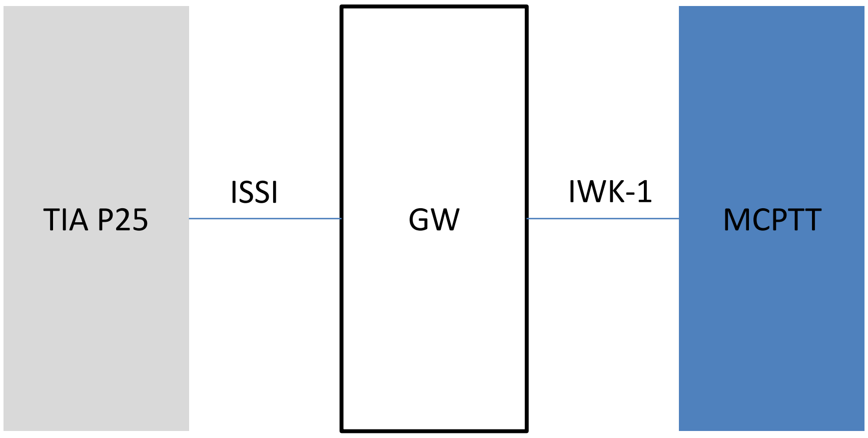
ETSI and ATIS are pushing requirements and use cases to 3GPP for Rel-14 along with terminology alignment between technologies (TETRA – P25 – Analog – MCPTT).

The standard will be developed by the 3GPP for the MCPTT side and by the ETSI WG4 for the Tetra side and by the TIA for the P25 side.

High level view of the solution should likely be this one for ETSI Tetra:



High level view of the solution should likely be this one for TIA P25:



In both cases (ETSI and P25), IWK-1 could be leveraged from MCPTT-3 reference point.

Airbus is a key contributor in Working Group dealing with this topic, namely ETSI WG4, ATIS and TIA P25. Airbus objective is to drive and ensure that the definition of these solutions fulfils the organisation requirements including at borders.

3GPP will also produce protocol conformance and interoperability specifications to ensure full interoperability.

3.2.5.7 SecInCoRe System Architecture based on Option 2

The SecInCoRe system architecture is depicted here below leveraging the 3GPP MCPTT solution:

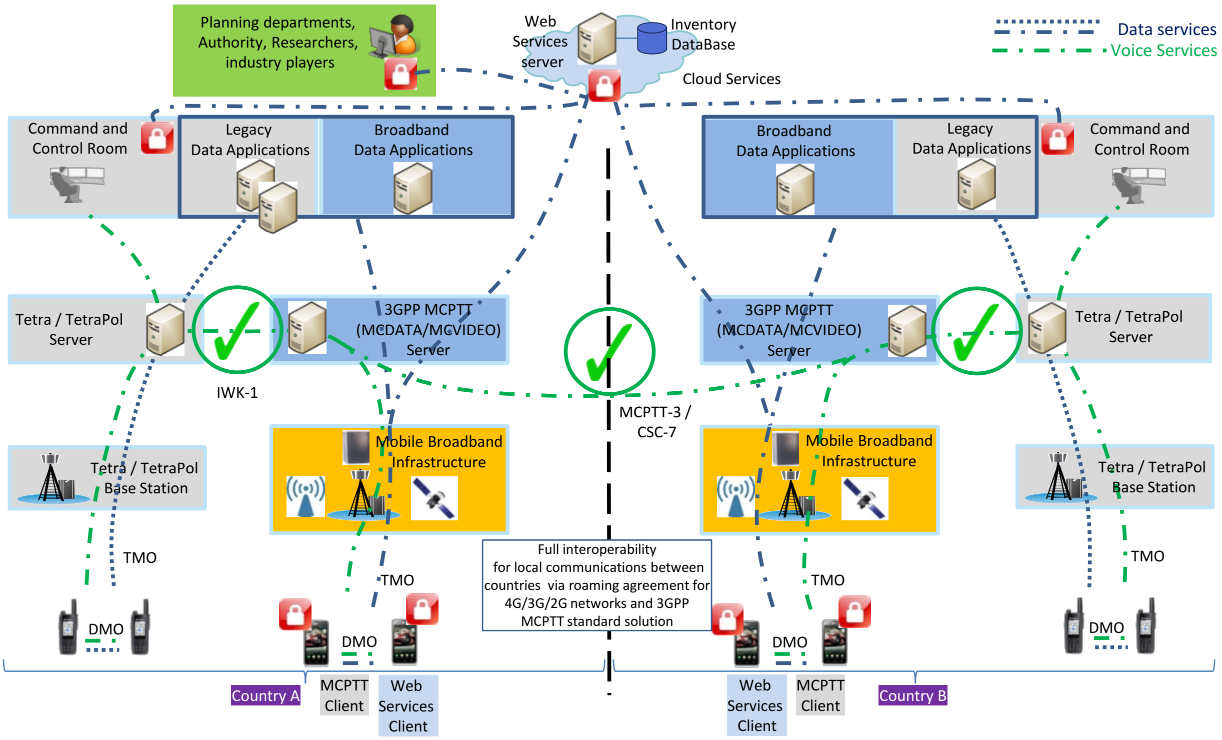

Planning departments, Authority, Researchers, industry players
Web Services server
Inventory DataBase
Cloud Services
Data services
Voice Services
Command and Control Room
Legacy Data Applications
Broadband Data Applications
Broadband Data Applications
Legacy Data Applications
Command and Control Room
Tetra / TetraPol Server
3GPP MCPTT (MCDATA/MCVIDEO) Server
3GPP MCPTT (MCDATA/MCVIDEO) Server
Tetra / TetraPol Server
IWK-1
MCPTT-3 / CSC-7
Tetra / TetraPol Base Station
Mobile Broadband Infrastructure
Mobile Broadband Infrastructure
Tetra / TetraPol Base Station
TMO
TMO
Full interoperability for local communications between countries via roaming agreement for 4G/3G/2G networks and 3GPP MCPTT standard solution
TMO
TMO
DMO
DMO
DMO
DMO
Country A
MCPTT Client
Web Services Client
Web Services Client
MCPTT Client
Country B

Figure 24 SecInCoRe system architecture

The general description provided for the option 1 related to Mobile Broadband services remains applicable (re infrastructure implementation models and IP Mobile Technology).

Mobile broadband services bring capacity for BB-PPDR users to access to legacy data applications but also to broadband Data applications (e.g. video, pictures, multimedia content). They also offer natively access to cloud services.

On the device side, PMR services are implemented in a client/server model leveraging the IP connectivity provided by the Mobile broadband services. Legacy PMR services are provided thanks to a MCPTT Client and a Web services client is provided to access to data applications including those hosted by the cloud services offered by SecInCoRe. Some data applications may require a specific data application client.

Moreover, some PMR services can be also provided in DMO (Direct Mode Operation) leveraging some technologies:

- WLAN with Wifi-direct
- LTE with ProSe (defined by 3GPP in Rel-12 and Rel-13)

In this architecture, interoperability with legacy PMR networks is provided by the MCPTT server via the IWK-1 reference point as described in the previous section.

Legacy PMR services supported by a MCPTT client are the same as the PMR services available on a Tetra/TetraPol device, but they could be offer in a different way.

If roaming agreement is in place between country A and country B, a BB-PPDR user from country A can access to MCPTT services of either country A (via MCPTT-3 reference point) or country B (mutual aid case) depending on the case, leveraging Mobile broadband services from country B.

Since this solution relies on a 3GPP standard MCPTT implementation, interoperability with other MCPTT systems is natively supported via the MCPTT-3 and CSC-7 reference points.

Moreover, BB-PPDR users from country A and B could have access to the same cloud services and could therefore be able to share/exchange information.

3.2.6 SecInCoRe NEC System concept Conclusion

Option 1 architecture leverages existing PMR network and is based on a proprietary solution which could be deployed immediately but with limitations when cross border communications are required.

Option 2 architecture is based on the 3GPP MCPTT standard which has been just approved by the 3GPP. Products need to be developed and will not be ready before 2017/2018.

The standardisation work will continue in 3GPP R14 (and likely in R15) on MCPTT in order to provide technical specifications which cover all the requirements identified in 3GPP SA1.

In 3GPP R14, the work will be also initiated on MCData and on MCVideo leveraging the framework already defined for the MCPTT.

MCPTT solution developed by the 3GPP standardisation bodies has solid foundation to provide interoperability between vendors and also across the borders. This will be addressed in 3GPP Rel-14 with inputs and close follow-up from ETSI and ATIS.

Both architectures may likely exist across European countries for many years since many of the public safety operators are today committed to sustain services on their legacy networks until 2025 (and even until 2030 in some cases).

However, it is more than likely that solution based on the definition done by the 3GPP will be the solution on which all the public safety operators across will converge and deploy.

3.3 Security Concept / principles

As part of the effort to standardise the MCPTT services in 3GPP Rel-13, the security aspects have been also addressed.

The security of the MCPTT has been described in the 3GPP TS 33.179.

This section starts by describing the main principles for security of MCPTT (for details see TS 33.179) and then proposes to go beyond and extend these principles to address the SecInCoRe concept.

3.3.1 Security of the MCPTT

Security topics covered in 3GPP TS 33.179 are:

- Authentication
- Service Authorisation
- Signalling plane protection
- End to end communications security

3.3.1.1 Authentication

Authentication phase is indeed split in 3 steps as described in the figure here below:

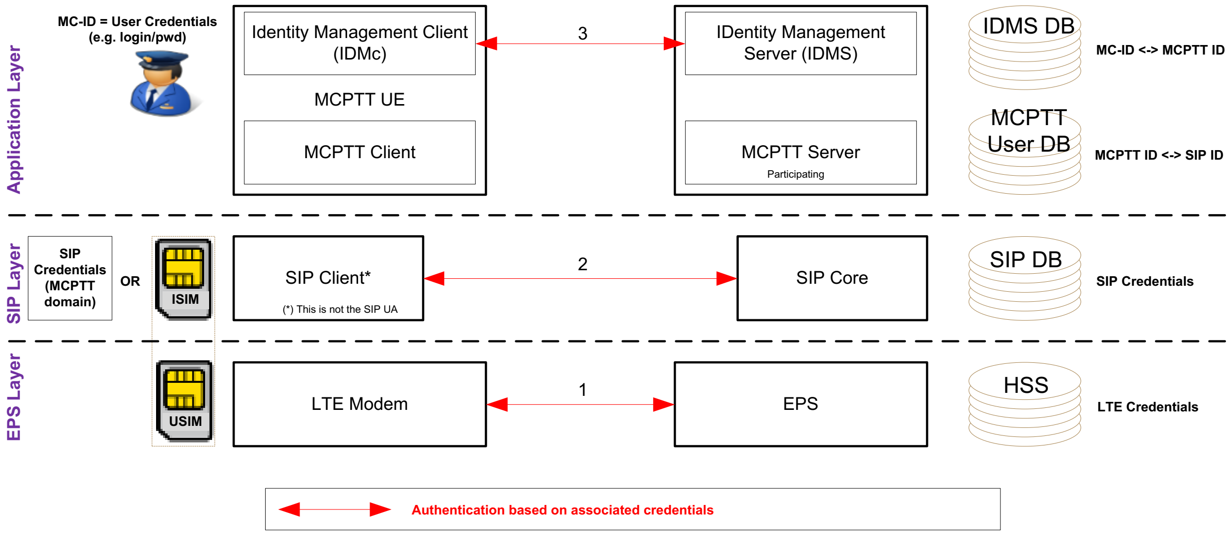


Figure 25 Authentication Layers

1 - LTE attachment (between UE and LTE Core Network): LTE mutual authentication

2 - SIP core authentication (between UE and SIP core): mutual authentication relying on IMS AKA

3 - MCPTT User authentication (between UE and Identity Management server):

1. relies on Open ID Connect 1.0

2. OpenID Profile is Authentication Flow Control
3. User authentication mechanism is left open (password, biometrics,…)
    a. in 3GPP Rel-13, the username/password-based user authentication is the mandatory supported method
4. User authentication allows UE to get an ID token defining the MCPTT ID of the user
5. User authentication allows UE to get access token(s) to be used for connecting different MCPTT servers (KMS, MCPTT server, GMS, CMS,…)

The user authentication is performed between identity management client located in the MCPTT UE and the identity management server located in the MCPTT common services core.

It is based on the OpenID Connect specification defined by the OpenID Foundation: http://openid.net/specs/openid-connect-core-1_0.html.

OpenID Connect is based on OAuth 2.0 protocol as defined in the IETF RFC 6749.

OpenID Connect (OIDC) is an authentication layer on top of OAuth 2.0 protocol, an authorization framework.

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. In technical terms, OpenID Connect specifies a RESTful HTTP API, using JSON as a data format.

Three flows are defined in OpenID Connect:

- Authorization Code Flow
- Implicit Flow
- Hybrid Flow

The MCPTT standard implements the Authorisation Code Flow.

To support MCPTT user authentication:

- the IdM server (IdMS) shall be provisioned with the user’s MC ID and MCPTT ID. A mapping between the MC ID and MCPTT ID is created and maintained in the IdMS.

Upon completion of the user authentication, the MCPTT client gets 3 tokens:

- an id token
  - The consumer of this token is the MCPTT UE
- an access token
  - The consumers of this token is the KMS, CMS, GMS and the MCPTT server
- A refresh token
  - The consumer of this token is the IDMS (Identity Management server)

3.3.1.2 Service Authorisation

MCPTT User service authorization (between UE and MCPTT servers) - performed in this order:

a. KMS Authorization (HTTP based)
b. MCPTT server authorization (SIP based)
c. Configuration Management Server authorization (HTTP based)
d. Group Management Server authorization (HTTP based)

There can be one access token per each server authorization

In other the validate the access token, the CSC Server (Configuration Management server, Key Management server, or Group Management server.) and the MCPTT server use the OAuth 2.0 Token Introspection procedures defined in the IETF RFC 7662.

3.3.1.3 Signalling plane protection

There are two signalling plane protection to support:

1 - SIP-1 protection (between UE and P-CSCF in SIP core):

The security mechanisms as specified in TS 33.203 for Gm interface are used to provide confidentiality and integrity of signalling on SIP-1 interface.

- IMS AKA
- IPSec ESP:
  - TDES or AES in CBC mode for encryption
  - HMAC-MD5 or HMAC-SHA1 for authentication

2 - HTTP-1 protection (between UE and HTTP proxy in network infrastructure side)

TLS with the profiles included in TS 33.310 Annex :

- TLS version should be >= 1.1
- Algorithm TLS_RSA_WITH_AES_128_CBC_SHA256 should be supported
- Either Pre-shared keys or PKI should be supported

The support of Transport Layer Security (TLS) on HTTP-1 is mandatory

The user authentication uses the HTTP-1 reference point, i.e. between the HTTP client in the UE and the HTTP proxy. The HTTP-1 reference point is based on HTTP and is secured using Transport Layer Security (TLS).

3GPP 33.179 defines several authentication mechanisms:

- one-way authentication of the HTTP Proxy based on the server certificate
- mutual authentication based on certificates
- mutual authentication based on pre-shared key

TLS 1.2 (RFC 5246) should be supported and should follow the rules on allowed and mandatory cipher suites given in RFC.

The cipher suite TLS_RSA_WITH_AES_128_CBC_SHA256 should be supported.

3.3.1.4 MCPTT Application plane security

Two different stream protections are specified by the 3GPP:

- Media stream protection (SRTP based) to protect the voice payload
- Media Control stream protection (SRTCP based) to protect the floor control

In order to proceed with these protection mechanisms, keys must be securely distributed to the key management clients.

Key distribution

The KMS (Key Management Server) is responsible for Identity Based Cryptography key material generation and distribution (to MCPTT server and UEs). Those keys are Key Encryption Keys.

Protocol used for key distribution is MIKEY SAKKE key encapsulation

Keys protecting media and floor control of a group call are:

- generated by the KMS
- delivered by the Group Management Server (GMS)
- Protocol used for key distribution is MIKEY SAKKE (Identity Based Encryption).

Media Stream protection

The media traffic protection ensures an end-to-end security from terminal to terminal (without infrastructure involvement).

The protocol is SRTP based on AES 128 GCM for payload encryption and authentication.

Floor Control protection

The Floor control protection ensures an end to end security from a terminal to floor control server in the network infrastructure.

The protocol is SRTCP based on AES 128 GCM for payload encryption and authentication.

3.3.2 Security for SecInCoRe concept

Principles defined for the security of MCPTT would likely be extended to provide security MCData and MCVideo:

- Authentication
- Service Authorisation
- Security of the signalling plane
- Optionally security of the MCData and MCVideo application plane.

Moreover, based on the security of the MCPTT defined in the 3GPP TS 33.179, the following principles can be leveraged for SecInCoRe:

- Authentication: This user authentication procedure has to be done once per user whatever are the services the user would like to access. The procedure defined by the 3GPP will be deployed to support the Mission Critical services such as MCPTT, MCData and MCVideo. Therefore, it would be beneficial for SecInCoRe to leverage this user authentication procedure also in the case of access to cloud services.
  However, the user authentication method could be enhanced to support also for instance biometrics or ID authentication via NFC. A AAA server (Authentication, authorization and Accounting) is a typical solution to provide these services.

- Authorisation: 3GPP has defined access tokens to access to different services. It would be beneficial for SecInCore to leverage this principle and use access token to access for instance to Cloud Services.

- User Profile: 3GPP has defined user-profile for MCPTT. Such profile of the user could be enriched in the CMS (Configuration Management Server) in order to manage access rights to the SecInCoRe cloud services.

Regarding transport security layer, in order that all the data applications could be accessed in a secured way typical deployment are based on VPN solution (IPSec based). It would be beneficial that SecInCoRe cloud services are also relying on such technology.

- As an option, data applications hosted in cloud services could also add additional security at application plane layer (e.g. authentication, encryption)

On the terminal side, keys materials distributed must be stored securely. It could be done either in the SIM card or in a smart SD card module.

4 Secure Cloud Services

4.1 Cloud Services

Cloud today inherently offers a lot of flexibility in terms of provisioning the required infrastructure on-demand when and where it is needed geographically, which in itself liberates service providers from the financial and temporal constraints of traditional infrastructure procurement, stack and subsequently application deployment and provisioning processes. In the following subsections, we will describe the challenges that need to be addressed in order to fully make use of the new opportunities presented by the cloud and the support services that facilitate this. We then proceed to describe the current SOTA in virtualisation approaches and technologies and the emergent edge and fog paradigms. Finally we apply these concepts to the SecInCoRe CIS, leveraging the NEC infrastructure to achieve a highly available and flexible framework.

4.1.1 Challenges to cloud infrastructure

This flexibility brings rise to new challenges and requirements in order to make full use of the potential of this new virtual infrastructure.

Although IaaS is available on-demand and facilitates a plethora of configurations and deployment topologies, the actual use-case specific stack deployment process remains a manual task. IaaS monitoring and scaling remains the responsibility of the system administrator, with provisioning and deprovisioning of service instances continuing to be a labor-intensive process.

In order to leverage the true potential of the cloud, additional tooling is required to provide extensive automation support in regards to the provisioning of infrastructure. Key enablers of cloud automation include the monitoring of virtual compute instances and optionally the services themselves. This facilitates health monitoring of service instances and their re-scheduling should they fail as well as the automatic scaling of service instances according to pre-defined IaaS and service specific QoS parameters.

4.1.2 Cloud support services

As such, clouds today offer a plethora of support services which act as enablers of cloud consumption. These include:

- VM / container monitoring
- Analytics, QoS and SLA services
- Provisioning of entire VM / container stacks using service and stack templates
- Scaling of VM / container instances to meet service demand
- Load balancing
- As-a-service availability of appliances, for example AAAaaS, DBaaS, HTTPaaS, VPNaaS, FirewallaaS
- For developers - Continuous Integration and Continuous Delivery support
- Life-cycle management of services

Concrete use-cases of these scenarios include the ability to deploy infrastructure topologies in an automated fashion with minimal involvement from system administrators, another being the need to adapt infrastructure availability to variable load where and when it is required in order to have services always run within SLA constraints.

For VM-based clouds, technologies that facilitate this include:

- Canonical's JUJU provides service aggregation, monitoring, orchestration to form independently scalable service stacks using the notion of 'charms', or VM composition templates. Each charm is a 'recipe' to deploy a given service onto a VM. JUJU then facilitates an easy way to link these services without the need for complicated configuration scripts. For example, to bring up a web server hosting wordpress, a database server and a cache service then to link them together in order to make them work takes just 5 lines of code:
    - Juju deploy wordpress
    - Juju deploy mysql
    - Juju deploy memcached
    - Juju add-relation wordpress mysql
    - Juju add-relation wordpress memcached

The deployment topology can subsequently be very easily visualised in figure 25:

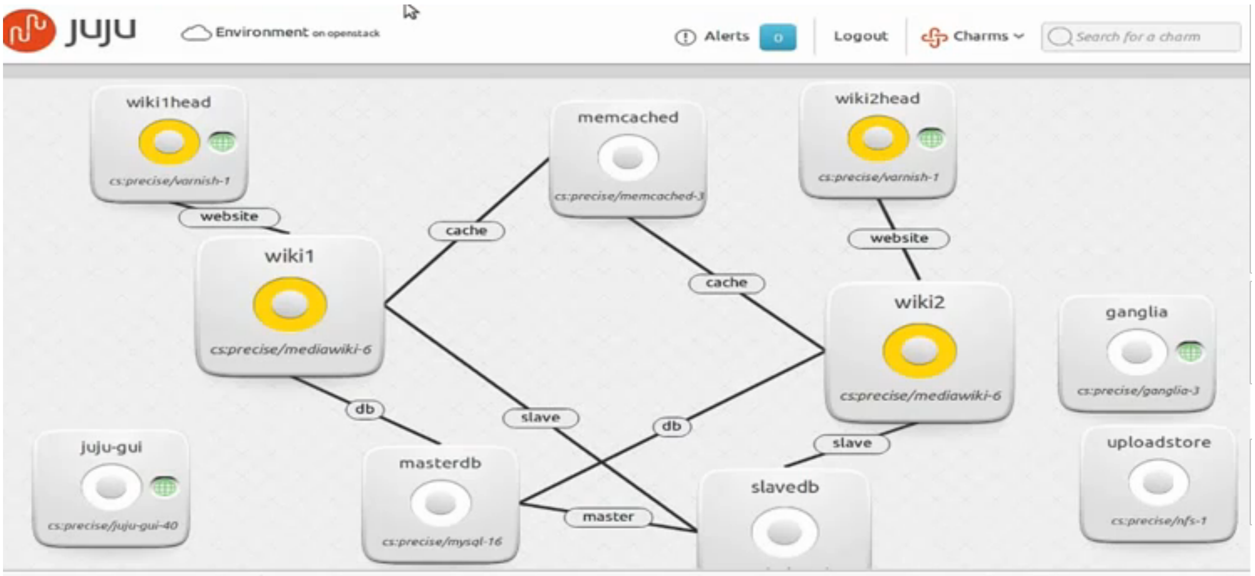


Figure 26 A visual representation of a JUJU stack topology with service dependencies

- Amazon Opsworks, Google Cloud Launcher, Flexiant CloudConcerto and RightScale facilitate commercial grade LBaaS and auto-scaling, as well as SaaS on top of IaaS. Scalr is an Open Source equivalent to these solutions and can provision SaaS across a number of clouds.
- Amazon offers VM-based service stack topology definition and automated creation using its AWS CloudFormation technology. OpenStack offers the same functionality using its HEAT technology and supports Amazon's CF templates.

Although a myriad of solutions do exist to achieve similar end-goals, industry initiatives are ongoing to standardise best practices and cloud formats, namely OVF, OCCI, TOSCA and OpenStack's HEAT.

4.1.3 Containers

More recent advancements in the cloud space revolve around the notion of 'container' technology. Although this technology is by no means new, it has recently come back into the spotlight, with intense development resulting in its rapid evolution and maturity.

Whereas VMs virtualise an entire physical machine, including all I/O interfaces and even CPUs, complete with the OS and its inherent storage and memory footprint, containers use a single instance of a 'host' OS and compartmentalise the remaining compute, RAM and storage available on that host far more effectively. It is also far easier to dynamically re-allocate resources to containers in relation to VMs.

Containers are distributed using public repositories from which services are fetched and instantiated, making the distribution of virtualised services highly efficient and lightweight.

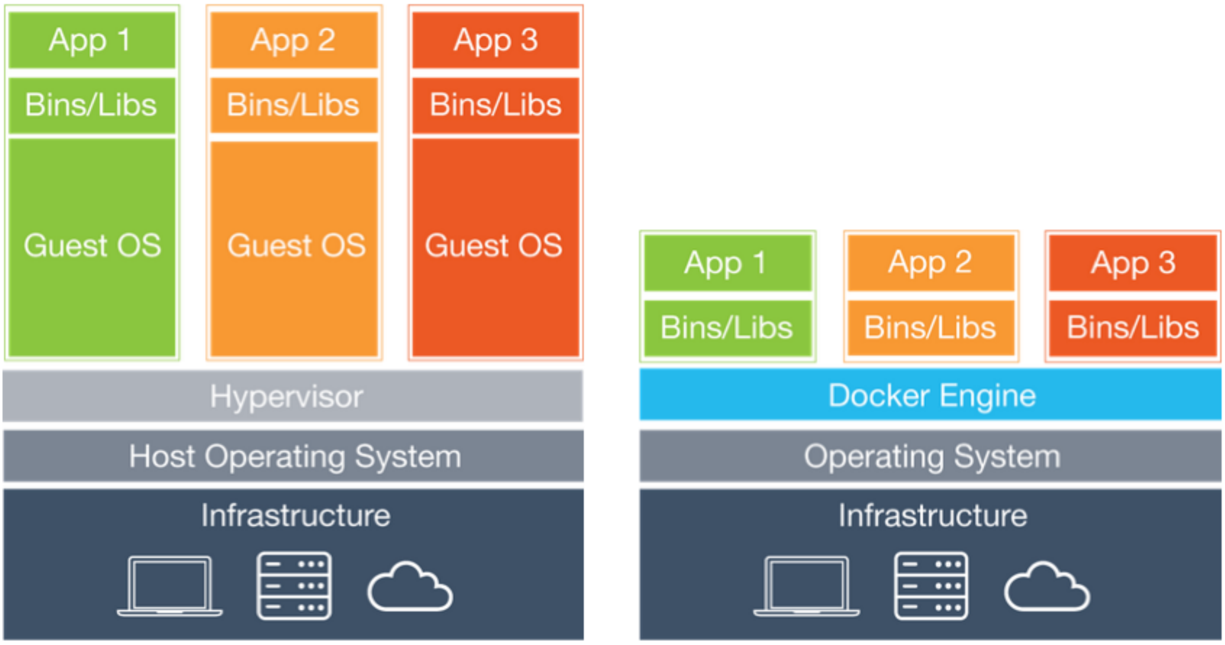


Figure 27 Hypervisor and Container based virtualisation footprints compared

Where this differs from deploying multiple services onto a single host without the use of containers is, much like when using VMs - the resource allocation guarantees, the security and privacy benefits in container isolation and the support services that a container platform offers.

The container paradigm has been extended significantly by leading industry players to offer many additional value-added services:

- Continuous Integration support for rapid and automated application deployment
- Support for a multitude of development languages and frameworks
- Support services easily available, much like in VM-based virtualisation: DBaaS, LBaaS, VPNaaS, FirewallaaS
- QA to publically published containers using a rating system
- PaaS solutions such as OpenShift are pioneering the current ‘microservices’ SOTA service composition pattern by recommending that service stacks are implemented in such a way as to have a single service run in an isolated container, with multiple containers aggregated in ‘pods’.
- Federated container deployment. Google pioneered the development of Kubernettes, which powers the Google services infrastructure. Docker Swarm has extended Docker to include container clustering across hosts.

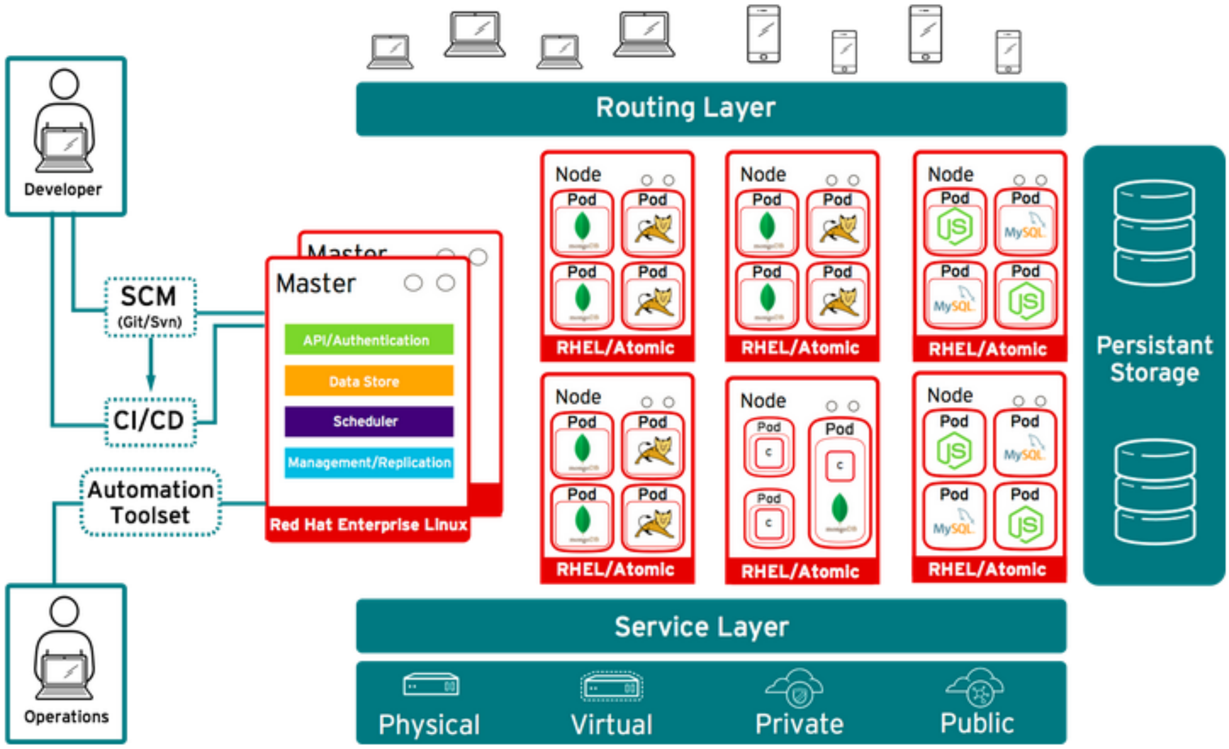


Figure 28 Container-based (micro)service deployment ecosystem, illustrating support services which enable service composition, service health monitoring, multi-node container orchestration and autoscaling

The ‘container’ virtualisation approach also brings with it the following benefits:

- Version control of container images. Snapshotting and stacking of container layers is possible, facilitating a highly productive means to build container images.
- Extremely rapid, near-instant instance provisioning times, as no OS needs to boot.
- Near-zero memory overhead per launched service instance.
- Where the containers are provisioned on bare-metal hosts, near-native performance is possible.

Negatives do however exist for container virtualisation:

- Containers are abstracted away from the underlying OS (hence kernel). There does exist the possibility for containers not functioning correctly on future versions of the underlying kernel.

4.1.4 Strategies for migrating legacy applications to the cloud

Legacy applications can easily be migrated to the cloud using Virtual Machines (VMs), which mimic in every way traditional bare metal infrastructure. As long as the underlying OS and software stack is that of a traditional bare-metal VM, the software deployed upon this VM will run without modification.

For example, if the application / service is architected in such a way so as to be stateless and runs across a cluster of machines in different layers, then deploying this stack within VMs in IaaS clouds is extremely straightforward. Legacy bare-metal hosts map directly to VM-based IaaS clouds, one example being the deployment topology for a web application server stack using the traditional 3-tier architecture model.

Once mapped to cloud, the auto-scaling support services of the cloud can facilitate the dynamic and automated scaling of service instances, liberating the now cloudified stack to make full use of the elastic and on-demand nature of cloud with minimal effort on behalf of the migration engineer.

4.1.5 VMs and containers compared

The core difference between VM-based virtualisation and container-based virtualisation is that legacy applications can be migrated directly to VMs and their deployment topologies rapidly mapped to deployment templates, even from live running physical servers as is the case with CloudSigma’s cloud. These service stacks can then relatively easily be provisioned on-demand on any cloud supporting industry standard VM and deployment template formats. The cloud provider’s auto-scaling services can be configured in such a way as to monitor and automatically scale VMs up or down, depending on their load. This is the most direct route to making existing software cloud-capable. Although the mapping of deployment topologies using containers can be achieved in much the same way as with VMs, it is not as trivial to migrate legacy applications to containers, with the process being somewhat more involved in order to accommodate the container architecture.

4.1.6 Security

Cloud IaaS technologies follow the same legacy security best practices including enabling SSH-only access to infrastructure, enabling firewalls per compute instance and at the edge of the network, service instances not being exposed on via a public IP address where unneeded and a comprehensive and timely vulnerability patch procedure. In addition, they offer VLAN traffic isolation (VPN can extend cloud to offer VLAN over WAN), hypervisor-level isolation of VMs, Access Control Lists and cloud-level Firewall functionality.

Containers (which often run on top of, hence build on, IaaS security) and Docker in particular help make applications safer as by design Docker provides a reduced set of default privileges and capabilities. It makes extensive use of namespaces, meaning that each container has an isolated view of the system. This includes the file system, the network stack and inter-process communication. Processes running in one container cannot see and effect processes in another.

Where containers are composed to form microservice stacks, best practices dictate that their communication channels are facilitated solely by Docker's container link functionality, which does not expose a container via network ports, adding an additional network security layer to services deployed using this approach. This is akin to not exposing a public IP address at the VM level.

All cloud technologies facilitate the running of 'appliances' or SaaS instances within the service stack, be it using an IaaS service graph or by composing together containers. These appliances include security services, such as VPNaaS, FirewallaaS, AAAaaS, PKIaaS, RadiusaaS. In essence, legacy security appliances can be architected together on-demand in the cloud, as opposed to relying on traditional physical devices.

In the scope of SecInCoRe, key security enabling services such as PKIaaS, IdMaaS or AAAaaS can be used as key enablers of the NEC infrastructure as detailed in section 3.3. Containers make possible Highly Available deployments, with on-site fog devices hosting local service instances in a HA and off-site traditional cloud facilitating replication and IdM federation.

Initiatives are underway to facilitate remote attestation of cloud infrastructure and the secure processing of workloads within encrypted areas of the CPU (so-called 'enclaves') using Intel SGX technology. Certain Container technologies already provide the ability to sign and validate images using the notion of 'content trust'.

4.1.7 SOTA and future opportunities

The cloud industry is currently focusing on the federation of distributed and disparate IaaS clouds, with the current SOTA moving on from the federation of traditional clouds and into the federation of 'edge' clouds which sit on the edge of traditional telecoms or other networks and the notion of the federation of 'fog' clouds, consisting of end-user and IoT devices. This federation of cloud federations aims to bring end-user devices into the computation and storage pool and make them available for geolocation aware, dynamic and ephemeral service deployment and provisioning. Largely due to the lightweight resource footprint of containers, their easy distribution, rapid provisioning and emergent technologies facilitating their clustering and federation, they will be a likely technology choice for fog computing.

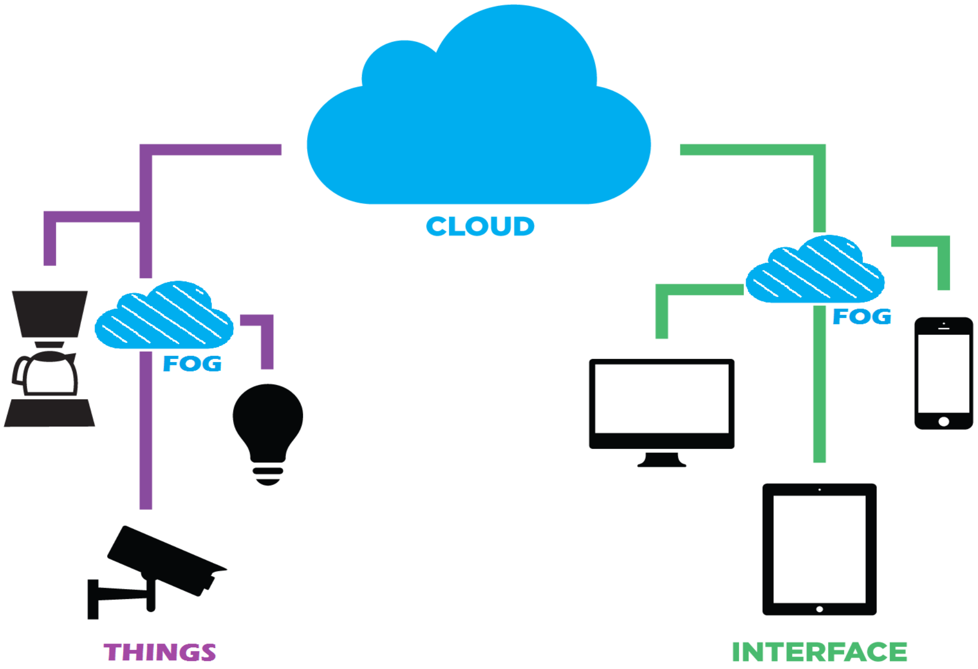


Figure 29 Traditional data-center Cloud and the emergent fog cloud

4.1.8 Common best practice approaches in cloud solutions

The common thread running through the cloudification of legacy services is that of the separation of services into atomic units of functionality, the ability for their snapshotting, versioning and storage in online repositories and their assembly into service stacks by means of aggregation and composition into stack deployment templates. Further cloud support structures that truly liberate the services is the automation of monitoring of services and their automated scaling based on load.

4.2 Secure Cloud Services in SecInCoRe

SecInCoRe's 'Eduroam' WiFi access point reference implementation provisions network access level AAA by means of provisioning LDAPaaS and RadiusaaS on a Synology 'fog cloudlet' enterprise SOHO NAS server offering SaaS. These AAAaaS services are coupled with a GeoIP restricted WiFi access point running modified Open Source firmware (DD-WRT), configured with WPA2-Enterprise WiFi. The AP authenticates with the Synology cloudlet by means of a Radius client-server relationship.

The NAS uses Synology's proprietary and highly scalable OS (DSM 6.0), which already runs physically or virtually on both data center infrastructure as well as end-user devices. In its most recent incarnation, the OS has re-engineered its SaaS repository to leverage container virtualisation and is strongly positioned to offer SaaS deployment across a variety of both cloud and fog infrastructures. The OS is also available as Open Source (see [WWW13]).

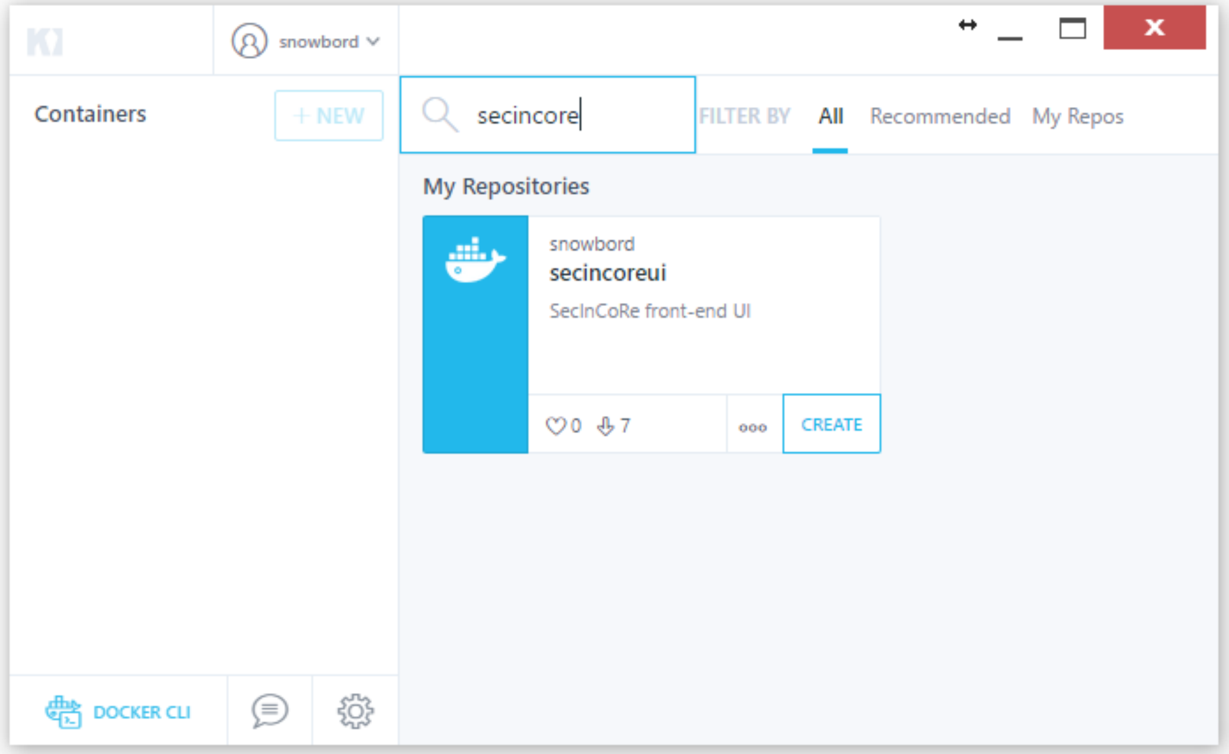
SecInCoRe's NEC subsystem implements Data-in-transit security using the VPNaaS in the form of OpenVPN, provisioned on CloudSigma's Zurich cloud. This can alternatively be facilitated using Synology's DSM OS, or an alternative VPNaaS provider, such as OpenSwan or by OpenStack Newtron within an OpenStack cloud.

The Semantic Framework reference implementation and its cloud service capability is described in chapter 4.3.

4.2.1 Distributing SecInCoRe services as containers

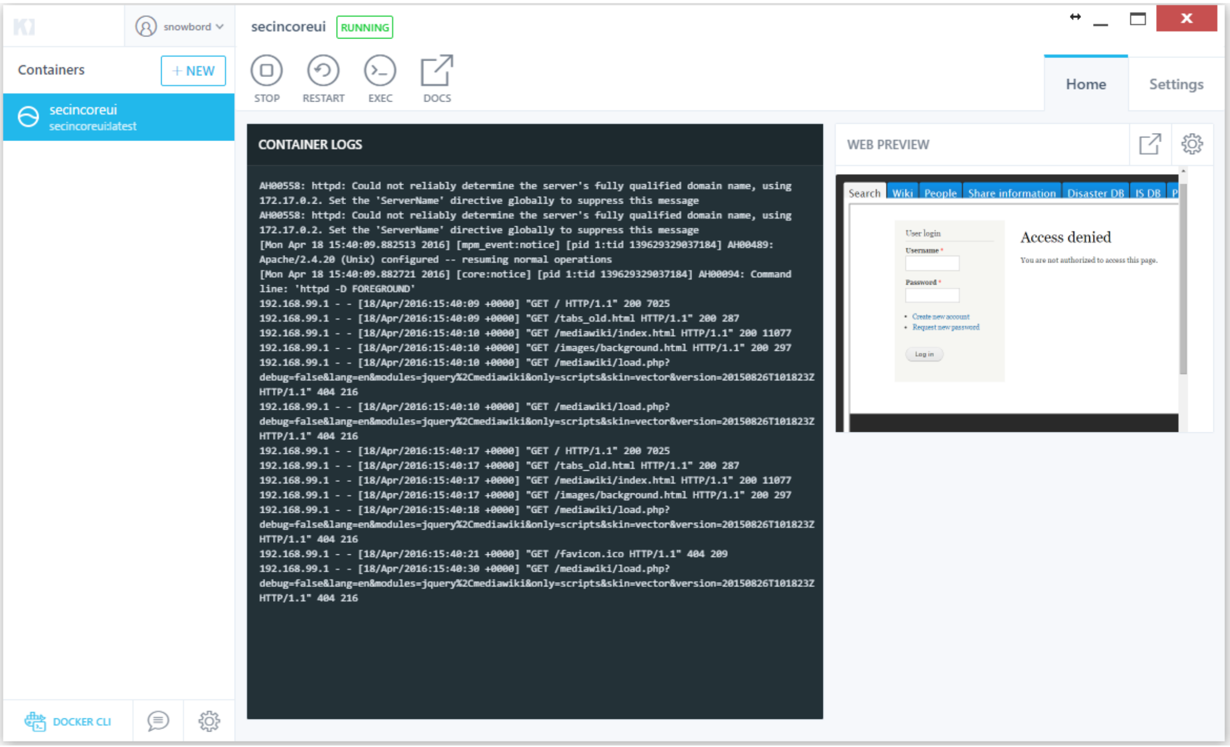
As a proof of concept of the aforementioned current best practices in the modularization and cloudification of legacy services into cloud services and how this can be applied within SecInCoRe, the web-based front-end interface of the SecInCoRe CISD was packaged within an official Topcat web server Docker image and committed to the Docker Hub registry.

Once committed to an online repository, containers can easily be downloaded and instantiated in an extremely resource-efficient manner on any Docker compatible device, something of ever-increasing significance bearing in mind the emergent role of edge and fog cloud within the cloud industry.



snowbord
secincoreui
SecInCoRe front-end UI

Figure 30 Searching the Docker Hub Registry for SecInCoRe images on Windows using Docker Tools' Kitematic



```
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using
172.17.0.2. Set the 'ServerName' directive globally to suppress this message
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using
172.17.0.2. Set the 'ServerName' directive globally to suppress this message
[Mon Apr 18 15:40:09.882513 2016] [mpm_event:notice] [pid 1:tid 139629329037184] AH00489:
Apache/2.4.20 (Unix) configured -- resuming normal operations
[Mon Apr 18 15:40:09.882721 2016] [core:notice] [pid 1:tid 139629329037184] AH00094: Command
line: 'httpd -D FOREGROUND'
192.168.99.1 - - [18/Apr/2016:15:40:09 +0000] "GET / HTTP/1.1" 200 7025
192.168.99.1 - - [18/Apr/2016:15:40:09 +0000] "GET /tabs_old.html HTTP/1.1" 200 287
192.168.99.1 - - [18/Apr/2016:15:40:10 +0000] "GET /mediawiki/index.html HTTP/1.1" 200 11077
192.168.99.1 - - [18/Apr/2016:15:40:10 +0000] "GET /images/background.html HTTP/1.1" 200 297
192.168.99.1 - - [18/Apr/2016:15:40:10 +0000] "GET /mediawiki/load.php?
debug=false&lang=en&modules=jquery%2Cmediawiki&only=scripts&skin=vector&version=20150826T101823Z
HTTP/1.1" 404 216
192.168.99.1 - - [18/Apr/2016:15:40:10 +0000] "GET /mediawiki/load.php?
debug=false&lang=en&modules=jquery%2Cmediawiki&only=scripts&skin=vector&version=20150826T101823Z
HTTP/1.1" 404 216
192.168.99.1 - - [18/Apr/2016:15:40:17 +0000] "GET / HTTP/1.1" 200 7025
192.168.99.1 - - [18/Apr/2016:15:40:17 +0000] "GET /tabs_old.html HTTP/1.1" 200 287
192.168.99.1 - - [18/Apr/2016:15:40:17 +0000] "GET /mediawiki/index.html HTTP/1.1" 200 11077
192.168.99.1 - - [18/Apr/2016:15:40:17 +0000] "GET /images/background.html HTTP/1.1" 200 297
192.168.99.1 - - [18/Apr/2016:15:40:18 +0000] "GET /mediawiki/load.php?
debug=false&lang=en&modules=jquery%2Cmediawiki&only=scripts&skin=vector&version=20150826T101823Z
HTTP/1.1" 404 216
192.168.99.1 - - [18/Apr/2016:15:40:21 +0000] "GET /favicon.ico HTTP/1.1" 404 209
192.168.99.1 - - [18/Apr/2016:15:40:30 +0000] "GET /mediawiki/load.php?
debug=false&lang=en&modules=jquery%2Cmediawiki&only=scripts&skin=vector&version=20150826T101823Z
HTTP/1.1" 404 216
```

Figure 31 The SecInCoRe UI running within a Docker container

Any Docker-enabled device can in an instant bring up the SecInCoRe UI using the following command, which checks if the container image is available locally and if not, downloads and runs it automatically:

docker run -dp 80:80 snowbord/secincoreui

In order to provision a Docker-enabled VM on an IaaS provider, thus enabling the ability to download and instantiate SecInCoRe (container) services in this case on an IaaS public cloud, a CloudSigma VM was contextualized using the industry standard CloudInit syntax.

```
#cloud-config
package_upgrade: true
package_reboot_if_required: true
ssh_authorized_keys:
 - << public SSh key >>
runcmd:
 - apt-get update
 - curl -fsSL https://get.docker.com/ | sh
 - curl -fsSL https://get.docker.com/gpg | sudo apt-key add –
 - docker run -dp 80:80 snowbord/secincoreui
 - echo "docker run -dp 80:80 snowbord/secincoreui" > /etc/rc.local
```

This achieves the following:

1. Secure system access using a SSh key.
2. Update the system, rebooting if necessary.
3. Install Docker and DockerHub’s GPG key, ensuring the downloading of container images is trusted and encrypted
4. Download and install the SecInCoRe UI image (containing the Apache web server) and run it in a container on the VM on port 80.
5. Ensure Linux runs this (web server) container every time the VM boots.

This Docker-enabled VM can then run any mix of SecInCoRe services that have been published to an online container image registry. It can additionally be configured for federated cloud container orchestration using tools such as Docker Swarm, Kubernettes, as well as visually using graphical front-ends such as Docker Shipyard.

4.2.2 Impact on SecInCoRe reference implementation deployment

The ability to compose service stacks from microservices packaged and distributed by means of containers and to provision these as-a-service on operating systems which run both on data center ‘cloud’ infrastructure as well as an ever growing range of consumer ‘fog’ devices will technically enable true trans-border on-demand service provisioning on any available infrastructure. When applied to SecInCoRe, this federation of cloud federations will facilitate an extremely resilient, secure, highly available and fault tolerant service provisioning infrastructure. Such a framework would complement UPB’s highly available NEC WiFi mesh network technology to make use of the computation and storage available on or in the proximity of each node of the mesh, hence make possible the automated deployment of the SecInCoRe service stack by leveraging all existing network-enabled devices.

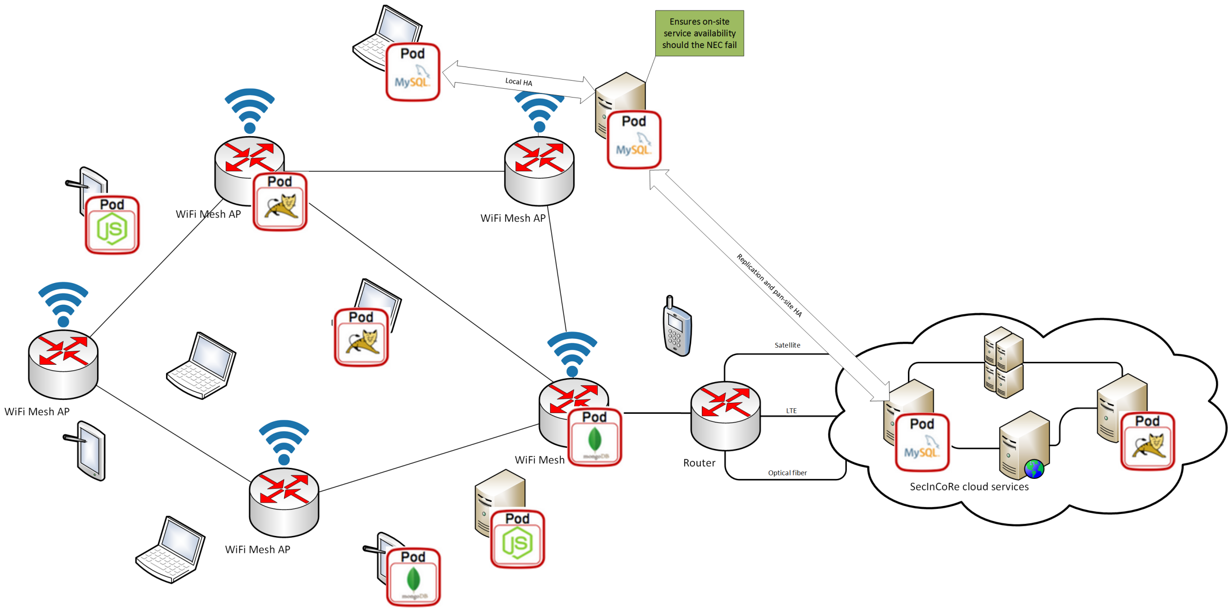


Figure 32 NEC mesh network and fog / cloud container service deployment

4.3 Semantic Framework

The Semantic Framework (SF) contains backend components of the User Interface Implementations described in D5.3. The Semantic Framework aims to crawl and analyze the Knowledge Base (KB) content and make it easily available for End Users. This aim should be reached by implementing a semantic search in distributed data sources in the domain, as described in D3.3 chapter 6. The SecInCoRe-Demonstrator builds upon the KB (data and metadata tier) and provides functionality to combine, search (logic tier) and visualise (presentation tier) data from the KB. The architecture concept of the Semantic Framework and the current status are explained below. At the end, the main components and the integration into the SecInCoRe Cloud Services are described in more detail.

4.3.1 Concept

To reach the above described aims, the Open Semantic Framework (OSF) was identified as the best fitting main component. To realize the analysis, search and visualization additional components are needed. The architecture of the overall system is shown in Figure 3332 on the next page. This Figure shows all main components of the Semantic Framework in an aggregated manner, therefore the details are not displayed. The core of the Semantic Framework is the OSF in the middle of the Figure. In this component, all Knowledge Base contents are stored RDF-based to enable the semantic search in them. After that, the content analysis using the SecInCoRe ontology (described above) is done by this component. The OSF consists of several separate components (as the Virtuoso triple store as RDF storage, a Solr Search Index etc.) which offers the functionalities öin strong interaction. The frontend of OSF will be implemented by our own, by the graphical user interface as described in D5.3. Beside the search GUI, the possibility to contribute documents into the Knowledge Base is given by the Upload GUI. The upload function is integrated as an easy way to share information. The overall concept focuses on the automatic integration of data sources instead of uploading single documents. The contribution is enabled by a Seafile instance, which enables the addition of documents of nearly every file type into the search. Theses user interfaces should be integrated into one central user interface, to enable an intuitive and simple access to these functionalities and the other reference implementations as the Open Atrium. The OSF has no in-built possibilities to integrate data from different data sources. To enable that integration, the data has to be crawled from several data sources, formatted and imported into OSF. In the upper right area of the Figure, there are several external and internal data sources shown in grey. These data sources could be located either on SecInCoRe internal file systems or on servers within the domain. The data is stored in different ways. The main data sources are file systems, SQL databases and websites. To integrate all these data sources, the open source tool ManifoldCF is used. ManifoldCF enables the crawling in several different data sources. After the crawling process, the data are converted to plain text via an Apache Tika plugin. When the data are in the unified format, they are semantically analysed and processed via a SOAP (Simple Object Access Protocol) Server. The semantic analysis performs a Named Entity Recognition on the document and searches for accordant entities in the document and the SecInCoRe ontology. When a matching is found, the new meta data is added to the document. The SOAP server can do a second analysis with the help of the AlchemyAPI. This program finds the topic of the document inserted, concerning a “world ontology” and adds it to the metadata of the document. After that the API of OSF is called by the SOAP Server and the data is inserted into the search. To enable the analysis of the data with the SecInCoRe ontology, it is needed in a machine readable form. To extend the ontology generated in SecInCoRe, the domain members could help. At least on a conceptual level, the integration of the Semantic Media Wiki (SMW) is planned. This Wiki could allow end users to work collaborative an intuitive to enhance the existing ontologies. To reach that aim, many extensions for the SMW have to be implemented, because the current SMW offers only a simple editing of instance data, but not of the ontology data. To get the “world knowledge” to analyse the data, there is the Alchemy API way as described above. Additionally, Linked Open Data (LOD) sources could be used. The LOD are used, to show definitions and information concerning the search query.

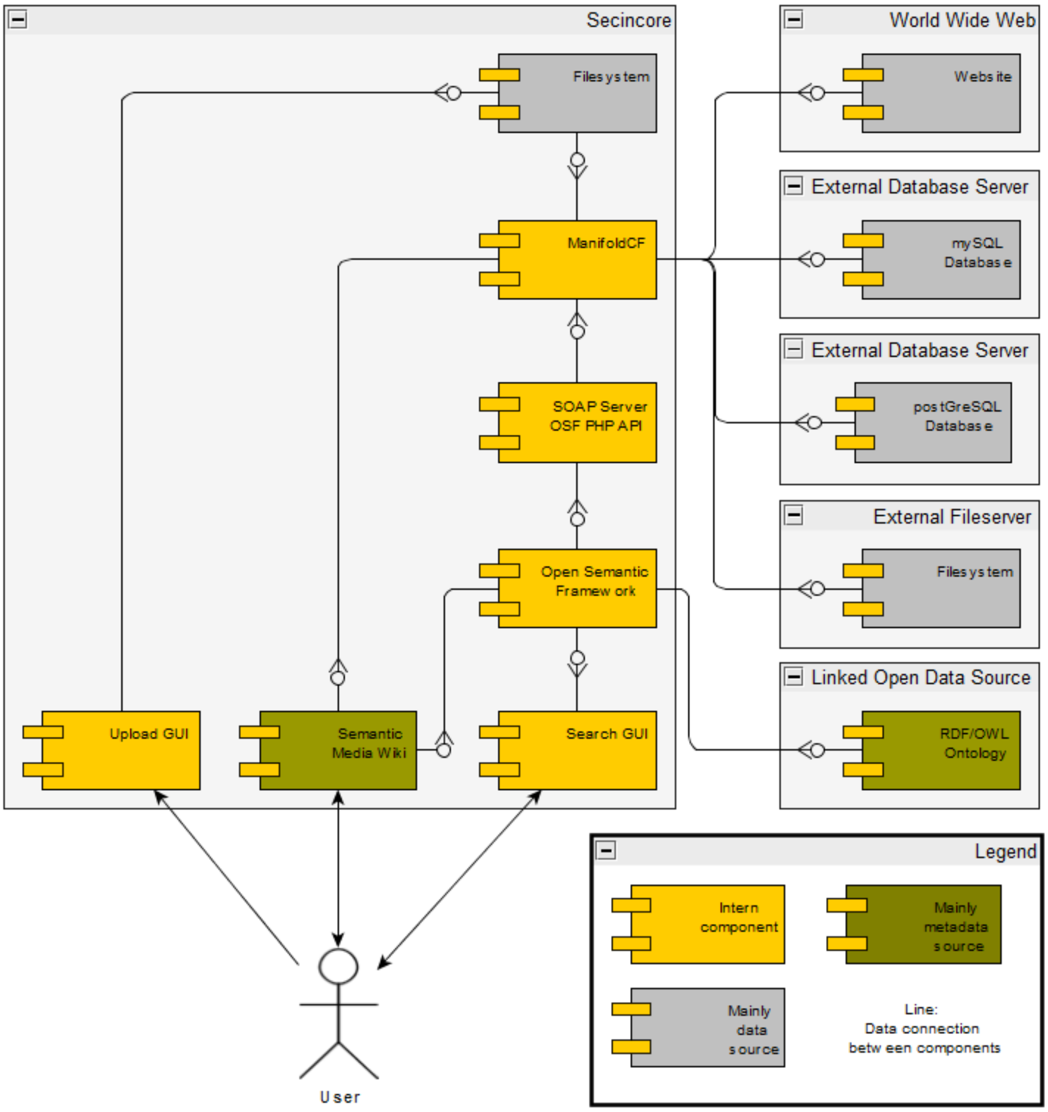


Figure 33 Semantic Framework architecture.

4.3.2 Current status

The current status of the Semantic Framework is explained below. The Open Semantic Framework is installed and configured properly. The search user interface is available in a first version and under development as described in D5.3. The SOAP Server is implemented and enables the connection of data sources into OSF. ManifoldCF is installed and the specialised connection to OSF is implemented in a first version, where the crawling of one data source at the same time into the search is enabled. In the next step, this component will be enhanced to handle multiple data sources in parallel. The internal file system is connected to the search. The Contribution GUI enables the Upload and automatic integration of documents into the search. At the moment one ontology could be used to analyse the data. The addition of more ontologies is planned. The analysis via Alchemy API is tested in a proof of concept and has to be integrated into the search. The Semantic Media Wiki is not in focus at the moment and will only be implemented, if there is time left. In this way a standard installation with a proof of concept is installed, but not further developed.

4.3.3 Open Semantic Framework

The Open Semantic Framework is a bundle of connected applications, which enable the semantic search. The main components are the “OSF Core” with the backend of the application and the “OF for Drupal” module, which offers a separate way of configuration and management of the backend. The tasks of OSF in the SecInCoRe demonstrator are mainly the semantic storage of the data, the management of the analysis and the search functionality. The storage is realized with a Triple Store named Virtuoso. Based on this store, the analysis is done by the integrated “scones” tagger and/or external analysis tools. To enable the search, the data is referenced in a “solr” search index. The access to all these services is enabled by “OSF for Drupal” and by the use of Web Services, which are bundled in different APIs. The data is stored internally in “Datasets” which represents a data source and “Records”, which represents a single document. The OSF needs as input data in RDF notation, which is provided by ManifoldCF.

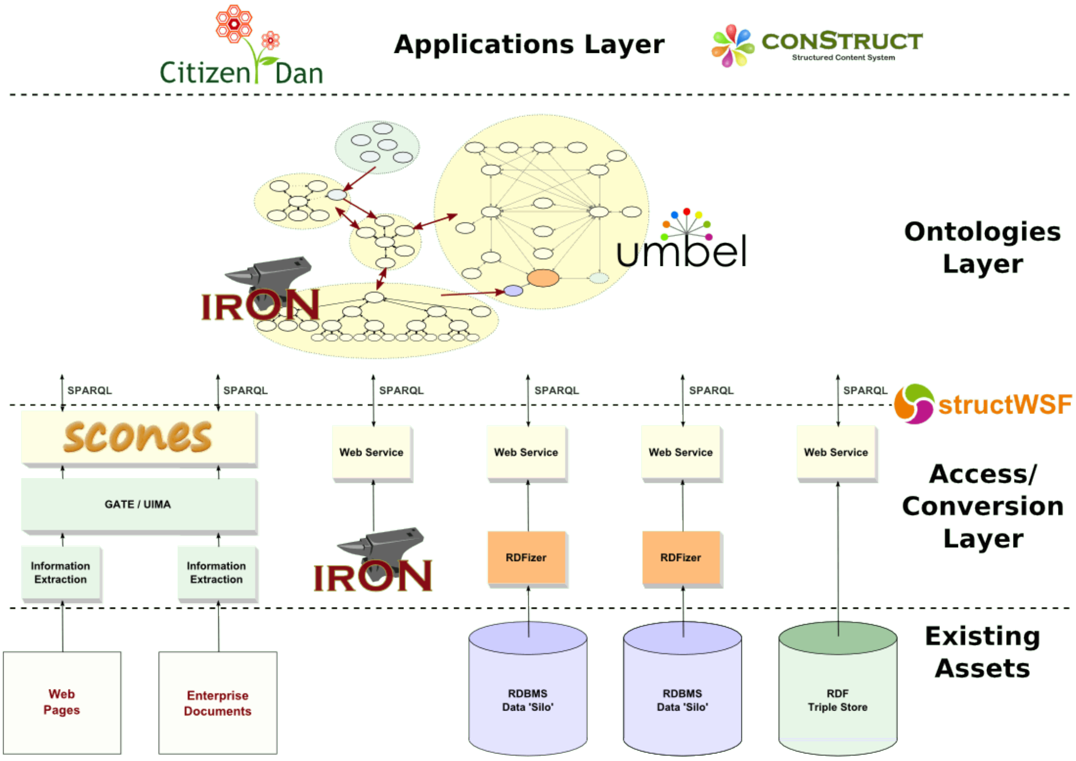


Figure 34 OSF architecture [GB14]

4.3.4 ManifoldCF

In ManifoldCF, the data from the different data sources are crawled and pre-processed. As shown in the Figure below, the main components of ManifoldCF are different connectors.

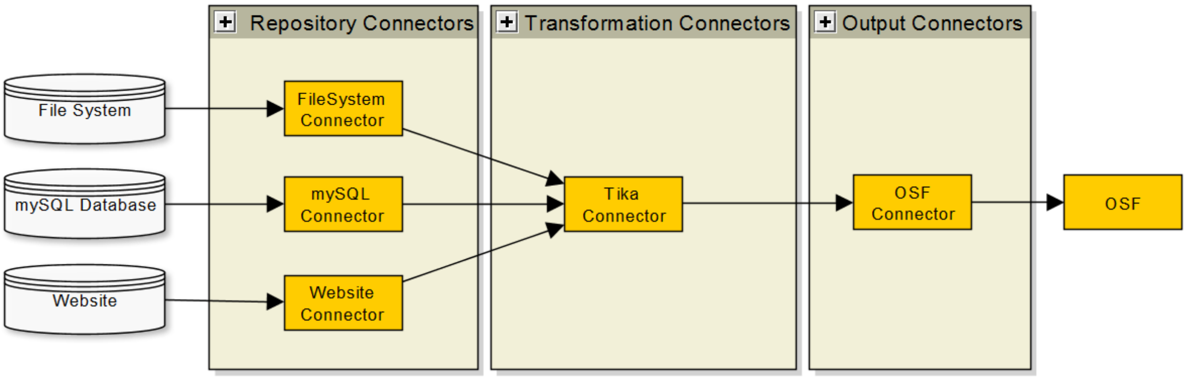


Figure 35 ManifoldCF crawling process

These connectors could be connected with each other as necessary by the data sources and search engines. In SecInCoRe, the data sources are crawled with existing repository-connectors built for MySQL databases, file systems, websites etc. Overall there are about a dozen different connectors for different data source types. These connectors enable the configuration of the crawling, collect the data and send it to transformation connectors. These transformation connectors process the data. In our case, the Tika connector is used, to extract the plain text out of different data formats. After the transformation connectors have done their work, there is the possibility to manage permissions with so called authority connectors. This aspect is not addressed yet. To send the data to OSF, an output connector is needed. There is no pre-built output connector for OSF sothis connector is implemented within SecInCoRe. The connector takes the processed data from the Tika transformation connector and sends it to OSF, using the SOAP server. The whole crawling process is visualized in Figure 36. The data is crawled and processed by ManifoldCF from different data sources as described above. In the following it is analysed using OSF and external analysis tools. When the analysis is finished, the data is stored both, in the OSF triple store and the search index. When a user starts a search query in the search GUI, the data is provided by the storages and shown in the GUI.

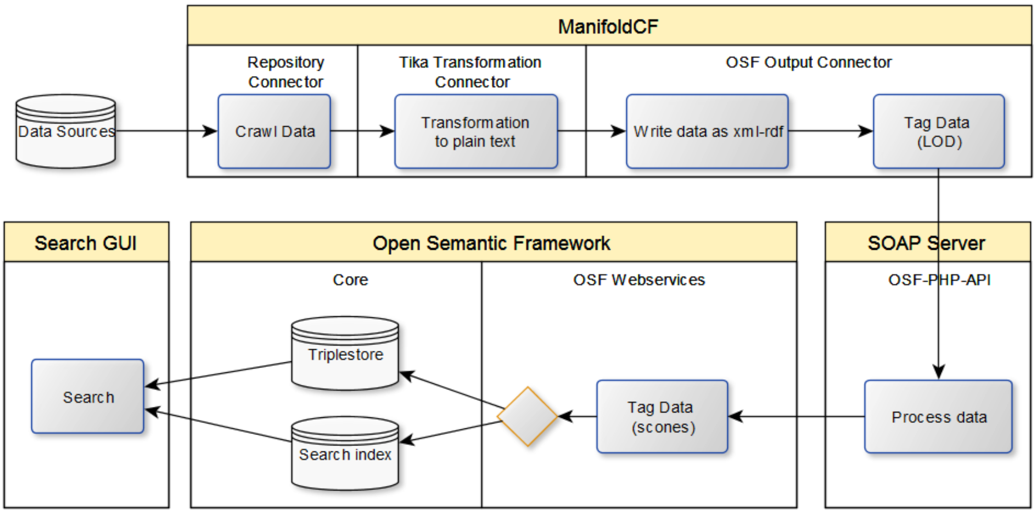


Figure 36 Crawling process

4.3.5 Cloud service integration

The Semantic Framework consists of many components which work together to enable the semantic search and the access to the other functions. All these components could be transformed into cloud services, which offer only a subset of the overall functions:

1. Open Semantic Framework
   It enables the management of the ontologies and datasets.
2. ManifoldCF
   It enables the Crawling from different data sources.
3. User interface
   The UI offers an integrated interface to all other components
4. Contribution
   This component offers the possibility to upload documents into the search

5. Semantic Media Wiki
   The SMW should enable the collaborative ontology creation.
6. Databases
   The databases store the Knowledge Base contents

The possibility to capsulate a component into a service is exemplified below by the user interface.

The user interface enables the access to the search in OSF, the databases, Open Atrium, Semantic Media Wiki and external implementations. The user interface could be installed completely separate from the other components. At the moment it could be installed on a virtual machine with Ubuntu 14.04 LTS via the following simple steps:

1. Install Oracle Java 8

3. Install and configure Tomcat 8

4. Go to the Tomcat Manager at http://server_IP_address:8080/manager/html and deploy the provided .war file.

4. You can now access the user interface at http://server_IP_address:8080/appframework

These installation steps have been automated and a pre-manufactured Docker image has been created for easy deployment of the user interface component in the SecInCoRe cloud (see section 4.2.1). These procedures could be adapted for the other components of the Semantic Framework and therefore enable a complete cloud compatible concept. The implementation of these concepts will not be part of the Semantic Framework, because the focus of the reference implementation is the demonstration of the common information space and not the technical backend functionalities.

5 Literature index

[AaEi99] Aas, Kjersti; Eikvil, Line: “Text Categorisation: A Survey”

[Ahlsén and Kool 2014] http://www.bridgeproject.eu/downloads/d04.3_information_and_deployment_view.pdf

[BiMR04] Biethahn, J.; Mucksch, H.; Ruf, W.: Grundlagen. Oldenbourg Verlag, 2004.

[BlLü95] Blohm, H.; Lüder, K.: Investition, 1995.

[BrMi14] Brickley, D., Miller, L.: FOAF Vocabulary Specification 0.99, January 2014, available at http://xmlns.com/foaf/spec/.

[Buscher et al.16] Buscher, M., Becklake, S., Easton, C., Kerasidou, X., Oliphant, R., Petersen, K., Jasmontaite, L.; Paterour, O. (2016). ELSI Guidelines for Networked Collaboration and Information Exchange in PPDR and Risk Governance. Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil

[EhSt04] “QOM – Quick Ontology Mapping”

[ELBB+04] “D2.2.3: State of the art on ontology alignment”

[FrMu00] Natalya Fridman, and Mark A. Musen. "Algorithm and tool for automated ontology merging and alignment." Proceedings of the 17th National Conference on Artificial Intelligence (AAAI-00). Available as SMI technical report SMI-2000-0831. 2000.

[Gabl15] Gabler Wirtschaftslexikon: Nutzwertanalyse. http://wirtschaftslexikon.gabler.de/ Definition/nutzwertanalyse.html, 19.11.2015.

[GaWo11] Galton, A., Worboys, M.: An Ontology of Information for Emergency Management, in: Proceedings of the 8th International ISCRAM Conference – Lisbon, Portugal, May 2011, available at http://oldway.org/publications/ISCRAM-122-final.pdf.

[GB14] Giasson, F.; Bergmann, M.: OSF Wiki. http://wiki.opensemanticframework.org/index.php/File:Product_landscape.png, 04.11.2015.

[GeLe14] Geldermann, J.; Lerche, N.: Leitfaden zur Anwendung von Methoden der multikriteriellen Entscheidungsunterstützung, 2014.

[GeoN12] GeoNames Ontology, November 2012, available at http://www.geonames.org/ontology/documentation.html.

[GoCa13] Government of Canada – Public Safety Canada: Canadian Disaster Database, September 2013, available at http://cdd.publicsafety.gc.ca/srchpg-eng.aspx?dynamic=false.

[GWIC10] Institute for Crisis, Disaster, and Risk Management (ICDRM), The George Washington University (GWU): ICDRM/GWU Emergency Management Glossary of Terms, June 2010, available at: http://www.gwu.edu/~icdrm/publications/PDF/GLOSSARY%20-%20Emergency%20Management%20ICDRM%2030%20JUNE%2010.pdf.

[JoSi11] Jovanovic, J., Siadaty, M.: IntelLEO Organization Ontology, April 2011, available at http://www.intelleo.eu/ontologies/organization/spec/.

[Lim12] Limbu, M.: Management of a Crisis (MOAC) Vocabulary Specification, January 2012, available at http://observedchange.com/moac/ns/.

[LoKi14] Loibl, P.; Kirchhöfer, K.: Kompendium Gefahrenmanagement- und Leitsysteme mit Leistungsübersicht – Marktstudie-, TeMedia Verlag, 3.Auflage, 2014.

[LoOh+05] Lorenz, B., Ohlbach, H. J., Yang, L.: Ontology of Transportation Networks, August 2005, available at: http://rewerse.net/deliverables/m18/a1-d4.pdf.

[Niso05] NISO Standards. "ANSI/NISO Z39.19 - Guidelines for the Construction, Format, and Management of Monolingual Controlled Vocabularies". 2005.

[NSH06] Choi, Namyoun, Il-Yeol Song, and Hyoil Han. "A survey on ontology mapping."*ACM Sigmod Record* 35.3 (2006): 34-41.

[OMCS11] Ontario Ministry of Community Safety & Correctional Services: English-French Emergency Management Glossary of Terms, December 2011, available at https://www.emergencymanagementontario.ca/english/emcommunity/response_resources/GlossaryOfTerms/glossary_of_terms.html.

[RaBe01] "A survey of approaches to automatic schema matching"

[Rey10] Reynolds, D.: An organization ontology, October 2010, available at http://www.epimorphics.com/public/vocabulary/org.html.

[RWP08] ReliefWeb Project: Glossary of Humanitarian Terms, August 2008, available at http://www.who.int/hac/about/reliefweb-aug2008.pdf.

[Su02] Su, Xiaomeng: "A text categorization perspective for ontology mapping"

[TRAD99] TRADE – Training Resources and data exchange: Emergency Management Issues – Special Interest Group – Glossary and Acronyms of Emergency Management Terms, Third Edition, May 1999, available at https://orise.orau.gov/emi/training-products/files/glossary-emt.pdf.

[WWW01] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): Glossar, available at http://www.bbk.bund.de/DE/Servicefunktionen/Glossar/_function/glossar.html?lv2=4968152, Access: 23.03.2016.

[WWW02] United Nations Environment Programme (UNEP), available at http://www.unep.org/resourceefficiency/, Access: 23.03.2016.

[WWW03] Australian Government, Attorney-General's Department, available at https://www.ag.gov.au/EmergencyManagement/Pages/default.aspx, Access: 23.03.2016.

[WWW04] Arizona Department of Health Services: Emergency Preparedness Glossary, available at http://www.azdhs.gov/als/childcare/documents/preparedness/emergency-preparedness-glossary.pdf

[WWW05] EM-DAT – The International Disaster Database – Centre for Research on the Epidemiology of Disasters (CRED): General Classification, available at http://www.emdat.be/classification, Access: 23.03.2016.

[WWW06] IDIRA Project, available at http://www.idira.eu/index.php/project, Access: 16.03.2016.

[WWW07] SECRICOM Project, available at http://www.secricom.eu/expected-results, Access: 16.03.2016.

[WWW08] FREESIC Project, available at http://www.freesic.eu/, Access: 16.03.2016.

[WWW09] http://www.eena.org/download.asp?item_id=167, Access: 23.03.2016.

[WWW10] http://crispproject.eu/, Access: 23.03.2016.

[WWW11] http://www.iai.it/sites/default/files/staccato_final-report-executive-summary.pdf, Access: 23.03.2016.

[WWW12] http://vocab.ctic.es/emergel/

[Zang76] Zangemeister, C.: Nutzwertanalyse in der Systemtechnik. Wittemannsche Buchhandlung Munchen, 1976

[Zimmermann et al. 2013] http://www.bridgeproject.eu/en/bridge-results/deliverables/d042