Secure Dynamic Cloud for
Information, Communication and Resource Interoperability
based on Pan-European Disaster Inventory

Deliverable 5.4 Validation report and final evaluation model of communication system concept

Final Version

Ivan Cucco[1], Simona De Rosa[1], Peter Grey[2], Bogdan Despotov[2], Christina Schäfer[3], Torben Sauerland[3], Katrina Petersen[4], Ioannis Danilidis [5], Paul Hirst [6]

T6 Ecosystems[1], CloudSigma[2], University of Padeborn[3], Lancaster University[4], Centre for Security Studies[5], British-APCO[6]

December 2016

Work Package 5

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	Restricted
Due date	30/12/2016
Sent to coordinator	13/12/2016
No. of document	D5.4
Name	Validation Report and Final Evaluation Model of Communication System Concept
Type	Deliverable
Status & Version	V1.0
No. of pages	145
Work package	5
Responsible	T6 ECO
Further contributors	CS UPB TUDO ULANC BAPCO KEMEA

Authors		Ivan Cucco, T6ECO Simona De Rosa, T6ECO Peter Grey, CS Bodgan Despotov, CS Christina Schäfer, UPB Torben Sauerland, UPB Katrina Petersen, ULANC Daniel Behnke, TUDO Ioannis Danilidis, KEMEA Paul Hirst, BAPCO		
Keywords		Validation, evaluation, common information space demonstrator		
History	Version	Date	Author	Comment
	V0.1	21/11/2016	T6 ECO	Draft sent to the internal review
	V0.2	13/12/2016	T6 ECO	Final version

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

Authors

T6 Ecosystems

Ivan Cucco

Email: i.cucco@t-6.it

Simona D Rosa
Email: s.derosa@t-6.it

University of Paderborn

C.I.K.

Christina Schäfer

Email: c.schaefer@cik.uni-paderborn.de

Torben Sauerland

Email: sauerland@cik.uni-paderborn.de

TU Dortmund

CNI

Daniel Behnke
Email: daniel.behnke@tu-dortmund.de

Mobilities.Lab

Centre for Mobilities Research

Department of Sociology

Lancaster University

LA1 4YD

UK

Katrina Petersen
Email: k.petersen@lancaster.ac.uk

CloudSigma

Bogdan Despotov

Email:bogdan.despotov@cloudsigma.com

Peter Grey

Email: peter.gray@cloudsigma.com

British APCO

Paul Hirst

Email: paul.hirst@bapco.org.uk

Center for Security Studies (KEMEA)

P.Kanellopoulou 4

1101 77 Athens

Greece

Ioannis Daniilidis
Email: i.daniilidis@kemea-research.gr

Reviewers

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

Catherine Easton
Email: c.easton@lancaster.ac.uk

University of Paderborn
C.I.K.

Christina Schäfer
Email: c.schaefer@cik.uni-paderborn.de

Executive summary

This deliverable provides an upgrade about activities foreseen and implemented within WP5. The deliverable starts from the methodology described in previous documents to validate and evaluate SecInCoRe's outcomes and impact, based on the combining of two well-established approaches, E-OCVM validation framework with SEQUOIA (a counterfactual evaluation methodology), but it then makes a step forward providing a detailed description of the activities performed so far in order to demonstrate project's outputs.

First of all, the deliverable provides a clear overview of the conceptual outputs of the project but, above all, it clarifies which demonstration implementations have been realised to make possible the demonstration of project's outputs. This clarification makes it possible to trace the work done for Demonstration Cases because it makes visible which of the conceptual outputs can be shown to the end-users in order to validate and evaluate.

The current description of demonstration implementations described in the first chapter is particularly relevant also for methodological issues, described in the following chapter. This is due to the fact that having a clear idea about how to implement Demonstration Cases, it makes it easier to define the whole process for validation and evaluation.

Thanks to this step forward, it has been possible to define the final version of the methodology that will be used until the end of the project. Methodology refinement has been achieved in multiple Pilot Demonstration Cases. Pilot Demonstration Cases have been reported in the current document in order to show the work of refinement of the methodology based on end-users' feedback and the state of the art of the outputs. The refinement has been performed in the continuous adaptation of the tools defined in the methodology in order to choose the more proper ones and on the final definition of High Level Requirements and indicators to take into account when validate the different components.

The entire process allowed the project partners to perform the first validation case, applying the established methodology and collecting results from the end users. Such results will be soon followed by the next round of validation and evaluation activities that will be then described in the final deliverable of WP5. For the moment, in this document has been reported what was possible to learn from past activities and how such lessons will be implemented and integrated in further Demonstration Cases. In line with this a timeline containing all demo cases that will be performed until the end of the project has been reported to give an idea of the work that will be achieved in the remaining time of the project.

Furthermore, the deliverable contains another crucial point very much related to the validation and evaluation activities, namely a reflection on the stakeholder's engagement within SecInCoRe. The whole strategy for validation and evaluation has been clearly based on the engagement of end-user experts in the field; however, the stakeholder engagement is not an easy task, so in order to have a more clearer idea of what have to be done to improve the upcoming actions foreseen by the project, some reflections and guidelines have been provided.

To conclude, the entire deliverable reports the stage of the art regarding the WP5 from several perspectives. The deliverable puts in evidence the state of development of the demonstrator implementations explaining from the point of view of projects partners in charge of the activities the state of the art of the implementation. Then, it gives clear indication about the work of validation and evaluation performed so far and about what still has to be performed.

Then, it also contains a reflection on the stakeholders and their participation on the past and future project's activities. In line with this the deliverable has seen a strong collaboration among almost all project partners putting in evidence that validation activities are strongly related both to partners in charge of technical and conceptual development and to partners in charge of relations with stakeholders. Thanks to the common effort, validation and evaluation strategy has been defined in its final version, has been applied to a first Demonstration Case and will be further implemented in the upcoming cases.

Table of contents

1 Introduction

SecInCoRe envisages a Common Information Space (CIS) for cooperation and collaboration among all relevant stakeholders in all phases of crisis management, and particularly on preparedness and training. This is based on an intense interoperability analysis focusing on first responder organizations and Police authorities. A strategy for the validation and evaluation of SecInCoRe expected outcomes and impacts through Demonstration Cases has been formulated as part of the project (see Deliverable 5.3). In the course of the last months, the SecInCoRe Validation and Evaluation Strategy (VES) was tested and fine-tuned. Indeed, in order to prepare the validation for Demonstration Cases, three Pilot Demonstration Cases have been performed. It was then applied in a first Demonstration Case in late October 2016, in the course of which a sub-set of components of the SecInCoRe concept (primarily the Taxonomy, Ontology, and Knowledge Base) was validated with end-users from Germany and Poland.

This deliverable reports on the results of these activities. Its aim is twofold: firstly, we explain how the VES was modified to consider the status of the conceptual tools and technical implementations that can be used in Demonstration Case to present different elements of the SecInCoRe concept to end-users; secondly, we report the results of the first validation activity conducted in Paderborn in October 2016. Based on these results, we derive recommendations and lessons learned for future Demonstration Cases and present the plans for the validation and evaluation activities that will be organized in the following months.

The deliverable is structured as follows:

Chapter 2 explains how different elements of the SecInCoRe concept were presented to users in Demonstration Cases. The chapter describes the technical implementations (Reference and Demonstrator Implementations) as well as the conceptual tools (such as presentations and mock-ups) that were used to include in Demonstration Cases those elements of the concept for which technical implementations were not available.

Chapter 3 summarizes the key elements of the SecInCoRe VES, explains the process behind the organization of a Demonstration Case and details the techniques, methods and indicators used to validate individual components of SecInCoRe.

Chapter 4 reports on the progress made during the three Pilot Cases in which the instruments developed for the VES (questionnaires, observation frames, semi-structured interview scripts, Demonstration Case templates) were developed, tested and refined.

Chapter 5 presents the results of the first Demonstration Case dedicated to the validation of elements of the SecInCoRe concept (including the Taxonomy, Ontology and Knowledge Base) through both conceptual tools and through end-users' interaction with the Semantic Search Function integrated in the demonstrator.

Chapter 6 discusses aspects related to stakeholders' engagement to clarify the work done by the project, summarizes the main impressions collected from stakeholders and derives recommendations for improving stakeholders' engagement in the following months.

Chapter 7 describes the plans for final validation and evaluation activities that will be organized before the end of the project and make some reflections on the most relevant issues that should be taken into account for future demonstrations.

1.1 Purpose of this document

This deliverable documents the final strategy for the validation and evaluation of SecInCoRe's results (DoW, T5.2). The validation and evaluation strategy will refer to different elements of the SecInCoRe CIS concept using the CIS concept specification presented in Figure 1. As described in D4.2, the CIS concept includes non-technical concept and technical elements, and its specification includes three main sections: CIS specification, Reference Implementations and demonstrations.

- CIS specification. The CIS specification is articulated in two main modules: the CIS concept with a socio-technical focus, that is mainly non-technical; and the Cloud Emergency Information System (CEIS) concept, with a technical focus.
- Reference Implementations. The CIS concept relies on specific types of IT systems and components being defined as part of the CEIS. Therefore, the implementation of the CIS concept implies the need to create technical components of this type. Reference Implementations are independent from specific applications and are driven by technological capabilities. They are developed to simplify access and lower barriers for uptake of the concept, and are meant to be installed and adapted to specific communities of users. Section 2.1.2 in this Deliverable describes a sub-set of Reference Implementations that have been adapted to the needs of different Pilot Demonstration Cases and Demonstration Cases.
- Demonstrations. SecInCoRe uses Demonstration Cases as part of the validation and evaluation methodology defined in WP5. For each Demonstration Case, a set of Reference Implementations are adapted to a specific scenario or community (subsuming a subset of the addressed users and specific purpose). Technical components of the CIS concept might be extended by non-technical CIS elements on a case-by-case basis. The aim of D5.4 is to explain how Demonstration Cases are built and how different components are validated.

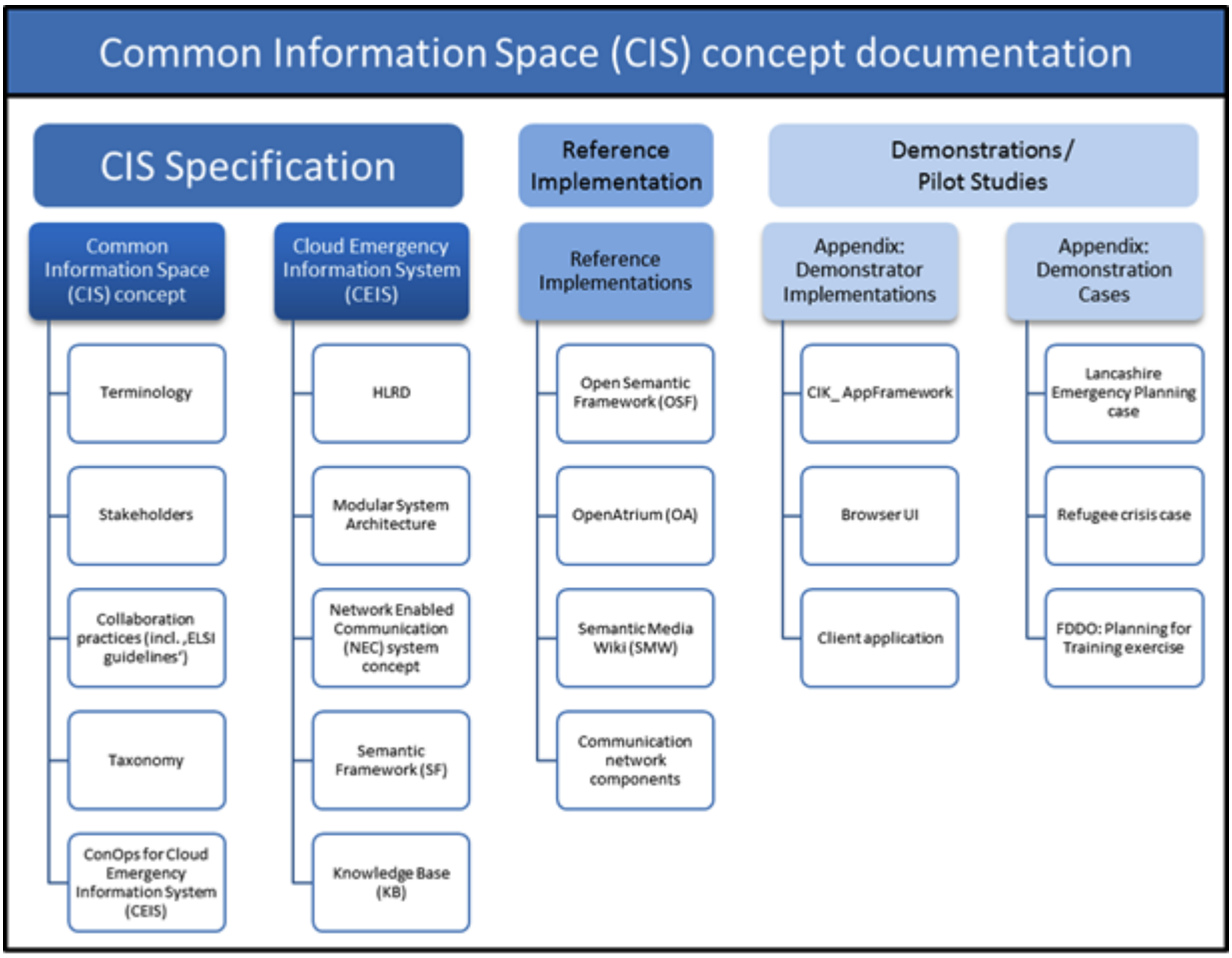


Figure 1. Structure of Common Information Space Specification and Documentation

1.2 Validity of this document

This deliverable summarizes the strategy designed for the validation and evaluation of SecInCoRe's outcomes and impacts, and explains how the strategy has been revised to take into account project progress and achievements to date. The instruments, methods and indicators used for validation and evaluation purposes have been tailored to the activities that can be realistically organized during Demonstration Cases, considering the current status of technical and conceptual implementations of different elements of the SecInCoRe CIS concept. Instruments, methods and indicators may be further improved or modified in response to future developments in SecInCoRe technical and conceptual demonstrators. The document reports on the activities performed in Pilot Demonstration Cases and on the subsequent refinement of the validation and evaluation strategy; describes the results of the first validation activity; and provides a timeline for the next steps of validation and evaluation.

1.3 Relation to other documents

This deliverable relates to the following foreground documents in the project:

[1] Grant Agreement (no. 607832) and Annex 1. - Description of Work
[2] Consortium Agreement

[3] D3.3 (WP-3) – Second publication of Inventory results including ethnography and holistic process models and statements on future evolutions
[4] D4.3 (WP-4) – Network enabled communication system concept and common
D5.2 (WP5)- Validation
[5] D5.3 (WP5)- Validation Strategy
Outputs:
[6] D.5.5 (WP-5) – Evaluation and Validation report for SecInCoRe stakeholders [in the form of T5.5 input to T6.3]
[7] D6.3 (WP-6) – Report and Evaluation on new Business Models [in the form of T3.4/T3.3 input to T6.4]

1.4 Contribution of this document

The SecInCoRe 'Common Information Space' concept is based on a 'Pan-European Inventory'. This deliverable contributes a final description of the strategy that is adopted for the validation and evaluation of project achievements and expected impacts. More specifically, the deliverable contributes to the understanding of results of the project's meetings and workshops in order to organize final validation activities. For these reasons, this deliverable is linked transversally to all the Work Packages.

1.5 Target audience

D5.4 is a restricted document and it is mainly addressed to the SecInCoRe project consortium and to the European Commission (EC). Since all project partners are engaged in validation and evaluation activities, it is important for them to be aware of the requirements, processes and objectives of the validation and evaluation strategy and to consider the indications provided in this deliverable when planning future development activities. In addition to this, the deliverable also intends to provide the EC with a summary of the activities performed to date, explaining in detail how validation activities were organized according to conceptual and technical project implementation.

1.6 Glossary

Abbreviation	Expression	Explanation
3GPP	3rd Generation Partnership Project	System for professional mobile radio
AAA	Authentication, Authorization and Accounting	Abbreviation is used as a description of a concept component and linked to security issues
AAA / IDM	Authentication, Authorization and Accounting and Identity Management solutions	Description of a demonstrator linked to security and management issues
AB	Advisory Board	Advisory Board defined within the

		consortium
CBRNE	Chemical, Biological, Radiological and Nuclear Defense	Protective measures taken in situations in which chemical, biological, radiological or nuclear warfare (including terrorism) hazards may be present
CEIS	Cloud Emergency Information System	Emergency information system which can be accessed via internet.
CIS	Common Information Space	Service-oriented software framework facilitating complex systems
CNBOP-PIB	Centrum Maukowo-Badawcze Ochrony Przeicwopozàrowy	National Polish Institute for research on fire protection
CONOPS	Concept of Operations	Abbreviation is used as a description of concept components
CPDP	Computer Privacy and data Protection	Conference dedicated to the topics of Computers, Privacy and Data Protection
DCP	Demonstration Case Protocol	Protocol for designing and planning Demonstration Cases for validation and evaluation purposes
DCT	Demonstration Case Templates	Standard Template designed as part of the validation and evaluation strategy for gathering information and to structure demo cases
DOW	Description of the Work	The description of SecInCoRe project as it has been approved by the EC.
E-OCVM	European Operational Control Validation Methodology	Methodology provided by an European project for validation activities
ELSI	Ethical legal social issues	Ethical and social challenges and opportunities that arise in emergency situations, especially with a view to the use of ICT. Legal issues arising, particularly around data protection, liability, and responder safety
EU	European Union	Supranational Institution

FDDO	Fire Department of Dortmund	Fire brigades operating in Dortmund in a dedicated Unit
HLR	High Level Requirements	Conceptual references for building the CIS
IT	Information Technologies	Application of computers and internet to store, retrieve, transmit, and manipulate data or information
KB	Knowledge Base	A Knowledge Base (KB) is a technology used to store complex structured and unstructured information used by a computer system. In the SecInCoRe context the Knowledge Base is the technical representation of the Inventory
LDAP	Lightweight Directory Access Protocol	Server for identity management solutions
LRF	Lancashire Local Resilience Forum	Multi-agency partnerships made up of representatives from local public services that aim to plan and prepare for localised incidents and catastrophic emergencies
NEC	Network enabled Communication	Abbreviation is used as a description of a concept component and contains everything dealing with communication infrastructure and technical solutions in this field
OA	Open Atrium	Platform for enhancing sharing and collaboration
PPDR	Public Protection and Disaster Relief	This expression compromises the domain of all first responder and police authorities and is used in literature
SEQUOIA	Socio-Economic Impact Assessment for Research Projects	Methodology for impact assessment provided by the Sequoia European project
UI	User Interface	User Interface is the interface for machines and software with the aim to maximize usability and user experience
VES	Validation and Evaluation Strategy	The strategy designed and implemented to validate SecInCoRe's outcomes and evaluate its expected impacts.

WP	Work Package	Work packages are defined steps in the DoW (see above) in order to achieve the project objectives

1.7 List of figures

1.8 List of tables

2 Common Information Space Demonstrator: Second Version

2.1 Introduction to SecInCoRe validation methodology

As described in deliverables D5.2 and D5.3, a methodology for the validation and evaluation of SecInCoRe outcomes and impacts has been developed within WP5. The SecInCoRe Validation and Evaluation Strategy (VES) combines elements of the E-OCVM methodology for the validation of outcomes, with elements inspired to the SEQUOIA methodology for the evaluation of impacts (Figure 2). Since SecInCoRe is conceptualized as a socio-technical system, the VES is based on the crucial interaction between project outputs and end-users' practices; this strategy is inspired to the E-OCVM case-based approach to validation. For this reason, the SecInCoRe VES is centered on Demonstration Cases. During a Demonstration Case, end-users are introduced to and (to the extent made possible by the status of technical implementations) interact with selected elements of the SecInCoRe concept in a structured manner that permits the systematic collection of data and their comparison and aggregation across different Demonstration Cases.

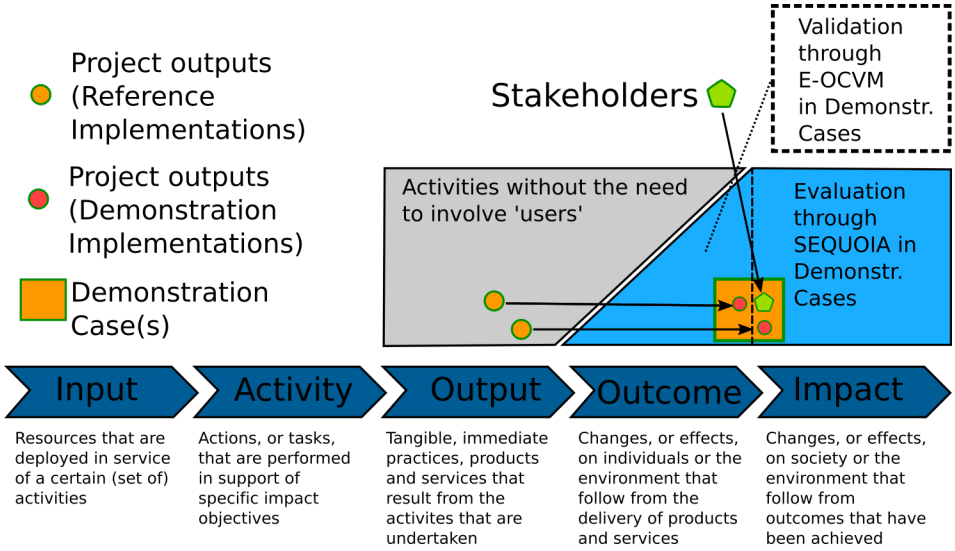


Figure 2. The Impact Value Chain, Demonstration Cases and validation / evaluation strategy

The SecInCoRe VES follows a multiple-case embedded design (Yin, 2003) based on the aggregation of evidence collected from Use Cases embedded in multiple Demonstration Cases. The multiple-case design has been selected in order to increase the external validity of results through logical generalisation based on a cycle of hypothesis generation – experiment - hypothesis generation[1]. The feedback provided from the analysis of Demonstration Cases is

[1] In the context of a Demonstration Case and its embedded Use Cases, the hypotheses to be tested are formulated on the basis of the High Level Requirements identified for the SecInCoRe project. In this sense, a Demonstration Case ultimately aims at testing whether the CIS concept developed in SecInCoRe (and the

also used to improve, where needed, the design of Reference and Demonstrator Implementations, to refine the SecInCoRe CIS concept and revise its High Level Requirements in response to end-users' needs and practices. The input generated from the evaluation of socio-economic impacts will eventually assist in the creation of business cases and business models that can favour the adoption of SecInCoRe and increase its sustainability.

Demonstration Cases are based on the deployment of Demonstrator Implementations (i.e. working prototypes of different elements of the SecInCoRe concept created through the adaptation of Reference Implementations) and non-technical representations of the SecInCoRe concept (such as presentations, stories and mock-ups) in a workshop setting organized around a realistic scenario co-designed with end-users to reflect their interests and practices (Figure 3). Whenever possible, depending on the status of Demonstrator Implementations and their evolution during the project life-cycle, Demonstration Cases are organized in a way that:

- permits end-users to experience the potentialities of a Common Information Space (CIS) designed according to SecInCoRe core principles; and
- allows them to perform guided practical activities (Use Cases) that entail their interaction with the available technical implementations of different elements of the SecInCoRe concept.

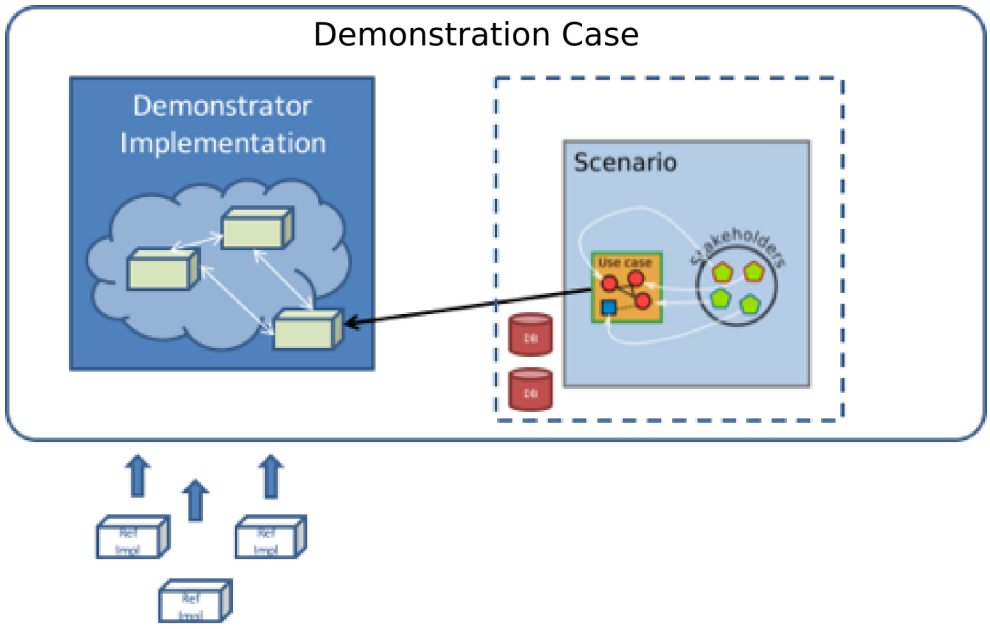


Figure 3. Relation between Demonstration Cases and Demonstrator Implementations

The case-based approach adopted for the SecInCoRe VES requires therefore the creation of multiple Demonstrator Implementations based on the adaptation of Reference Implementations[2] to the specific scenarios and use cases designed with the involvement of end-

translation of some of its elements in Reference Implementations) is able to achieve its intended aims (outcomes and impacts).

[2] Reference Implementation are used to implement concepts of the CEIS.

users for each Demonstration Case. For this reason, a specific task within the project is dedicated to the adaptation of Reference Implementations to generate Demonstrator Implementations that respond to the specific needs of each Demonstration Case. The aim of the following section is to describe the results of these activities and to introduce the demonstrators (both Demonstrator Implementations and non-technical tools such as presentations, mock-ups etc.) that are currently available for use in Demonstration Cases. Each of the following sub-sections is dedicated to the elements of the SecInCoRe concept that have been identified as candidates for validation during the last two project plenary meetings: CIS concept, Inventory, Knowledge Base, Taxonomy, NEC, and collaborative practices including ELSI.

In Chapter 3, the limits that the status of technical and non-technical demonstrators pose to what can be validated in a Demonstration Case will be discussed, and the tools utilized for the collection of data for validation and evaluation purposes are described. Since the participation of end-users is a key element of the case-based approach, Chapter 6 discusses the aspects related to stakeholders' involvement in Demonstration Cases.

2.2 An introduction to the CIS concept

A CIS is a space created by the interactions of diverse stakeholders as they approach a problem from different perspectives, angles, and layers. The concept of a CIS is more than just its parts, a technology through which to share information, or a platform for collaboration. They are systems that are continually emerging in and through socio-technical collaboration practices that emerge from a joint necessity and mutual interdependence (not from an "I need what you have interaction"), such that there is an allocation of accountability, which is more than just the need to share each other's resources.

SecInCoRe aims to conceptualise or help produce CIS-relevant services, tools, and infrastructure which can support inter-agency, cross border, and Pan-EU collaboration in Emergency Management (Pottebaum et al., 2016).

A Common Information Space: facilitates cooperative work. Doing so, it must enable a sense of shared or commonality between user understandings that does not result in one person reducing their understanding to the other (see D2.2). This is vital because a willingness of stakeholders to share information is not enough to support collaboration because of the different types of expertise of those interacting. Instead, they need to be able to also establish a common ground through which to interact.

In addition, CIS facilitates the alignment of different interpretational frames. Without the understanding of different contexts in which information is produced and the concerns of the different originators, incorrect inferences are likely to be made (Bannon and Bodker, 1997).

Supports meaning (not just data) in a way to be moveable from one place/context to the next in ways that support not changing it in ways to make data mean other than intended (to help make sense of and trust between the different infrastructures, languages, methods, etc. so not completely dissociable form the site of production) (see D2.4).

Requires the ability to defend points of view. This is because cooperative work involves incommensurate perspectives (professions, specialties, work functions, responsibilities) as well as incongruent strategies and discordant motives (see D2.4).

This is because cooperative work is not facilitated simply by the provision of a shared database. A functioning CIS, then, requires participants actively sharing, debating, and – at least temporarily – resolving meaning so that a common language can be used, even if users have different backgrounds and use the same terms with other meaning at other times (Schmidt and Bannon, 1992). This also requires the need for supporting smooth (but visible) ways of achieving openness and continuing renegotiations regarding what information means, who is allowed to access it, and what it may be used for (Kuhnurt et al., 2015). In general, the production of a common understanding can be supported by Taxonomies and Ontologies help both identify and establish how words are being used to facilitate exchange, translation, and thus successful communication.

Moreover, all CISs are influenced by different modes of governance external and internal to the system, as well as different modes of sustainability. They need to create a balance between the collaborative, institutional, societal, economic context, need for experts, and public trust. While the above elements and concepts describe components vital to the functioning of a CIS; what makes for a CIS, as a whole, is how and to what they all work together. CISs can be stable or need to be able to support short-lived arrangement and the constant need for re-negotiations (Rolland, Heps and Monteiro, 2006)

As already reported in D2.4, this means that data within a CIS is used to:

- Construct peripheral awareness and at a glance overview.
- Defend points of view.
- Persuade and educate others.
- Privilege different uses.
- Build and lose stakeholder legitimacy.
- Do things in unintended ways.
- To develop new, appropriate frames for the combined data.

Data within a CIS needs to:

- Be flexible enough to change use and reading depending on circumstances and goals.
- Provide interpretive context.
- Create enough commonality between data to allow for translation and portability.
- Be entered with a reflexivity towards thinking about meaning of information for the different groups involved.
- The SecInCoRe CIS concept is described in D4.2 and the visualization of the concept will reviewed in D4.4.
- Using and presenting elements of the SecInCoRe concept in demonstration cases

There are two approaches to build up demonstrators based on the CIS concept described above:

- Presenting end-users with conceptual representations based on the CIS concept documentation. Under the web portal at www.secincore.eu/cis-concept the overall concept is documented and described. Rules for defining the content was given in D4.2.
- Showing the benefits of the CIS concept for specific end user, by using a combination of Demonstrator Implementations (e.g. Semantic Search, Collaborative Platform, see also parts of the description in paragraph 2.4).

As part of Demonstrator Implementations there is the need to select elements from the concept to demonstrate the overall benefit and build up several Demonstrator Implementations. The following two sections describe, respectively:

- the Demonstrator Implementations that end-users have utilized to date in Demonstration Cases (Knowledge Base and Semantic Search);
- other elements of the CIS concept that have not yet been directly used in Demonstration Cases because the process of adaptation to the needs of Demonstration Cases is still ongoing (Collaborative Practices and ELSI guidelines; OpenAtrium), or elements that, although shown to end-users in previous activities, are not envisioned as candidates for further validation activities with end-users since they will undergo an internal verification process (the Network Enabled Communication System)

2.3 Description of demonstrator implementations already used in pilot and Demonstration Cases

This section starts provides a detailed description of the demonstrator implementations utilized to date in Demonstration Cases; they include the Knowledge Base and the Semantic Search. Each Demonstrator Implementation is a customization of the respective Reference Implementations. The customized demonstrator implementations are designed to fit the specific needs of the Demonstration Cases they should support. Below, the underlying Reference Implementations are explained very briefly. Afterwards the changes which are done to customize the Reference Implementations into Demonstrator Implementations are described.

2.3.1 Knowledge Base

Reference Implementation:

The Knowledge Base is the technical implementation of parts of the Inventory. It contains a data layer including different data sources, like data bases, filesystems, etc. and a semantic layer derived from the Taxonomy to define relations between various data. Figure 4 demonstrates the overall approach of the Knowledge Base.

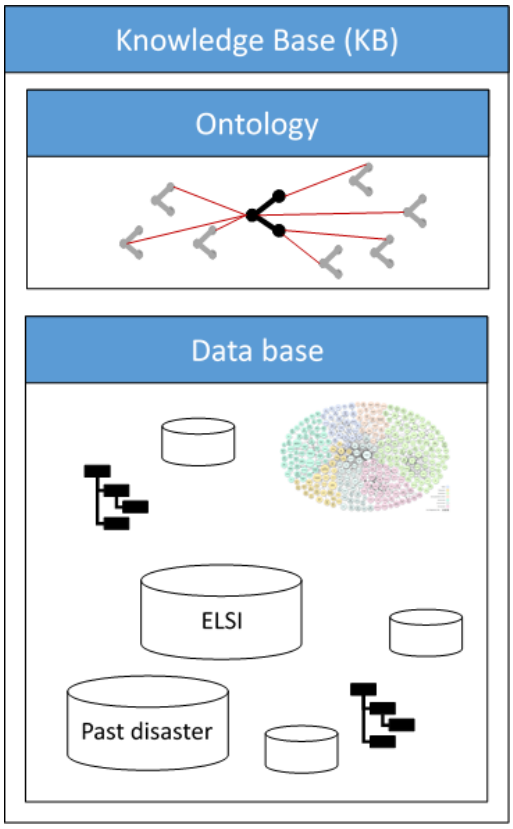


Figure 4. SecInCoRe Knowledge Base approach

The structure of databases with regard to the Knowledge Base will be published in D3.4.

Data layer

Reference Implementation:

The SecInCoRe Inventory as the underlying concept of the Knowledge Base is addressed in a twofold way: first from a WP 2 perspective - gathering past disaster and existing crisis management models. Here, a comprehensive overview about past incident is documented especially in D2.1 and gaps of existing databases of past disaster are shown in D2.5, e.g. the need to include lessons learned in the description of past disaster.

The WP 3 perspective aims to collect knowledge about data sets, processes, information systems and business models used by first responders and Police authorities. For each item separated databases are developed and included in the Knowledge Base. They are accessed in the Demonstration Cases mainly using the Semantic Search, which offers a consolidated view on all Knowledge Base contents.

Demonstrator implementation:

Nevertheless, as part of a demonstrator implementation the Knowledge Base and further the Inventory changes depending on the defined Demonstration Case – identify relevant data bases and files to be included or deepening the structure of the Ontology in a specific way to consequent target the respective Demonstration Case.

The Knowledge Base therefore grows with every Demonstration Case. It is expanded every time with fitting content, i.e. for the Paderborn case, information about past CBRN incidents was added. Another example for information added are Training plans for special incidents and documents, the participants are familiar with.

Semantic Layer

Reference Implementation:

To use the Taxonomy (described in D4.3 and D4.4) in Reference Implementations, parts of it are realised in the Ontology and e.g. used in the Semantic Search. The Ontology is part of the Knowledge Base. Its conceptual background is given by the Taxonomy. The Taxonomy in SecInCoRe manner is a non-technical conceptualization of different PPDR domain relevant items and terms.

Demonstrator implementation:

In relation to a Demonstration Case it is needed to deepen the Ontology in a specific direction or to integrate further existing ontologies to be concrete enough for a respective case.

These customisations are on the one hand on a conceptual level, but mainly on an implementational level, where the displayed thematic range as well as the ways to explore the Ontology are modified. The Ontology itself is deepened using input and lessons learned from Demonstration Cases. For example specific relations are proved for consistency by participants, the general way to use the Ontology is evaluated and specific topic ranges as pandemic incidents are detailed.

2.3.2 Semantic Search

Reference Implementation:

The Semantic Search, the Reference Implementation to access the Knowledge Base, contents, using the Semantic Framework concepts. The search uses the Ontology to refine search results in accordance to the respective user.

Demonstrator implementation:

To customise the Semantic Search for specific Demonstration Cases, there are several changes possible. Besides design adjustments as fitting logos and appropriate labeling, the available sub-pages could be customized as well as the search itself.

The sub-pages contained in the Reference Implementation (the search itself, database views, Upload pages etc.) are modified for each Demonstration Case. For every case only the relevant sub-pages are shown, to avoid distracting the user from the important content.

The search itself is customized, editing mainly:

- Organisations: Which organisations should be mentioned as contributing?
- Authors: Which authors should be added to make the case realistic?
- Restricted documents: Which documents should be restricted, to fit the needs of the case?
- Categorisation of specific documents: Are there documents, which should be categorized in a special way?

After that the customization of the Knowledge Base content influences the Search demonstrator implementation, too.

Some Demonstration Cases urge the development of new functions (e.g. the "Edit" function for the Paderborn Demonstration Case), which are implemented for the specific case, but are directly transferred into the Reference Implementation.

*2.4 **Description of other elements of the CIS concept***

2.4.1 Collaborative practices and ELSI

Collaboration implies different organisations and/or individuals working together to achieve a common goal. Collaboration is enacted through various practices, including: seeking out and finding partnerships, communication and interaction, identifying and defining a common goal, allocation of responsibility, organisation and leadership, cooperation and sharing data, information, and resources (etc.), mutual learning, compromise, and more. Collaboration can be long-term or short-lived; it can be done face-to-face and, increasingly, with the advent of new Internet and communications technologies (ICT), at a distance. Vitally, though, there is no omniscient body that knows all in a collaboration.

In the context of SecInCoRe, the collaborating organisations/individuals are conceptualised primarily as public protection and disaster relief (PPDR) stakeholders, who share the common goal of providing European citizens security from and in times of disaster. Collaboration between these stakeholders is hindered for numerous reasons, including, but not limited to: different understandings of the 'common' goal (e.g. different risk analysis, priorities, etc.), cultural contexts, geographical distance, languages, inter-agency distrust, legal concerns.

In general, collaboration is built upon:

- The idea of sharing as the production and distribution of information resources
- Clarity in motivations for sharing, as they can range from power/access to community building.
- The recognition of familiar problems.
- Collaborative practices of articulation work and configuring awareness.
- Support for the negotiation of tensions over sense of information control
- Participation, not dissemination. "I share with you" does not make for collaboration.
- Seeing legitimacy in others' work. This emerges when each element in a communication process offers a solution to a problem of another actor in a multi-directional inter-dependant way.
- Engaging differences. Just knowing about differences can often increase silo-ing, instead of increasingly collaboration.

Within a CIS, this specifically means:

- Support the strategic use of data to be written into how data is shared. For example, each time an incident log is shared the networks of collaboration become increasingly stable. As stability increases, so too does trust (D2.4)
- Support establishing structures that that let stakeholders know they are appropriately combining different data from different sources, that enable heterogeneous groups define and pursue shared goals.

- Support the arrangement of new methods for gathering information, new classification schemes to identify what is important about a situation, and new methods for making it common.
- Support the creation of enough commonality in data to allow for translation and portability in order to reduce this risk of misinterpretation, even if just a temporary commonality.
- Support diverse actors in new situations in seeing new problems as familiar.
- Not enable an omniscient agent, as they are none in cooperative work in non-technical settings.
- Support active and peripheral awareness of others activities
- Support articulation work, in which people dovetail the work: divide, allocate, coordinate, schedule, interrelate. These are extraneous to the specific tasks being accomplished by the collaboration but necessary for the collaboration to work.

It relies on mechanisms for interaction (such as maps, schedules, etc) that support the often conflicting politics of information, of control and sharing.

Configuring awareness: managing where others attention is focused in a way that it might be possible to affect (to configure) where the others focus is for the sake of sharing information.

2.4.2 ELSI guidelines

In order for digital and cloud-based tools for information sharing and interoperability to facilitate collaboration and increase interoperability, while not producing new risks, requires being aware of and having strategies for dealing with complex ethical, legal, and social issues (ELSI). These new tools hold considerable opportunities for collaborative disaster management and response. Their effectiveness depends on how they are designed, governed, and used in accordance with diverse ethical, legal, and social issues.

In order for the potential risks to be mitigated, first they need to be reflexively understood and, second, need to be addressed through concrete design, governance, and use policies and practices. These guidelines seek to help designers, managers and users of these tools, at the institutional/hosting level, understand how their implementation of these new tools have transformative potential, to enable transformations which are ethically, legally, and socially sensitive and proactive.

In so doing, the guidelines aim to support the development of ELSI reflexivity - that is, to become more aware of how ELSI both inform and are informed by the design, governance, and use of such tools - and offer constructive strategies for dealing with ELSI as they arise.

In particular, these guidelines focus on how ELSI inform and are informed by common information spaces (CISs) in the domain of public protection and disaster relief (PPDR) and risk governance. CISs are socio-technical systems which are produced in and through Collaboration Practices, such as sharing data/information, cooperating, negotiation, discussion, finding new partners, which are enabled and shaped by technical and organisational infrastructures. The Guidelines are directed at those would establish and implement a CIS.

The Tables below (from Table 1 until Table 9) explain how ELSI guidelines are related to different elements of the CIS and to SecInCoRe collaborative goals, and describe their actual or planned representation in Reference Implementations.

CIS Element	Key ELSI guidelines	SecInCoRe Collaborative Goals	SecInCoRe Innovations	Implemented in the RI
Stakeholders	Inclusiveness	Support finding and establishing new partnerships.	Include within meta data standards for system/document use access to information about author and contact information.	Ability to click on authors and to send a secure note through the system. Ability to connect through the NEC and collaborative platform.
		Support ways of finding counterparts in other regions	Tags for personal data that support tasks/duties/goals to see role differences and similarities. Support in seeing how others classify their own documents in relation to yours.	The ability to edit and define own meta-data for document. The ability to edit personal meta data linked to login/contact. Search via Ontology
		Support ways of seeing common goals and the relevance of different goals.	Put different ways of classifying risks, disasters, and security issues into conversation with each other.	Clicking on a category in the graph view will reveal the range of documents and their meta-data that also are connected to it (supposed to be implemented)

		Managing different professional and cultural languages	Ability to see value in a document without a full translation.	Situating documents in the domain relevant Ontology Translating keywords and abstracts into English
	Engaging with Diversity	Maintain local and regional variations	Scalability of the system and CIS	Ability to edit and revisit the high level goals, as supported by the governance documents.
		Controlled access	The system acknowledgement that trust and security sometimes come from not sharing everything with everyone. Having the ability to limit access at times is part of having a system that can support diversity A CIS that includes enough structure to enables consistency, but with enough flexibility to deal with unforeseen stakeholders or unpredictable contexts that ask for new or modified value systems.	Layered of access to documents with the Knowledge Base. Ability to add in new users or remove old users and reset NEC groups without losing connectivity

		Support ways of negotiating interoperability	Developing open source tools that work between a variety of systems and data sets, based on an Inventory of data sets and information systems and flows.	Open source and editable systems to be personalised to the individual systems in which they will be used. Governance guidance that requires discussion of the ELSI of different interoperability choices.

Table 1. CIS and stakeholders

CIS Element	**Key ELSI guidelines**	**SecInCoRe Collaborative Goals**	**SecInCoRe Innovations**	**Implemented in the RI**
Terminology	Engaging with Diversity	Support bridges across diversity that do not erase diversity.	System managing multiple languages instead of requiring all to work within one single language. Visual connections between terminology	Automatic language translations that can be edited by users with editing user profile documented for others to help their interpretations). Graph search based in Taxonomy

Table 2- CIS and terminology

CIS Element	Key ELSI guidelines	SecInCoRe Collaborative Goals	SecInCoRe Innovations	Implemented in the RI
Collaboration Practices	Avoiding Fragmentation	Support negotiability in communication	Making one-way communication difficult so that the CIS does not become, by default, a space for the dissemination of facts, but rather becomes a space of negotiation	Multiple two-way, many-way forms of communication, both real time (e.g. collaborative space) and over time (traceable edits to meta data or ways of tagging points within documents)
		Allow for differences in interpretation to be visible and contestable.	Mutually accessible data. Meta data that supports seeing differences in meaning attributed to that data by the various actors involved.	Automatically produced meta data and user editable keywords.
		Create awareness of how a given standard/ technology affords uneven power.	ELSI guidelines that ask questions to encourage a heightened awareness of who will enable an effective and efficient response, who has the necessary data, and who would benefit from share data.	ELSI guidelines chapter

	Right to be Forgotten	Design support for people to understand what exceptions might apply, work out whether exceptions apply	Ability to see data stored in relation to self and request it to be deleted	Ability to delete personal data within the system.
	Data Protection	Clarity on who has the rights to the data; who is responsible for it; how long can it be assured; what happens when it is breached. Critical considerations about what does data security secure.	ELSI guidelines that ask questions to encourage a heightened awareness of who will enable an effective and efficient response, who has the necessary data, and who would benefit from share data.	ELSI guidelines chapter Ability to see who is responsible for given data-set and when looking at the data set.

Table 3. CIS and Collaboration Practices

CIS Element	**Key ELSI guidelines**	**SecInCoRe Collaborative Goals**	**SecInCoRe Innovations**	**Implemented in the RI**
Taxonomy	Contextual Reasoning	Support users to understand how data is given different meanings in different contexts by different users, and how	Information about others' contexts, especially through the Knowledge Base.	User meta-data accessible to all with access to system. Collect user meta data be less about the individual and more about what

		this relates to their own context and given meanings.	Collect User Terminology and put in relation to each other	they do with data and why. Visualisation tool, highlighting how one's document is related to others.
	Articulation Work	Support users verbal and non-verbal communication in order to document what they are doing, what they understand about what they are doing, and how this relates to others. Provide sense of disciplinary context over time that can help think about a bigger picture within a familiar frame of action.	The system should have functions that allow users to freely negotiate task allocation and articulation. That is, the system should provide multiple alternative channels of interaction. Should aim at supporting self-organization of cooperative ensembles as opposed to disrupting cooperative work by computerizing formal procedures. Cooperating actors must articulate (divide, allocate, coordinate, schedule, mesh, interrelate, etc.) their respective activities.	The range of direct communication tools provided in the system. The range of editing and commenting tools provided in the system. The ability to tag within documents why something was useful The ability to edit keywords, but have the edit directly linked, visible to all, to the editing users.

Table 4. CIS and Taxonomy

CIS Element	Key ELSI guidelines	SecInCoRe Collaborative Goals	SecInCoRe Innovations	Implemented in the RI
ConOps	interoperability	Support ways of developing mutually agreed upon standards for cooperation and responsibilities.	Provide tools for being aware of different data types, scales, resolutions, frequencies. Provide tools to help support necessary translations. Provide tools for uninterrupted sharing. Provide tools for filtering data so a user does not end up in the situation of too much data, and different roles need different data. The MOUs between groups help determine who is responsible for collecting and sharing data with who else. Support ways of seeing different national interpretations of command and control models	NEC Search Filters Various Access levels Governance document support ELSI Guideline Chapter Tools for finding counterparts in other countries. Tools for comparing information flows and crisis management models as collected in the KB.

	Right to be Forgotten	Support ways of smoothly ending collaboration	'Nuclear Option'	Ability to delete user profile (and with that system access) without contestation.
	Aligning Data Quality	Have technology aligned with the problem to begin with (which is always a moving target) Aligning local meaning-making practices (which are diverse and not always reconcilable)	Make it possible to flexibly work with the tools Include in the meta data how and why any given data was gathered, including what it is used for, how and why it was derived, and how it fits with other information it is being used with.	Open Source/Modular
	Accountability	Balancing tracking and surveillance with right to anonymity and autonomy	Make what is tracked transparent to a user and delete-able at their request. Provide mechanisms to contest the recorded use histories. Too much tracking can discourage collaboration and system use.	Guidance to this in the governance documents, this is up to the hosts to determine, as different ways of tracking are possible with the system, and at minimum logging in to search the KB, to the collaborative platform, and to the NEC are stored and traceable. But depending on wether the CIS is local, national, EU, there are

			If tracking is done, users need to be aware of which practices they could be held accountable for.	different legal and regulatory issues to be dealt with so not a single solution to the issue.

Table 5. CIS and ConOps

CIS Element	**Key ELSI guidelines**	**SecInCoRe Collaborative Goals**	**SecInCoRe Innovations**	**Implemented in the RI**
Modular System Architecture	Good Governance	Awareness that as these tools get combined in new ways, various ELSI arise.	Guidelines with which to see these and deal with them.	Governance documents supported by ELSI guidelines.

Table 6. CIS and modular system architecture

CIS Element	**Key ELSI guidelines**	**SecInCoRe Collaborative Goals**	**SecInCoRe Innovations**	**Implemented in the RI**

NEC	Good Governance	Support ways of providing context to data (i.e. how produced, motivation for sharing) Following privacy laws Following data protection laws Make transparent how long data is stored, who gets to delete it, and systems in place to ensure effectively actions on sensitive data. Avoid issues of pseudo-anonymity Support a data controller in a collaborative situation	Social tools to support user awareness that these rules may apply differently to different individuals. Social agreements that ensure that the personal data is only enough to fulfil your purpose in relation to this data. This also is balanced with enough to manage role improvisation. Support users in engaging critically with how the different data is combined in different modular configurations of the system using the NEC.	Governance documents supported by ELSI guidelines.

	Data Controller	If there is a dispute within the CIS or a breakdown of the system, who is responsible to provide support, mediation, resolution and how can this support be	By default, the parties brought together in a CIS are joint data controllers, but provide governance support tools for different hosting situations.	Governance documents supported by ELSI guidelines.

Table 7. CIS and NEC

CIS Element	Key ELSI guidelines	SecInCoRe Collaborative Goals	SecInCoRe Innovations	Implemented in the RI
Semantic Framework	Risk Assessment in Diversity, Contextual Reasoning, and Configuring Awareness	The system needs to be flexible enough to not impose one community's way of thinking, doing, planning. Encourage in how interactions are set up a degree of reflexivity towards thinking about meaning of information (yours and others) for the different groups involved. Make it possible to hold in the same space conflicting ideas and to still be able to take action without assuming or expressing that action as 'the' only correct answer.	A system that moves away from deficit models of communication to ones that are flexible enough to not impose one community's way of thinking, doing, and planning for disasters onto another community. Provides some degree to contextual meta-data Creates a shared, intersubjective vocabulary of action	Graph View Search Editable Ontological Categories and relationships Editable Tags A variety of ways of deriving and combining document and user meta-data

	Transparency	System acknowledgement that when technologies are designed, social logics become programmed into them, thus making those logics as visible as possible for those wanting to implement the system in order to not accidentally exclude or make invisible specific parts of social life.	Guidelines with which to see these and deal with them.	A Quick Start Guide for designers to think about where in their design they might be making social decisions and make those moments visible and legible to users.

Table 8. CIS and semantic framework

CIS Element	**Key ELSI guidelines**	**SecInCoRe Collaborative Goals**	**SecInCoRe Innovations**	**Implemented in the RI**
Knowledge Base	Contextual Reasoning	Provide contextual understanding of why specific decisions were made and why an incident played out as it did and why specific ELSI arose, because a simple list of ELSI will not translate to	Build in a way to provide contextual and situated understanding of ELSI, in action, not just as abstract concepts. Support the better ability to identify and gather lessons learned for future case studies.	ELSI as made visible in the choice of categories and how they are able to relate to each other. Explicit inclusion of ELSI and lessons learned categories

		other incidents or uses.	Support greater awareness of how data could be better shared between stakeholders in a CIS.	
		Structures of archive visible.	The relationships created for these elements in an Inventory have ethical implications, especially in relation to inclusiveness and neutrality, for how the incidents become knowable.	ELSI as made visible in the choice of categories and how they are able to relate to each other.
	Risk Assessment in Diversity	Set up the collaborative platform in ways that support the presentation of conflicting ideas, including the identification of concepts, terms, and technologies that enable communication without forcing everyone to understand things in exactly the same way.	Provide the larger repertoire of patterns seen by one actor in order to help another actor gain insight into their practices of situational awareness. This also allows for anticipation of what's to come, which is important for planning purposes	Requirement for case studies to be researched from a range of sources, and inclusion of different categories of actions and understanding.

Table 9.CIS and Knowledge Base

2.4.3 OpenAtrium

Reference Implementation:

OpenAtrium is an open-source knowledge management platform based on Drupal and maintained by Phase 2 Technology. Until now, we have been adapting OpenAtrium for the following primary uses:

- Host the Common Information Space (CIS) concept public documentation
- Host the documentation relating to the ELSI guidelines
- Provide an internal collaboration platform for the project consortium

In D5.3 we described the conceptual model and the basic functionality, including existing access control features. In June CloudSigma launched an updated SecInCoRe OpenAtrium platform. This update (OA v2.64) led to a number of enhancements and improvements to the overall usability of the platform and enabled some more specific functionality. In general terms the new theme and layout has improved usability and functionality of the platform and puts more tools at the disposal of administrators and space members alike. As Open Atrium was initially chosen as a collaboration tool, it made sense to extend functionality that makes it easier for collaborators to communicate, especially in real-time and with time-stamping.

In this deliverable we will describe how we have extended functionality as a basis for supporting future Demonstration Cases.

Demonstrator implementation:

A new 'Demonstration Space' (http://185.12.5.114/demonstration-space) has been created specifically for the purpose of demonstrating the functionality of the OpenAtrium platform in the context of the CIS concept. We have preconfigured the space to include a Discussion Board, Chat Room, Document Share and an Admin Support section. We have also integrated the Semantic Search engine so users can access the Knowledge Base. The following functionality provides the basis for potential integration into future Demonstration Cases.

Demonstration Space > Discussion Board. A Discussion Board (http://185.12.5.114/demonstration-space/discussion-board), (Figure 5) allows users to create and contribute to conversations in the form of posted messages, which are time-stamped and archived. Access rights and permissions can be configured at section level by administrators, but unlike regular internet forums administrators will not necessarily have the same level control as moderators. This functionality (or lack thereof) will be evaluated during end-user testing. Users will typically be granted the ability to create new topics (or threads) and reply to existing ones, but this will depend on the permissions set by the administrator. The administrator will also be able to add groups, teams or members to receive notifications for this section, set publishing options and authoring information.

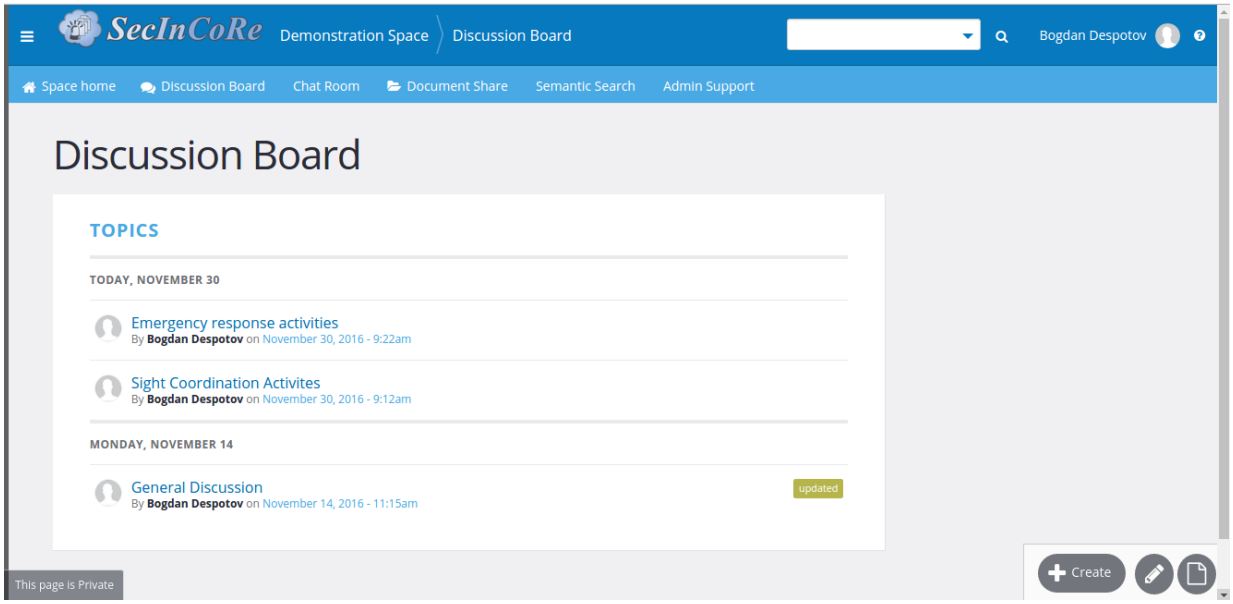


Figure 5. SecInCoRe OpenAtrium Demonstration Space - Discussion Board

Demonstration Space > Chat Room. This section (http://185.12.5.114/demonstration-space/chat-room) enables site administrators to create chat rooms where users can message each other in real time (Figure 6). This benefits real-time coordination between teams. It is envisioned that multiple public and private chat rooms might be required. This is fully supported within OpenAtrium. Multiple chat rooms can be created and configured so each chat room has different group access parameters. It is also possible to give the chat room a unique name to help focus discussion.

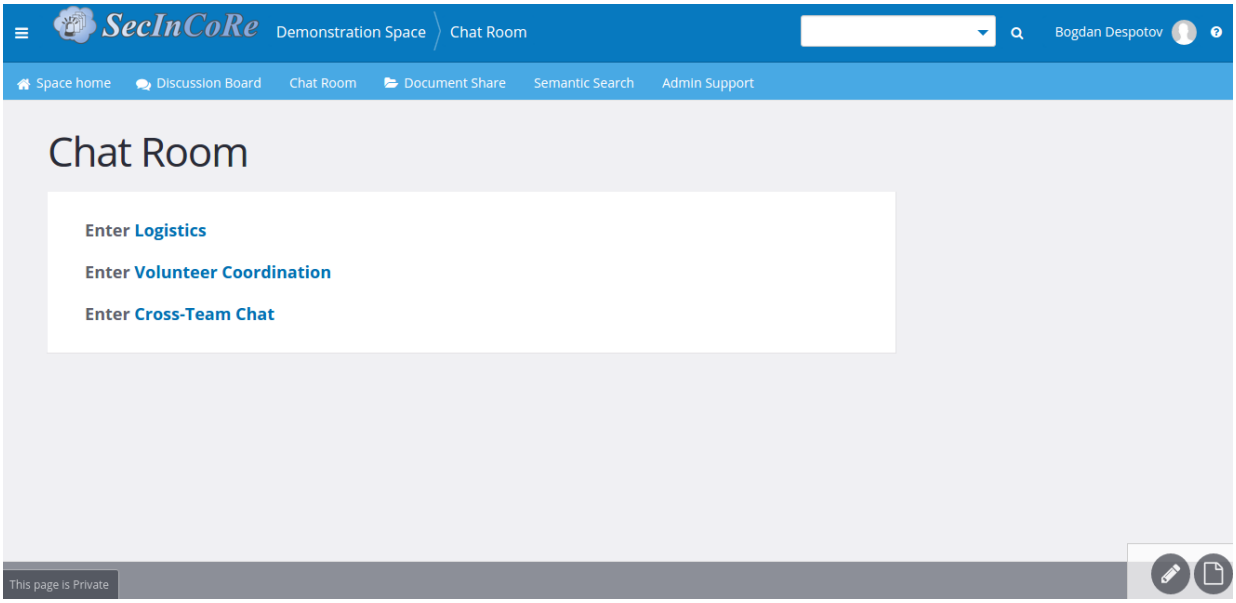


Figure 6. SecInCoRe OpenAtrium Demonstration Space - Chat Room

Demonstration Space > Document Share. The document share section (http://185.12.5.114/demonstration-space/document-share), (Figure 7), allows users to both create and upload content. Uploaded files are restricted to 2MB in size and the following commonly used file types are supported: jpg, jpeg, gif, png, txt, doc, docx, xls, xlsx, pdf, ppt, pptx, pps, ppsx, odt, ods, odp, mp3, mov, mp4, m4a, m4v, mpeg, avi, ogg, oga, ogv, weba, webp, webm, zip, tgz, gz, key, dotx. All added content is shown time-stamped below in a recent activity pane. Web content from external media provider such as YouTube or Vimeo can be embedded by entering the URL to the file or media resource. Users can also link to documents or files from other spaces or section. The usual access control parameters are available for administrators.

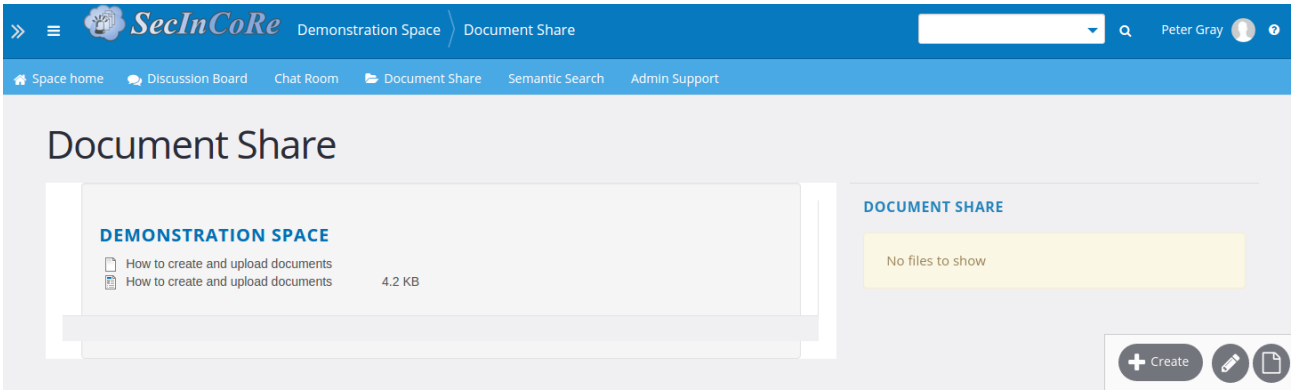


Figure 7 .SecInCoRe OpenAtrium Demonstration Space - Document Share

Demonstration Space > Semantic Search. An iFrames module was installed allowing for the integration of the Semantic Search (Figure 8) within the SecInCoRe OpenAtrium Demonstration Space (http://185.12.5.114/demonstration-space/semantic-search). This allows for all activities to be concentrated within one tool, which is the OpenAtrium. It would immensely improve the workflow of the end user as they would not need to load multiple platforms in order to use the full capabilities of the system. Also it would provide an additional layer of security when accessing the Semantic Search as it can be restricted for members of a certain group or registered users in general. The implications are described in more detail in the following section.

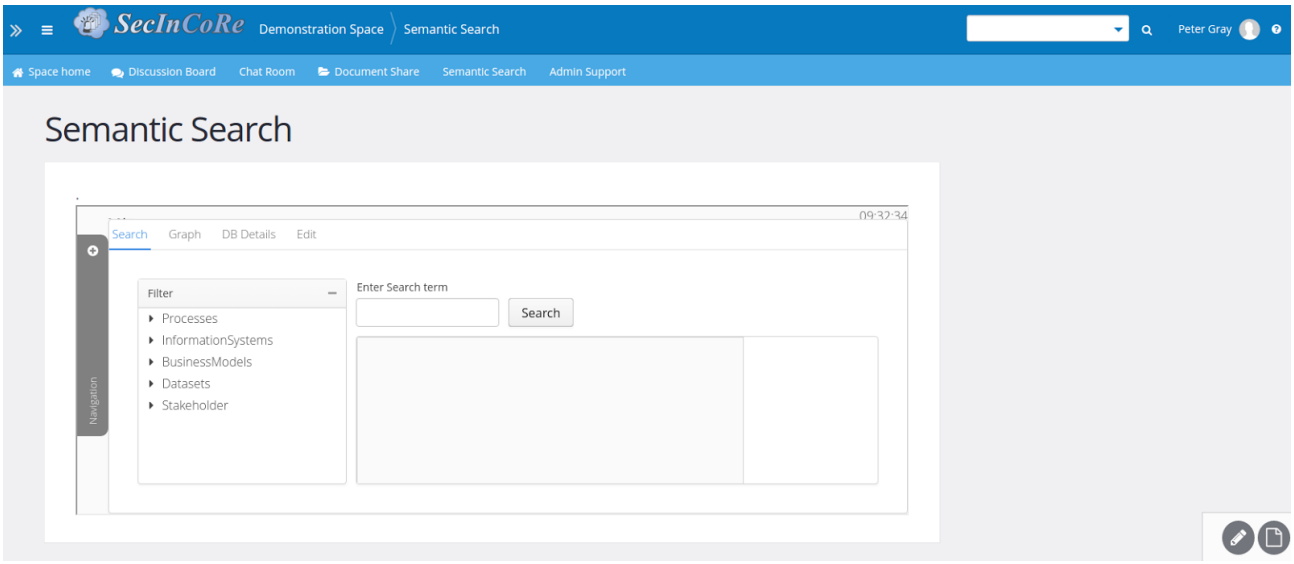


Figure 8. SecInCoRe OpenAtrium Demonstration Space - Semantic Search

Demonstration Space > Admin Support. This section (http://185.12.5.114/demonstration-space/admin-support) offers a set of "how to" guides for administrators covering topics relevant to setting up and maintaining the space (Figure 9). This could be used in a Demonstration Case to guide end-users acting as space administrators through the necessary steps. As described in D5.3 Open Atrium features robust access control that outperforms many other open source solutions by providing administrators full control over access for individuals, project teams, and organizations. It will be important to demonstrate the following to end-users:

- Information can be shared globally or to restricted groups
- Communications can take place among larger communities or highly classified teams
- Attached media and file documents can be made private to specific groups and teams.

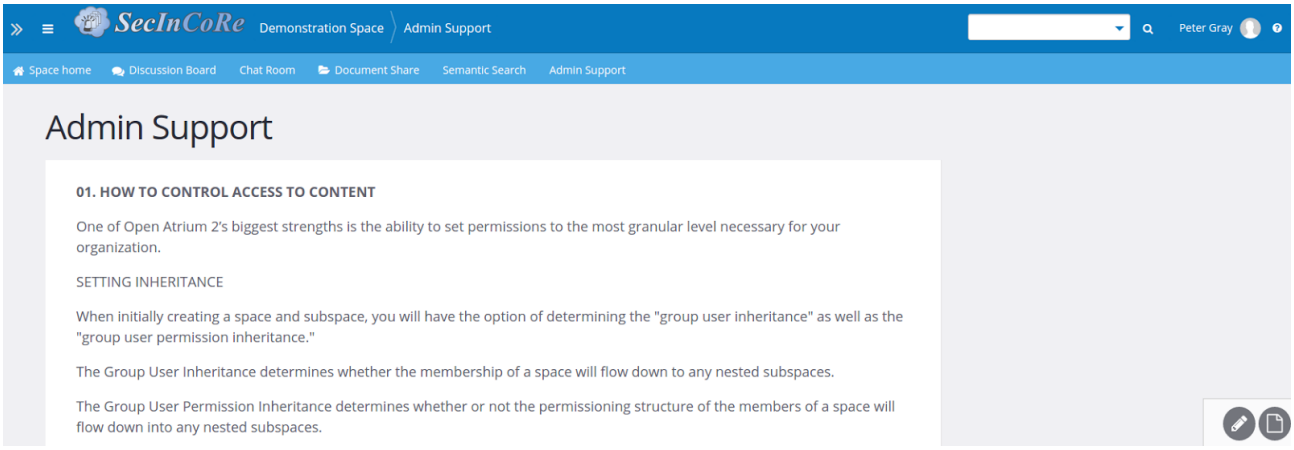


Figure 9. SecInCoRe OpenAtrium Demonstration Space - Admin Support

2.4.4 Network Enabled Communication System (NEC)

The Network Enabled Communication system provides secure and resilient access to the Knowledge Base and the underlying services. Parts of the NEC, e.g. Network Coding algorithms and 3GPP Professional Mobile Radio, are implemented and analyzed using

simulation environment and laboratory equipment. Therefore, they are not part of the demonstration implementations. The aim of this research is the improvement of operational communication capabilities using multiple communication technologies to access the CEIS, available data rates and communication reliability will be improved. To test the developments scientific measurement series are necessary. Results will be published on scientific conferences.

One core concept of the NEC is the establishment of a RescueRoam access network for all European emergency services. This is an innovative service to enable interaction between emergency services. This component was introduced to end-users during the 1st Lancaster workshop and the 2nd review meeting. Feedback from end-users was very positive, considering the concept as very helpful for their work.

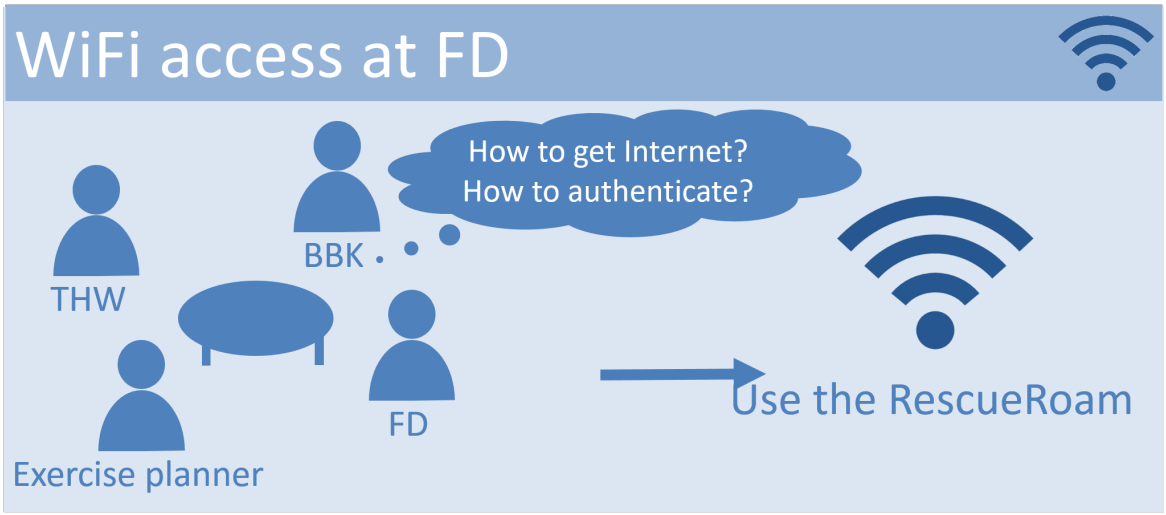


Figure 10. Benefits of RescueRoam for emergency services

The RescueRoam concept as presented in D4.3 describes a federated communication system which enables the usage of the SecInCoRe Knowledge Base from different locations. More concrete it is the aim to provide network capability using the same user credentials at Fire Station A, Fire Station B, etc. Figure 10. Benefits of RescueRoam for emergency services depicts the idea behind RescueRoam: Different emergency services use the CEIS at their home locations, they use the Semantic Search and the Knowledge Base. When these emergency services identify the need to collaborate and to meet face-to-face, they want to have access to the CEIS at this remote location as well. With RescueRoam, a WiFi network is enabled to provide access to the CEIS using the same user credentials as every time the person login into the CEIS.

The RescueRoam concept describes principles how to setup such a system, what requirements have to be fulfilled. In order to demonstrate the benefits of such approach the RescueRoam Reference Implementation (R3I) is setup. The R3I consists of one or many LDAP directories which provides the user account management, a RADIUS server which is used to identify the Wi-Fi Access Points and the access points themselves. During the 2nd review meeting in Dortmund, a Moxa AWK-6332 Wi-Fi access point was used to provide the RescueRoam SSID, CloudSigma used a Microsoft Active Directory domain to manage user accounts. Combining these components users could login to the Wi-Fi network and access the Knowledge Base.

Most user accounts have been created before the meeting but it was shown that a user account can be created and used spontaneously. The next step is the implementation of an interface between the LDAP system and the semantic framework. As mentioned in the previous paragraphs the user credentials shall be used for CEIS access as well. At the review meeting a different user account was needed to e.g. use the Semantic Search. The R3I demonstrates the capabilities of the NEC component for the overall system, providing a secure and reliant access to the system with minimum effort for the users.

2.5 The integration between different validation objects

To combine the concepts and research work behind the Inventory, Knowledge Base and Taxonomy, the Semantic Search was developed. The Inventory as the conceptual representation of the relevant domain-content collected within SecIncoRe, is realized in the Knowledge Base. The Knowledge Base is structured, using the Taxonomy, representing the thematic relations within the domain. The Semantic Search is used to enable the access to all Knowledge Base contents in the Demonstration Cases. Figure 11 shows the process.

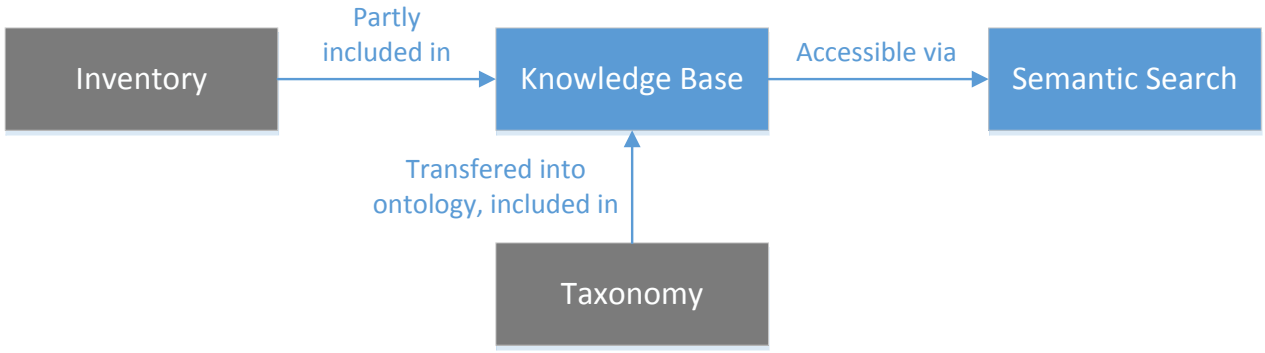


Figure 11. Integration of Inventory, Knowledge Base and Taxonomy

2.5.1 OpenAtrium integration with the Identity Management Solution

An Identity Management solution, consisting of networking hardware and LDAP server, was presented in D5.3 and at a plenary meeting in October 2015 as part of the AAA / IDM demonstrator. The system has been configured and maintained to serve as authentication for the following CEIS components:

- Open Semantic Framework / Semantic Search
- Semantic Media Wiki
- Knowledge Base

At the time of writing this deliverable, further integration has commenced to include OpenAtrium. However, it is not yet confirmed whether SSO can be successfully implemented.

2.5.2 OpenAtrium integration with Open Semantic Framework / Semantic Search

As mentioned above it Section 1.1.6, the Semantic Search has now been integrated within the SecInCore Open Atrium deployment, inside a protected space which is only visible to

registered users. Further restrictions will apply, depending on the user groups and permissions set by administrators. As the Semantic Search is integrated within the Demonstration Space, it will only be visible or accessible to registered members of that Space. It does not require further authentication. To make the Knowledge Base searchable within the Open Atrium, an iFrames module has been installed. This allows users the ability to search data directly from within the OpenArium, where the data is then displayed within the same pane.

Considering the SecInCoRe OpenAtrium platform (as a knowledge management and collaboration tool) has only partially been discussed and explored by end-users in a workshop context, we intend to offer selected end-users a chance to experiment with the various collaboration and administration functions as part of a subsequent Demonstration Case. A realistic demonstration scenario will be designed to incorporate three aspects of the CEIS.

1) Identity management - This will primarily include administrative functions, access configuration and permissions, but could potentially be extended to include Single-Sign-On if this functionality is integrated successfully.
2) OA communication and collaboration functionality - This will include interaction with the Discussion Board, Chat Room, and Document Share.
3) Semantic Search - Access and functionality will be tested for validation purposes.

2.6 Adapting the Reference Implementations to demonstration implementations: the general process

To perform the Demonstration Cases and customize the Reference Implementations into demonstrator implementations, several steps are necessary. In a first step the needs of stakeholders within the PPDR domain are monitored in SecInCoRe. Knowing these needs, different Demonstration Cases are developed, to show specific elements of SecInCoRe to specify target groups. Once the Demonstration Case is developed, the Reference Implementations are customized, taking the specific needs of the Demonstration Case into account. In addition, to build a full (or part) CIS for the Demonstration Case, the demonstrator implementations, as well as the underlying concepts and functionalities are matched together, to support the case. The Demonstration Case itself uses all selected implementations and concepts in loose or narrow story, to guide the participants (Figure 12).

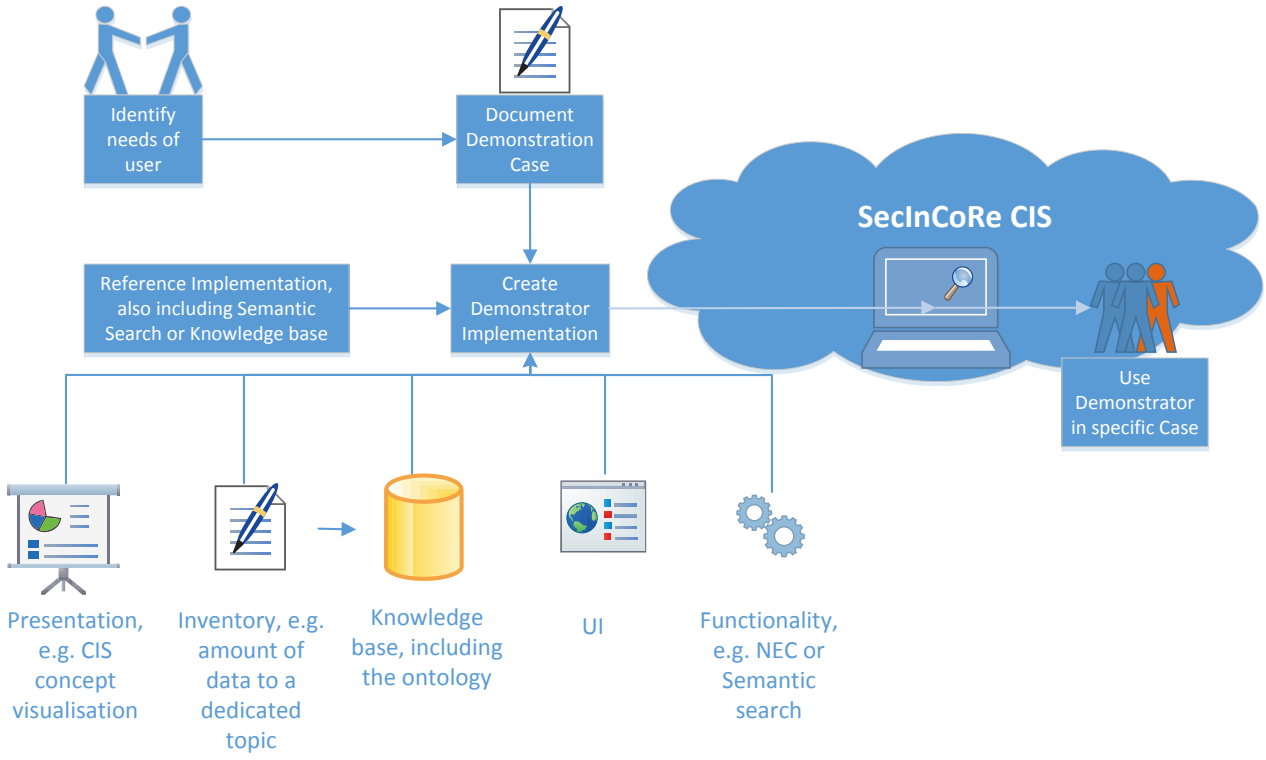


Figure 12. Showing the process

2.6.1 Example "GraphView" show-casing the process

Specific cases are defined based on the need of the respective end-user group. In separate interviews with the LRF the need to clarify and visualize the relevance and kind of relations between different information or documents, become evident. On this grassroots a workshop and demonstrator implementation are planned to come up with SecInCoRe solutions to this need. The process was as follow:

In a first PowerPoint- Mock-Up, shown in the Figure 13, the approach to settle documents within a Taxonomy was demonstrated. A document in the middle at the bottom is shown with topics, where the document is classified in. These topics are themselves arranged within a part of the SecInCoRe Ontology, to show the thematic classification.

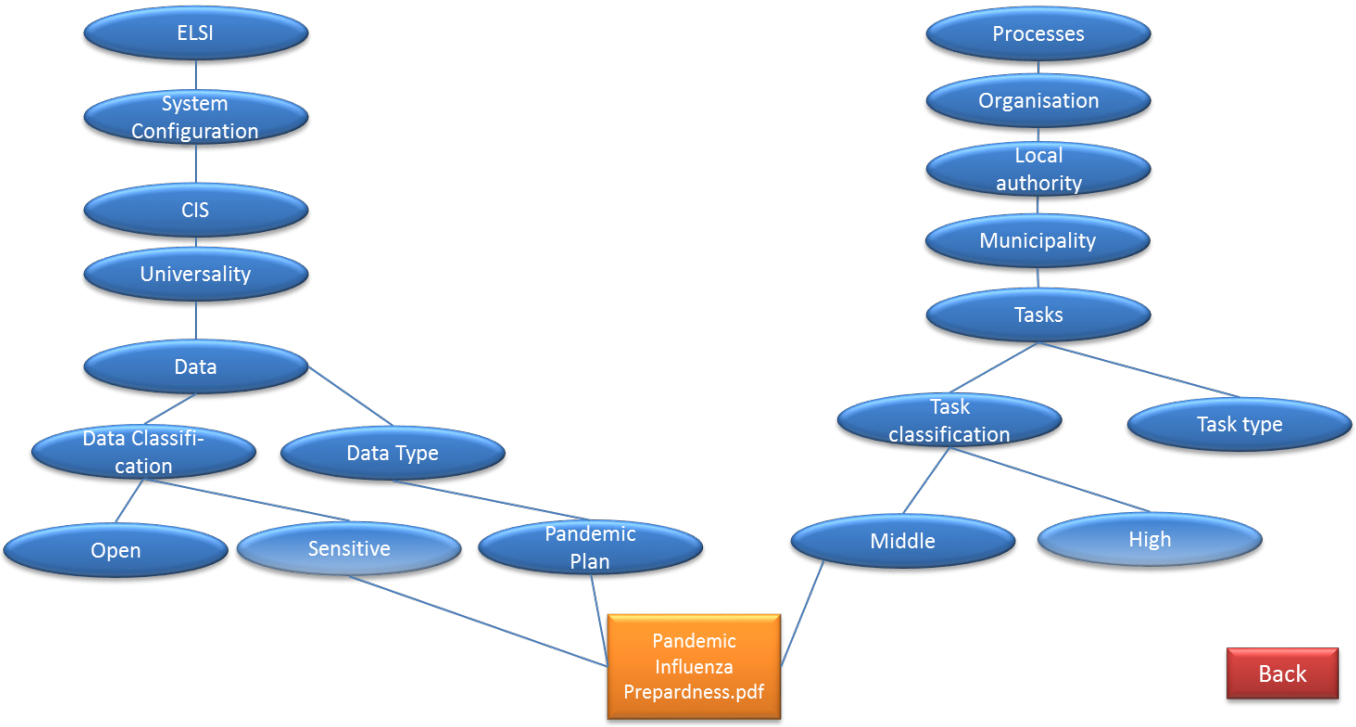


Figure 13. Mock-Up to show the integration of documents in a Taxonomy

Based on the presented and used interactive Mock-Up, the handling of user with this Mock-Ups and recommendations are used to modify the demonstrator implementation of a graphical view on search results. The photos in the Appendix (section Figures from the Second Lancaster Workshop) show some results of the dedicated workshops during the meeting in Lancaster with the LRF in May 2016. In this workshop based on example documents expected search words and a definition of different cluster was conducted from a end-user perspective.

First step to build up and implement a "graph view" (a graphical representation of search results), on existing information and documents, was to define the way of visualizing the Ontology. In Figure 14 WebVOWL was chosen as a basic tool. More information about the implementation of the Ontology and the realization of the graph view will be described in D4.4.

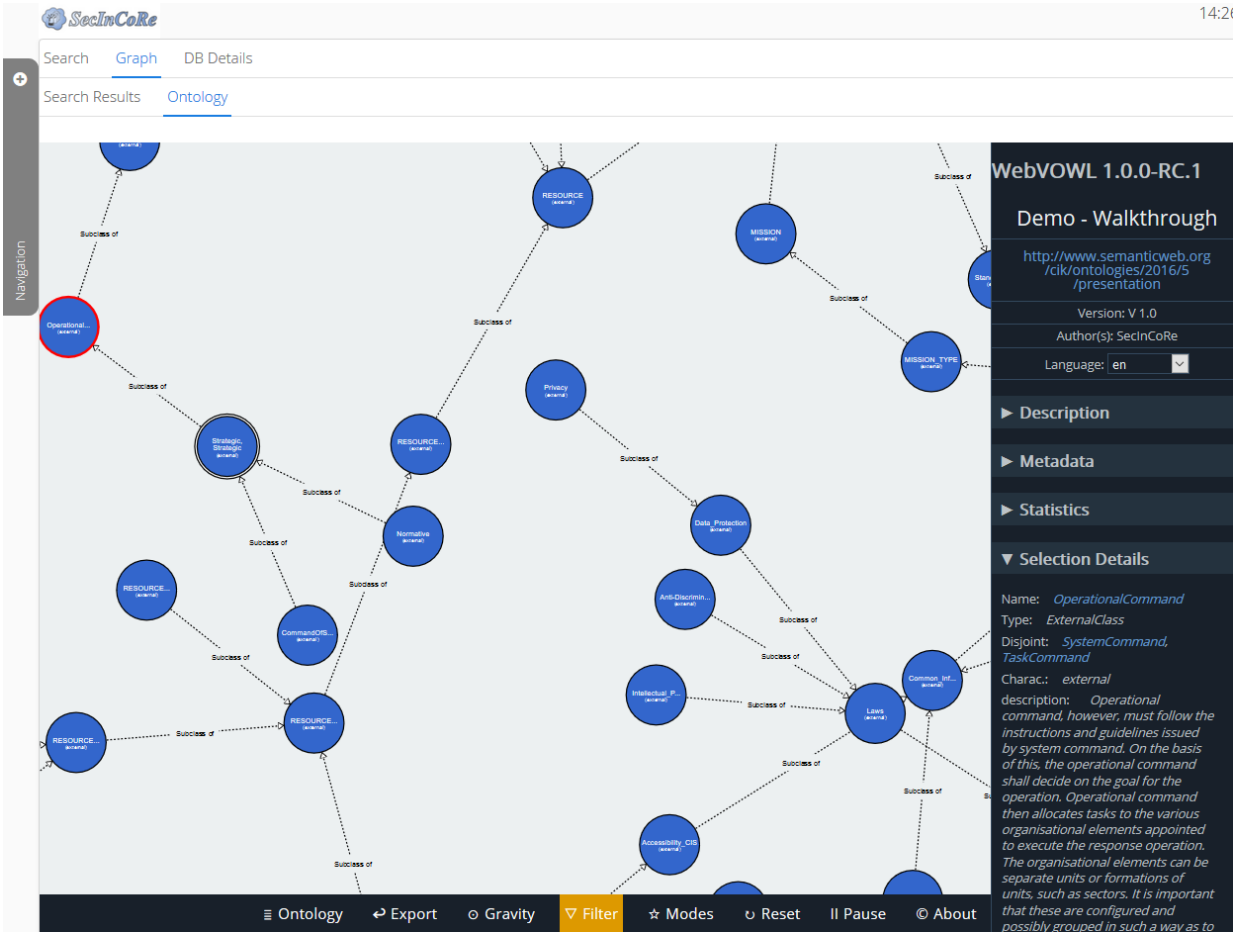


Figure 14. WebVOWL visualisation

Based on the experience with visualizing the Ontology, the integration and therefore the combination with the Semantic Search and the linked data sources was aimed. Figure 15 shows a first realization of the graph view.

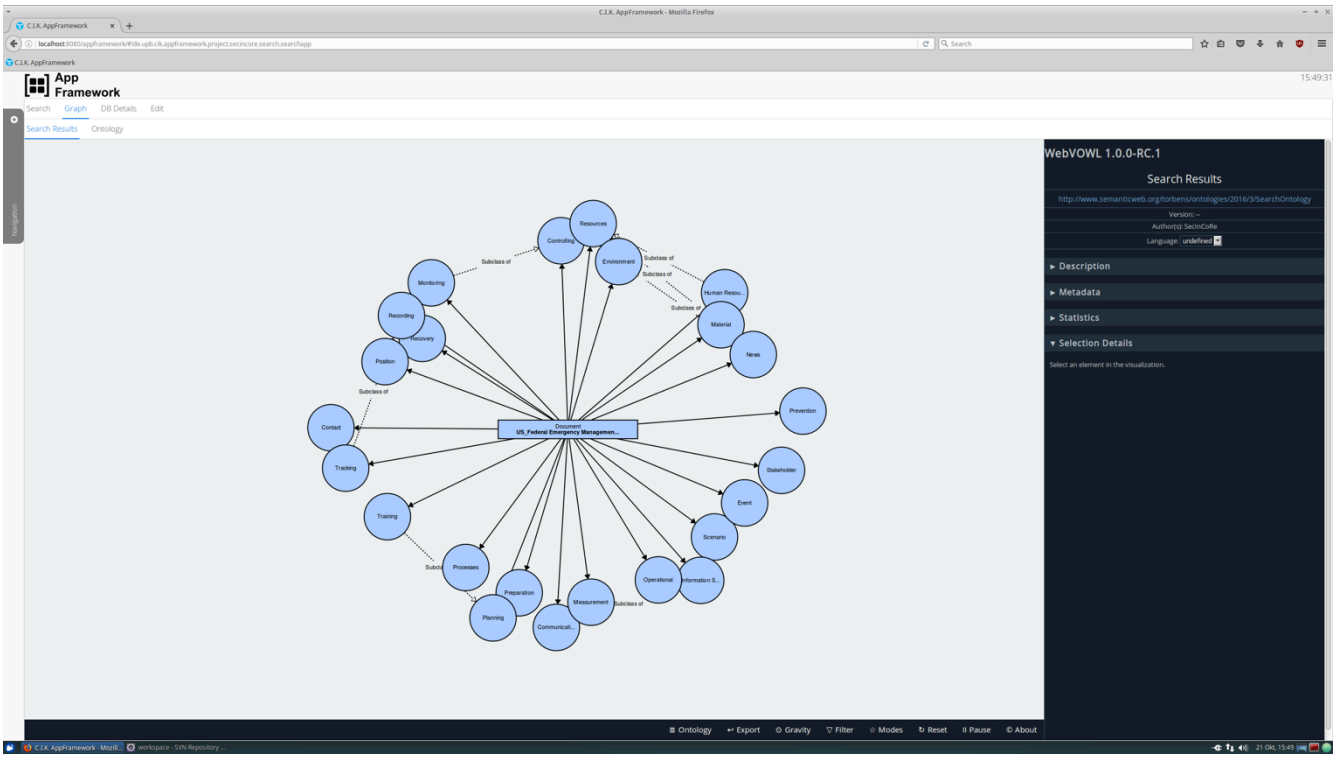


Figure 15. First version of the graph view

3 Final version of the validation methodology

The organization of a Demonstration Case requires close cooperation between project teams working on different aspects of SecInCoRe, including: ELSI and collaboration; validation and evaluation; stakeholders' engagement; development of the CIS concept and of its technical implementations. It is for example essential that team members in charge of technical aspect (such as the deployment and adaptation of Reference and Demonstrator Implementations) closely collaborate with partners responsible for stakeholders' engagement to co-design the Scenarios and Use Cases that provide the basis for a Demonstration Case. At the same time, the Validation and Evaluation team must coordinate exchanges between other partners and provide them with inputs required to align the creation and implementation of a Demonstration Case to the SecInCoRe validation and evaluation strategy.

Furthermore, Demonstrator Implementations and other project outputs must be adapted to the interests, requirements and fields of operation of the end-users that participate in the Demonstration Case. This is required for at least two reasons: on the one hand, the adaptation to end-users' needs and interests favors their active participation in demonstration activities; on the other hand, the organization of Demonstration Cases around more realistic Demonstration Scenarios helps end-users relate their experiences with the technical and conceptual representations SecInCoRe to their work practices. Creating Demonstration Cases, it is crucial to provide a more solid base for the evaluation team to assess the potential impact of SecInCoRe against the baseline scenario represented by end-users' current practices.

Summing up, the adoption of a case-based approach implies that the scope, design and organization of a Demonstration Case ultimately depend upon:

a) the availability of concrete technical and conceptual tools that provide the means through which different elements the SecInCoRe concept can be communicated to or experienced by end-users;
b) the time restriction that stakeholders have to overcome to take part in workshops and other activities organized around a Demonstration Case, and the degree of connection between what is demonstrated and their specific practices, needs and competences.

These aspects constrain the range of activities that can be performed in a Demonstration Case, ultimately defining the boundaries of what can be validated and influencing the selection of data collection tools and methods to be used in validation activities. Although the principles and approach underlying the SecInCoRe VES are the fundamental guide for validation and evaluation activities, the implementation of the strategy evolves as different concepts and demonstrators proceed to maturity. The aim of this chapter is to explain how the overall strategy has been adapted and fine-tuned in response to the feedback received in three Pilot Cases, and to describe the tools that have been used to date to collect data from end-users involved in Demonstration Cases.

3.1 The adaptation of the SecInCoRe VES

Three main elements have been considered in the adaptation of the VES to the Pilot and Demonstration Cases performed to date:

1. The nature of demonstrator implementations as prototypes, rather than fully working implementations of the SecInCoRe concept

2. The short-term nature of Demonstration Cases
3. The limited usage of collaboration tools for end-users involved in Demonstration Cases at the current stage of writing

Regarding the first point, it must be noted that the aim of Demonstration Cases (and of the associated Demonstrator Implementations) is not to present end-users with a finalized, integrated and fully functional system. In all the Pilot and Demonstration Cases performed to date, the exposure of end-users to crucial elements of the SecInCoRe concept has been based on the integration of technical (interactive) implementations showcasing a limited sub-set of SecInCoRe functionalities with conceptual tools that provided them with the context and overall picture in which such implementations should be framed. Conceptual tools have for example included: booths in which focused discussions on specific aspects of the CIS concept were held between members of the SecInCoRe team and end-users; mock-ups and PowerPoint presentations that were used to illustrate functionalities not yet fully implemented; stories and posters that were used to help end-users envision realistic scenarios in which SecInCoRe could be used and how it would contribute to improved Collaboration Practices. For this reason, elements that would otherwise lend themselves to structured quantitative evaluation through standardized tools and instruments (usability, design, performance of the system etc.) have been excluded from the scope of validation activities.

Regarding the second point, as noted above "CISs are socio-technical systems which are produced in and through Collaboration Practices, such as sharing data/information, cooperating, negotiation, discussion, finding new partners, which are enabled and shaped by technical and organisational infrastructures". Assessing whether the technical infrastructures and conceptual apparatus developed by SecInCoRe can be appropriated by end-users (and more generally stakeholders) to produce a CIS that provides a significant added value over current practices would require a medium- to long-term Demonstration Case, ideally in a real-life setting that would enable the observation and analysis of the interactions between the social, organizational and technical aspects of the CIS.

All Pilots and Demonstration Cases organized had a very limited time span, being generally constrained to one or maximum two days in a workshop setting. This has of course limited the possibility to directly map the results of validation activities to SecInCoRe high-level objectives, since most of these objectives would only become visible if end-users had the possibility to establish, use and contribute to a CIS in a longer period.

This has for example become apparent in early attempts to validate with end-users the Data Layer based on the Inventory. For what pertains past disasters and existing crisis management models, the collection and uploading of documents presented to end-users has been performed by members of the SecInCoRe team. While it is true that the Knowledge Base grows with every demo case, this happens through the mediation of team members. Although they operate according to the requests, needs and contributions provided by end-users, the document base that end-users can access through the search is not the result of actions and choices made by end-users themselves in the performance of their daily practices.

This of course also influences which parts of the Ontology (as a representation of the underlying Taxonomy) becomes visible to end-users through their use of the Semantic Search. Although the Ontology is deepened in a specific direction to be adapted to a specific demo case, this deepening is the result of decisions taken before the Demonstration Case. In the

limited time available for end-users to experience the Semantic Search during a Demonstration Case, the thematic range displayed for the Ontology is therefore to a large extent pre-determined. Although lessons learned from each Demonstration Case are subsequently used to inform choices made for future demo cases, this happens in-between different Demonstration Cases rather than as a direct response of end-users' activities.

For these reason, assessing the perceived usefulness of the Semantic Search based on the actual documents or categories shown to end-users would not provide a valid assessment of the potential added value of these concepts and tools. The challenge is therefore to help users abstract from the specific results of their activities in the artificial and limited setting of the Demonstration Case.

Finally, while ELSI and Collaboration Practices have a crucial role in SecInCoRe, until now the interactive aspects of Demonstration Cases have focused on individual use. Although most of the ELSI guidelines described in Table 3- Table 9 have been included (or have the potential to be included) in Demonstration Implementations, the activities performed to date in Demonstration Cases have not yet involved any real-time collaboration practices. For this reason, the response of end-users to the collaboration and ELSI-informed practices envisioned by SecInCoRe has only been obtained through guided discussions based on conceptual tools (such as presentations, booths and stories).

The three elements listed above motivate the decision to primarily base the implementation of the validation strategy for this first phase on qualitative data collection methods including structured observation, focus groups discussions and semi-structured interviews. The tools used to date in Pilot and Demonstration Cases are briefly described below, while examples of the observation and interviewing frames used during Demonstration Cases are provided in the Appendices.

3.2 Tools and methods used for data collection and for the organization of Demonstration Cases

3.2.1 Demonstration Case Protocol and Templates

As already explained, the range of activities performed in a Demonstration Case is adapted to the degree of maturity reached by the conceptual and technological expressions of different elements of the SecInCoRe concept. Progress on Reference and Demonstration Implementations, as well as the development of non-technical representations of elements of the CIS concept, do not proceed in isolation from demonstration activities. Part of the organization of a Demonstration Case entails in fact a feedback process that involves the technical team, the ELSI team, the evaluation team and the involved end-users. The SecInCoRe outputs (i.e., Demonstrator Implementations and any other technical or conceptual representations of elements of the CIS concept) utilized in each Demonstration Case need to be calibrated according to the outcomes that have been selected for validation. Requests for improvements or for the development and adaptation of specific Demonstrator Implementations coming from partners, end-users and the validation team are collected by the validation team and transferred to the technical team, which assesses their feasibility against the current status

of technical implementations. The validation team[3] consequently identifies which elements of the SecInCoRe concepts and which specific requirements can be validated in a Demonstration Case, and prepares (or adapts) the tools and instruments that will be used to collect data for validation and evaluation purposes.

To guide the process and to ensure that Demonstration Cases are coherent with the SecInCoRe VES, a Demonstration Case Protocol (DCP) has been developed with the following aims:

- coordinate the activities of different teams and facilitate the flow of information between them
- guide the design of preparatory activities
- check the alignment of Demonstration Cases with SecInCoRe's VES objectives
- ensure the collection of background data according to a standardized format

The DCP provides therefore detailed guidelines to ensure that all activities related to a Demonstration Case are performed in a consistent way, in this way permitting the comparability of results and the collation of data across different Demonstration Cases. Detailed information about the DCP are available in D5.3.

The DCP involves the use of standardized Demonstration Case Templates (DCT) for the preliminary and final phases of the organization of a Demonstration Case; the empty template is provided in the Appendix of D5.3, while in the Appendix at sections about Templates from the preparation of validation activities it is possible to see the templates used so far. The collected DCTs, being the formal documentation of all Demonstration Cases organized during the project, form an integral part of the CIS concept documentation and will be stored in OpenAtrium.

3.2.2 Structured observation

As explained above, the activities performed in Demonstration Cases involved a mix of technical and conceptual representations of selected elements of the SecInCoRe concept. To allow the natural flow of these activities while permitting the collection of useful data for validation, an observation frame was developed. The observation frame consisted of a set of shared guidelines given to each observer that reported (a) an *a priori* list of codes, based on categories derived from the SecInCoRe High-Level Requirements related to the aspects of the CIS concept that were the focus of the Pilot Case or Demonstration Case; (b) instructions on the verbal and non-verbal aspects of end-users interactions with Demonstration Implementations, and of their reactions and comments to conceptual presentations, should be recorded. Visual and audio recordings were also taken, to integrate the notes produced by each observer.

To ensure that observation would not be influenced by biases emerging during the Demonstration Case (e.g., an observer consciously or unconsciously giving priority to the participants whose opinions were more aligned with her or his own), an observation schedule was designed in advance for each pilot / Demonstration Case to pre-assign each observer to a specific group, participant or activity. The schedule was designed to maximize the exposure of

[3] Validation Team is composed by T6 ECO staff.

each observer to different aspects of demonstration activities and to guarantee that each observer would closely follow, for an equal amount of time, each of the participants. This arrangement also intended to increase the reliability of conclusions, since it permitted the triangulation and cross-checking of the impressions collected by different observers on each participant and activity.

3.2.3 Questionnaires on end-users' backgrounds

A structured questionnaire was developed to collect standardized information on the background of each participant, their current job and their previous experiences with CIS in the PPDR domain. The questionnaire included both closed-ended and open-ended questions. Questionnaires were distributed at the end of each pilot or Demonstration Case, and were transcribed in an end-users' database by members of the validation and evaluation team.

3.2.4 Semi-structured interviews and focus groups

At the end of each Pilot Demonstration Case, a validation focus group was held with end-users. A protocol was designed to guide the discussion and to ensure that all relevant topics were covered. An audio recording was taken of each focus groups to integrate the notes taken by moderators.

At the end of the Paderborn Demonstration Case, semi-structured interviews were conducted with end-users to collect their impressions and feedback. A standardized protocol, designed prior to the Demonstration Case, included a list of topics, questions and probes to ensure that all relevant materials was covered; interviewers had however the possibility to alter the ordering of questions to ensure a more natural flow of the conversation. As part of the probes given during the interview, end-users were asked to perform some guided activities using the Semantic Search demonstration and comment on the results. Each interview was conducted at a separate workstation. The interviews were recorded and subsequently transcribed.

3.3 The analysis of data and evidence collected through Demonstration Cases

Data collected through the different tools (observations, focus groups, semi-structured interviews) went through two coding cycles. The first coding cycle was based on an a-priori list of codes derived from the High-Level Requirements related to the elements of the SecInCoRe concept used in the Demonstration or Pilot Demonstration Case. The first coding was individually undertaken by each observer / interviewer; results were then compared and triangulated.

Where needed or in the case of ambiguities, video or audio recordings of Demonstration Case sessions were used to integrate observation notes.

The aim of the second coding cycle was twofold: (a) generate aggregate categories from the individual codes; (b) identify emerging themes or topics that were not originally included in the a priori list. The ensuing enlarged coding frame was then used as the starting base for observation and coding in the following demonstrations.

4 Reports from Pilot Demonstration Cases and preliminary activities

Pilot Demonstration Cases (also called Pilot Cases) are an integral element of SecInCoRe VES. The aim of Pilot Demonstration Cases is to test and refine the methodology and the tools that will be used during actual validation activities. These improvements are based on an assessment of the validity, viability and reliability of the validation tools used during Pilot Cases. The chapter describes the data collection methods that were used in three different Pilot Demonstration Cases implemented as part of the activities undertaken during workshops and meetings with end-users organized by the project. The three Pilot Cases here presented have to be considered as setup for validation process activities. It is important to stress that Pilot Cases are part of the VES, since they help to redefine the methodology and to test tools and instruments that will be used in Demonstration Cases where SecInCoRe components will be validated.

Looking at the interaction between meeting participants and the organized activities, it was possible to gather lessons and improve the tools used to demonstrate concepts and outputs for validation activities. An additional aim of Pilot Cases is to give input to other partners on how to refine conceptual and technical implementations to better serve the needs of future Demonstration Cases. Finally, information gathered from end-users during Pilot Cases, if considered of adequate quality and if collected through tools and instruments that have been deemed valid for future validation activities, is also used as part of the actual validation of SecInCoRe components.

The next paragraphs summarize the activities and main results of three different Pilot Cases that were conducted by the SecInCoRe team with different stakeholders to co-design the system or to discuss its potential added value for end-users. Through observation and dedicated interviews, T6 ECO identified the main points that arose during these meetings and provided inputs to other project partners on the organization of validation activities and on the fine-tuning of the design process.

The Pilot Cases are described in the next paragraphs using a consistent structure that allows retracing the main information of the meeting (e.g., when, where, who participated) and the main concept that arose from it. Each Pilot Case report closes with a summary of the results from the meeting and the lesson learned that were (or will be) implemented in subsequent validation activities.

4.1 First Lancaster workshop

On 3-4 May 2016, SecInCoRe organised a workshop with different stakeholders engaged in planning and training in order to discuss with them about SecInCoRe's progresses and visions (Table 10).

Name	Title	Organisation
Andreas Immick	Emergency Services Division	Dortmund Fire Brigade
Maik Haalboom	Head of functional	Dortmund Fire

	group scheduling and Civil Protection	Brigade
Tabea Schwandt	Deputy Chief Officer/Manager Corporate Affairs	Fire Department of Bremerhaven
Ioannis Galatas	CBRNE Planner and Instructor	‚Hellenic National Defence
Mark Bartlett	Civil Contingencies Officer	Lancaster City Council
Collette Taylor	Health Protection Service Delivery Manager	Lancashire County Council
Ed Savile	Lead Officer - Social Responsibility	Blackburn Diocese
Geoffry Mackett	Senior Civil Contingency Officer	Somerset Local Authority
Jon Gunns		Jon Gunns Resilience Training
Stefan Grobelny	Scientific Assistant in the Department of Fire and Rescue Technology	Dortmund Fire Brigade

Table 10. Attendees to the First Lancaster Workshop

SecInCoRe team
Christina Shaefer, UPB
Jens Pottebaum, UPB
Torben Sauerland, UPB
Monika Buscher, ULANC

Katrina Petersen, ULANC
Sarah Becklake, ULANC
Catherine Easton, ULANC
Ivan Cucco, T6 ECO
Simona De Rosa, T6 ECO
Daniel Behnke, TUDO
Ioannis Danilidis, KEMEA
Paul Hirst, BAPCP
Olivier Patereur, ADS

Table 11. SecInCore's members to the First Lancaster Workshop

The following documentation is based on the observational notes and recordings taken during the workshop. Workshop activities were organised according to the agenda presented in the Table 12; the table also reports whether technical or conceptual demonstrators were utilized for each activity.

Activity N.	Topic	Group	Demonstrator
Activity I	Experimenting with SecInCoRe Inventory for Pandemic Planning	Group 1: Grobelny, Immick, Haalboom, Schwandt, Galatas	Technical demonstrator
		Group 2: Bartlett, Tylor, Sevile	Technical demonstrator
Activity II	Experimenting with SecInCoRe Taxonomy	Group: Schwandt, Immich, Gunns, Tylor, Savile	Power Point presentation

Activity III	Presentations and Discussion	Group: all	N/A
Activity IV	CIS Future-spective: Socio-Technical	Mackett, Tylor and Groblny	Booth
	Inventory	Savile, Halboom and Gunns	Booth
	NEC:	Bartlett, Galatas, Schwandt and Immick	Booth
Activity VI	Plenary discussion	Group: all	N/A

Table 12. Sessions description and typology of demonstrator

4.1.1 Report on SecInCoRe components

The aim of the report is to make a summary about end-users' feedback related to the following elements of SecInCoRe:

- CIS concept
- Taxonomy, Ontology and Semantic Search
- Knowledge Base and Inventory
- Collaborative practices and ELSI

4.1.1.1 CIS concept

The CIS concept was presented to participants and discussed. The general feeling gathered from users is that a system that permits live connection between people and fosters information exchange is extremely valuable for end-users who work in emergency services. Among the positive feedback, participants highlighted the value of SecInCoRe for cross-country collaboration thanks to the possibility of debriefing experiences and exchanging lessons learned. However, some crucial issues were raised by participants. In particular, trust emerged as a key element to building a CIS; participants were doubtful that the trust needed to favour collaboration and information exchange in emergency services could be entirely built within an online CIS (without face-to-face exchanges).

4.1.1.2 Semantic Search (and the underlying concepts of Taxonomy and Ontology)

Workshop participants generally welcomed the concept of the search engine that was presented. Almost all participants found the search a relevant tool to get access to information, which is one of the crucial phases when planning an emergency.

During a dedicated exercise, stakeholders had the chance to interact with the Taxonomy and with the search engine.

One of the attendees searching for pandemic, however, found the relations among topics and categories not relevant for him. The same person found the interface of the search engine not very clear and user friendly. Looking at the Search Function and related results, the user suggested that it would be helpful to be guided in the document. The research and the documents showed should be related to abstract, key words, word highlighted in the documents having a kind of "more advanced research". Then, he suggests having a different Search Function based on a first separation for threats, and then on the application of filters.

4.1.1.3 Knowledge Base and Inventory

During the interactions with the demonstrator, it was also possible to discuss theoretically and practically the contents and the functioning of the Knowledge Base created by SecInCoRe.

The most positive feedback that was collected about the Knowledge Base regards the creation of a past disaster database in which, through a dedicated template, it is possible to gather consistent information for each incident. In this sense, stakeholders expressed their interest in the lessons learned contained in the Inventory and made accessible in the Knowledge Base. In particular, two users found the idea to have a common template to collect and read information very useful. In addition, one user suggested to insert in the template information on statistics in relation to specific and more operational issues. Having data presented and collected not from an historical point of view but from a specific perspective could really provide a value added over the general content available on the internet.

At the same time, users were concerned about the fact that information stored in the Inventory should come from good and trustable sources. In addition, it was also requested to clarify if the Inventory is for planning phase or operational phase.

4.1.1.4 Collaboration Practices and ELSI

Talking about the value of Collaboration Practices, the main point that was touched during the workshop was mainly linked to the possibility to create new contacts offered by SecInCoRe.

Several users agreed that, during the working routine, First Responders who need information directly call the person they know to have access to the information. This appears to limit the possibility to access relevant information, due to the fact that access to information is strongly related to personal connections.

In this sense, almost all participants agreed that SecInCoRe could improve the current practices by creating an alternative network. Particularly, if documents searched in the Inventory could contain the contact details of their authors it would be possible to establish a link without otherwise hard to reach sources. In other words, end-users expressed their positive feeling about the option to have a function that allows creating new connections that they cannot reach

in their current practices. Such function could also be very different from what internet services offer.

In line with this, the idea to create a network of contacts linked to information is seen as an added value.

4.1.2 Results from the workshop

Results from the workshop show that participants appreciated the overall value of the system. Indeed, they welcome a system that could establish a live connection between people and information stored in the system. They envisage to use the system for planning and to get access to documents to prepare a plan. In this sense, language issues arose in the reading the documents. What emerges is that non-English speakers search for their own language.

Attendees would like to have the possibility to directly access authors' to build connections that go beyond their personal networks. This possibility has been identified as a very valuable output from the project. Another great benefit is the possibility to have access to lessons learned, that are crucial in the creation of a plan.

However, during the workshop also some critical issues arose. The main points that, according to participants, should be discussed further are the following:

- management of the system and boundaries
- security issues
- sustainability of the system

After the workshop, the management of the system and its boundaries are not clear to participants. This leads to other critical points, such as the management of sensitive data and the security of the system. What emerges from the users' perspective is that the system would be trustable if it is somehow sponsored by a trustable organisation or is related to an organisation of which they are already part. Both issues are clearly related to sustainability.

4.1.3 What we learned for validation purposes

Given that Pilot Demonstration Cases are intended as an opportunity for setting the methodology and improving the way in which concepts and project's output are presented in further validation activities, the following paragraphs summarize what we learned from the First Lancaster Workshop.

What clearly emerged from the workshop is directly related to the presentation of SecInCoRe to attendees. Participants to the workshop stated that presentations of core concepts were too difficult to understand. This point was particularly true for the presentation about Taxonomy and related exercises that were performed without the use of technological support. In this case, one user suggested to discuss Taxonomy in another way to be more effective.

The value and potentialities of the Taxonomy were fully appreciated by workshop participants. The Taxonomy was not analysed according to the underlying categories, but mostly through the Search Function. On this point, we learned that the Search Function must be more user-friendly and that documents need to come out with some key words or some reference that can help user skim the document to save time.

It was particularly clear that, for the Taxonomy exercise, it is important to reframe the question in terms of keywords rather than Taxonomy to eventually set things in motion. Also, participants tended to relate the concept of Taxonomy to the idea of administrative hierarchy (cataloguing documents according to the level at which the document / plan was produced appeared at the beginning as the most 'natural' approach for most participants). The Taxonomy remains quite a hard concept to grasp in a short time; translating the concept in actual practices could help get participants more easily involved.

The same feeling was expressed about the explanation of the NEC component.

Some attendees agree that most exercises were too theoretical, and that more tangible activities and tools could be useful to better understand the project's scope and outputs. In this sense, it was suggested to use prototypes or more mock-ups to show SecInCoRe potentialities.

It was also suggested to make things easier for the users, more user-friendly in their presentation, in order to attract more stakeholders though simplicity.

Then, the initial presentations of the project but also the Taxonomy and NEC booths were too complicated and abstracted. Attendees want to see something concrete or at least they want to listen to something more tangible. This suggests to rethink the way in which we communicate project's outputs and objectives.

To conclude, a demonstrator is something different from the co-design and need to be shown through a dedicated technical support.

*4.2 **Dortmund workshop***

On 23-24 June 2016, SecInCoRe had the second review meeting. The review was held in Dortmund. The first day was entirely dedicated to the demonstration of SecInCoRe concepts and outputs to reviewers and attendees to the meeting (Table 13).

Name	Title	Organisation
Francesco Lorubbio	Project Officer	European Commision
Sokratis Varakliotis	Reviewer	European Commission
Roberto Mugavero	Reviewer	European Commission
Tabea Schwandt	Deputy Chief Officer/Manager Corporate Affairs	Fire Department of Bremerhaven
Andreas Immick	Emergency Services Division	Dortmund Fire Brigade

Leon Teipel	Fire Officer	Fire Department of Dortmund

Table 13. Attendees to the Dortmund Workshop

SecInCoRe team
Silke Corall
Rainer Koch
Jens Pottebaum
Torben Sauerland
Christina Schäfer
Daniel Behnke
Niklas Goddemeier
Christian Wietfeld
Katrina Petersen
Ivan Cucco
Simona de Rosa
Andrea Nicolai
Olivier Paterour
Alexander Georgiev
Paul Hirst
Ioannis Daniilidis

Table 14. SecInCore's members to the Dortmund Workshop

Among all activities performed, on the 23rd a session was organised dedicated to Demonstrator cases that took around two and half hours. The aim of the session was to show SecInCoRe's concepts and outputs through a demonstration of all components developed at the time of project's development. To perform the demonstration, components where shown using different approaches such as Demonstrators, mock-ups, booths and presentations. Particularly, the CBRNE training exercise preparation with the FDDO (*FDDO story*) and the Pandemic Plan

Revision (*LRF story*) were used to test the template that is the tool for building up Demonstration Cases cases for validation activities. Completed templates are stored in the dedicated section about Templates from the preparation of validation activities.

The activities were organised around the topics reported in Table 15.

Activity N.	Topic	Group	Demonstrator
Activity I	CBRNE training exercise preparation with the FDDO	All	Technical demonstrator
Activity II	Pandemic Plan Revision	All	Mockup
Activity III	Knowledge Base and Taxonomy	All	Power Point presentation
Activity VI	ELSI guidelines and ELSI register	All	Power Point presentation

Table 15. Activities description and typology of demonstrator

4.2.1 Report on SecInCoRe components

During the meeting it was possible to observe attendees discussing mainly:

- Taxonomy, Ontology and Semantic Search
- Collaborative practices and ELSI

However, due to the fact that most of the comments were made by the Project Officer and by the reviewers rather than by end-users, they will not be included in this deliverable.

4.2.2 Results from the workshop

At the same time, it is possible to report some conclusion from the structured observations that took place during the Dortmund's meeting. The Dortmund meeting was an important step for the project to collect feedback from participants to calibrate the next steps of validation. It was possible for the consortium to better understand how to proceed in further project's activities and to identify the components that required further development.

4.2.3 What we learned for validation purposes

For validation purposes, the Dortmund meeting suggested that the general organisation of the meeting should be reviewed for next workshops and could not be applied to validation activities as it was. However, some positive results derived from the application of lessons learned in previous meeting were already visible.

The organisation of the meeting was not useful to communicate to participants SecInCoRe as a unified concept. The observation suggests that organising the workshop around different booths was not helpful to convey an overall idea of the project.

However, the positive side is that the opportunity to show a demonstrator, even in a mock-up form, helped end users better understand the concept and its functions, as also confirmed by participants who had also attended the First Lancaster Workshop.

The Demonstration Case Template was used by partners in charge of the stories and it is confirmed as a valid tool to structure demonstrations, collect information and organize activities and needs.

To conclude, it must be stressed that feedback from participants that already attended the Lancaster workshop were positive. Users were satisfied about progress accomplished by the project. In addition to progress relating to technical implementations, it is possible to conclude that the approach used in Dortmund was able to more effectively communicate project results to end-users, compared to the one adopted in Lancaster.

So, on the basis of feedback from the Lancaster and the Dortmund meetings the aim for future workshops will be to have a more concrete approach to demonstrate concepts and outputs based on stories and real Demonstrations.

In line with this, partners in charge of the validation activities will work on a better integration of the future Demonstration Cases, supporting the idea to have a comprehensive demonstration of project's outputs. To support the process, the standardised template has been used for this purpose and of course it will be strengthened to reach the aim of coordinating stories and different approaches.

*4.3 **Second Lancaster workshop***

On October 11th, from 9AM to 17PM, a SecInCoRe workshop with stakeholders (Table 16) from the Local Resilience Forum (LRF) took place in Lancaster.

Name	Title	Organisation
Mark Bartlett	Civil Contingencies Officer	Lancaster City Council
Ed Savile	Lead Officer - Social Responsibility	Blackburn Diocese

Table 16. Attendees to the Second Lancaster Workshop

SecInCoRe team
Katrina Petersen, Ulanc

Catherine Easton, Ulanc
Sarah Becklake, Ulanc
Torben Sauerland, UPB
Christina Shaefer, UPB
Paul Hirst, BAPCO
Daniel Bhenke, TUDO
Simona De Rosa, T6 ECO

Table 17. SecInCoRe's members to the Second Lancaster Workshop

The activities were performed according to the agenda in Table 18.

Activity N.	Topic	Group	Demonstrator
Activity I	Introduction to the system and what's behind-the-scenes	All	Power Point presentation
Activity II	Explore Graph View	Group 1: Ed Savile, Paul Hirst;	Technical demonstrator
		Group 2: Mark Bartlett, Torben Sauerland	Technical demonstrator
Activity III	Issues around Catalogue vs Library	Group Library: Ed Savile, Simona De Rosa, Daniel Behnke, Christina Shaefer Group Catalogue: Mark Bartlett, Sarah Becklake Torben Sauerland	Power Point presentation

		and Paul Hirst	
Activity VI	ELSI Guidelines	All	Presentation

Table 18. Activities description and typology of demonstrator

4.3.1 Report on SecInCoRe components

The aim of the report is to make a summary about:

- Taxonomy, Ontology and Semantic Search
- Collaborative practices and ELSI
- CIS concept

4.3.1.1 Taxonomy, Ontology and Semantic Search

Through dedicated exercises, users had the chance to play with the demonstrator experiencing the main functions implemented so far. Particularly, they had the chance to experiment the Semantic Search and the concepts that are behind it, namely the Taxonomy and the Ontology. In this sense, users expressed their positive feedback on the general concept of the Semantic Search as a tool that could help them finding data and information

One of the two users added a document on the demonstrator, then he performed a search in order to retrieve the same document and understand the categorisation. Actually, we were able to find the document and he agreed that the key-words assigned by the system correctly reflected the scope of the document.

At the same time, some issues were discussed on the assignation of tags to documents, because in some cases the users were not able to understand why some words were relevant and some others not. Particularly, in some cases the terms extracted as key words for the document were seen as too generic and not very helpful in providing additional information; in some other cases, key words were too specific to be relevant for a quick understanding of the document.

In order to solve these problems, it was discussed with the users whether it could make sense to insert manual tags for the documents. However, such an option was perceived as time consuming and not useful for a part of the attendees.

Regarding the organisation of the document, users stressed the need to have more accurate summaries for each document, and not only a random retrieval from the text. One of the users suggested to use Chapter headings to extrapolate the summary.

In addition, they asked to have the name of the author of the document (instead of the name of the system user who uploaded it) to facilitate information sharing.

Regarding the filters, both users suggested the need to improve it. Some feedback was given on the graph view that was not connected to other documents, therefore it was not possible to get access to more information.

4.3.1.2 Collaborative practices and ELSI

Through discussions on collaborative practices, it was possible to discuss the ELSI perspective in the design of the system. By looking at the demonstrator, however, users were not able to really judge the ELSI and they stated that currently the information stored in the database is not so transparent.

One user suggested to make the user's profile transparent and to make all main users' information visible. In addition, to enhance collaboration a system based on the reciprocity of the information exchange could help. Certainly these requests, while potentially useful from an end-users' perspective, raise very sensitive data protection issues and the consortium is working to address them in line with ELSI principles.

According to the users, however, ELSI guidelines should not be directly addressed to the users because this makes things harder for them. ELSI guidelines should instead be written for those who design and manage the system. In other words, transparency as understood in social sciences does not necessarily matter for end-users because they just to want to get results and understand them. On the other hand, IT staff and high levels personnel could be interested in ELSI-sensitive design. Even in this case, the issue has been reported to the ULANC team who will investigate possible responses.

The point that emerged clearly is that first responders need quick and easy access to the systems; discussions on the design principles system should not be addressed to first responders but to the people involved in the back office.

4.3.1.3 CIS concept

In relation to the CIS concept, security and sustainability issues were mainly discusses. One user stated that it could be difficult for emergency services to store sensible information on the cloud.

Regarding the sustainability of the system it was stated that such system should not be used for profit but for not profit aims.

4.3.2 Results from the workshop

The main results from the workshop can be summarised as follows:

First of all, the workshop was organised taking into account previous suggestions. In line with this, the workshop was organised following a plan focused on the interaction between stakeholders and Demonstrator Implementations working in real time.

Stakeholders involved in this Pilot Demonstration Case had the chance to play with a tool and this allowed the team to clarify certain aspects of SecInCoRe's implementation. In addition the small size of the group, in which SecInCoRe's staff interacted with only two stakeholders, facilitated in-depth reflections and discussions on workshop topics and favoured the collection of useful feedback.

For these reasons, stakeholders were satisfied of the workshop and they are still available for further collaboration with the SecInCoRe team in the next steps.

Other aspects were also clarified. For example, it is possible to confirm that a demonstrator is a very useful tool to discuss SecInCoRe's concepts and outputs with end-users. Furthermore,

activities should be better defined according to the final goal and according to the kind of stakeholders that are engaged in the activity.

In relation to the major topics that were investigated, the interesting points raised about the ELSI guidelines provided interesting insight to the ULANC team. In the same way, the suggestion to have a not-for-profit system gives important insights to the discussion on sustainability.

4.3.3 What we learned for validation purposes

The activity organised around the use of the Demonstrator Implementation for the Semantic Search greatly facilitated the discussion, with stakeholders moving from an abstract to a more concrete focus.

For validation purposes, it was possible to understand that the Semantic Search is a good way to present the Taxonomy to end-users since they can interact with the Taxonomy through the search.

The next steps will be to refine the topics selected for discussion and validation according to the stage of the development of the demonstrator, and the planning of future validation activities. In this sense, feedbacks have been collected from all partners and they will be implemented in the next stages.

5 Results from validation activities in Paderborn

5.1 Introduction about participants and aims

On October 25th SecInCoRe organised a workshop dedicated to validation activities with stakeholders (Table 19). The meeting took place in Paderborn, hosted by UPB.

Name	Title	Organisation
Detlev Harries	Chief Department Officer	Fire Department of Dortmund
Marco Sickmann	Officer	Fire Department of Paderborn
Grzegorz Wenarsky	Researcher	CNBOP, Center for Scientific Research Protection in Poland

Table 19. Attendees to the first validation case

SecInCoRe team
Rainer Koch, UPB
Torben Sauerland, UPB
Christina Schäfer , UPB
Linda Panzer, UPB
Ivan Cucco, T6
Simona De Rosa, T6

Table 20. SecInCoRe's members to the forst validation case

The aim of the workshop was to show SecInCoRe's concepts and outputs through conceptual presentation and through concrete interactions between the users and the SecInCoRe demonstrator.

The day was organised according the agenda presented in Table 21.

Activity Code	Topic	Demonstrator
Activity 1	Introduction "What is SecInCoRe"	Power Point presentation

Activity 2	Concept of the Semantic Search	Power Point presentation
Activity 3	Guest session: Experience interactive 3D crisis-scenario	N/A
Activity 4	Case Introduction	Power Point presentation
Activity 5	Experience SecInCoRe demonstrator	Technical demonstrator
Activity 6	Validation activity	Technical demonstrator

Table 21. Activities description and typology of demonstrator

The activities were organised to run a validation on the following concepts:

- CIS concept and derived principles informing the design of the demonstrator
- Taxonomy/Ontology and Semantic Search
- KB/Inventory

5.2 Participant background information

The three participants in the workshop were involved according to their different expertise and skills. The same background information was collected from all participants in order to understand the following points:

- Their previous experience in disaster management (e.g. in mitigation, preparedness, response, recovery, and/or business continuity).
- Their previous experience in the use of technologies for information exchange and multi-agency collaboration.
- Their previous experience in cross border operations, planning and training activities.
- Their previous experience in operation with multi-agency collaboration.

The three participants share a background in emergency services, both in planning and emergency, but strongly differ in regard to the kind of the work they perform in the sector. Two participants are directly related to the emergency phase, while one of them is more involved with the research aspects of the emergency sector. For this reason, it was possible to explore SecInCoRe's output from both points of view.

To have a better picture of the respondents, their profiles derived from the background information collected during the workshop are here reported.

Detlev Harries is Department Chief Officer of the Dortmund Fire and Ambulance Service and he has ten years of experience in disaster management as a volunteer and as professional fire fighter. During his work, he was involved both in incident planning and emergency and disaster response. Within such activities he served on scene as well as in the staff room. Regarding the use of technologies for information exchange, Harries asserts that he currently uses IT-systems in the staff room and in the control room. The use of IT systems is also relevant to exchange information with city crisis committee and police staff room. On the other hand, he does not use systems for planning in his daily working activities. Harries also has a

great experience in cross border operations. In particular, he joined training for industrial fires in the Netherlands. In addition, he worked as a consultant in planning for mass events in South Africa, Brazil, Poland and Austria. Regarding the experience in multi-agency collaboration, he has a range of experience in planning and operational activities with police, Red Cross organisations, companies and city departments at different levels.

Marco Sickmann is Field Manager for rescue services in the Fire Department of Paderborn. According to this current position, he is in charge of rescue services. Around 20 per cent of his working routine is devoted to searching. At the same time, he is involved in training people engaged in rescue services. In relation to the use of IT systems, Marco Sickmann asserts that to perform his work he generally uses Google and similar internet services. While Marco Sickmann does not have cross border experiences in his background, he has worked in operation with multi-agency collaboration, particularly with the Red Cross and partners at the local level.

Grzegorz Wenarski is Senior Specialist at the CNBOP-PIB Institute in Poland. He is specialised in research activities in disaster management. During his regular working routine, he has access to IT systems. Particularly, he uses to work with SharePoint, Google Drive and Redmine. Such systems are mainly relevant for sharing documents and improving communication with partners. In relation to cross-border collaborations, he has been working on a project aimed at creating an online tool for training fire fighters. Cooperation was established with fire fighters based in the UK, Belgium, Netherlands and Denmark. He was also involved in multi-agency collaboration with State Fire Service, Schools for Fire service, Police and other research institutes.

5.3 Main results from the validation activity

This section reports the validation results from the workshop; data were collected through three different activities that conducted during the Paderborn demo case:

- Structured participant observations;
- Semi-structured questionnaire:
- Semi- structured interview.

Comments and answers from end-users are reported anonymously; to this aim, end-users have been randomly named Attendee 1, 2 and 3.

5.3.1 CIS concept

Through dedicated questions in the questionnaire, the three participants were asked to share their impression on the CIS as presented by SecInCore's partners. Particularly, it was asked whether a CIS built according to SecInCoRe concepts and specification would improve their working routines compared to other systems that they are currently using or that they have used in the past. All participants agreed or strongly agreed with this statement.

Then, end-users were asked whether a CIS built according to SecInCoRe concepts and specifications could help increase collaborations and establish new partnerships. Two participants agreed on this point, while one was uncertain on such possibility and did not have a clear idea on this point.

All feedback collected from end-users was positive with regard to the capacity of a CIS built according to SecInCoRe concepts and specifications to make their work more time-efficient, by helping them find relevant information in less time. Two attendees strongly agreed with such statement, while one just agreed.

Even if only positive feedback was collected on the ability of the CIS, as designed by SecInCoRe, to improve working routines, enhance collaboration and make their job more time efficient, during the discussion about the nature of SecInCore some issues emerged.

On the one hand, the discussion focused on the managing authority perspective. Issue related to data sharing emerged very clearly during the discussion; due to different legal aspects in each organization, it is difficult to easily share data. Both Attendees 1 and 3 agree that the difficulty is closely related to organisational structure and to the fact that internal procedures differ across organisations even within the same country. In this sense, Attendee 3 stated that a crucial role could be played by some national institution which could take care of legal issues providing solutions at a transversal level.

Following the discussion on managing authorities, Attendee 1 agreed with the presentation made by UPB and suggested to have a two-layers system in which a national authority manages the coordination exchange at the national level, and a Pan European-level institution coordinates the exchange among European countries.

In addition to legal aspects, the function of the Semantic Search was also discussed with regard to its utility for a CIS that allows the gathering of different kinds of information. Positive feedback was shared by Attendee 3, who appreciated very much the possibility to access a CIS with data, information and best practices. In his view, the relevance of such a system is crucial when knowledge of best practices needs to be increased, particularly by having access to experiences generated in different countries.

Attendee 1 agreed with this statement, also stressing the relevance of such a system for collaboration enhancement. Indeed, the general mechanism behind the documents and data sharing is very much related to personal relations. SecInCoRe could go a step forward by enhancing data sharing and fostering collaborations even between unknown people.

The general feeling about the concept was positive. Attendees agree that, if such concept will be developed, it could be really of help to emergency services and researcher communities working on emergency since it would allow a faster and easier information exchange and collaboration.

5.3.2 Taxonomy and Search Function

During Activity 5, users had the chance to directly interact with the demonstrator and it was possible to collect their feedback on the main functions implemented.

Following instructions that were circulated by project partners, users performed a series of activities mainly based on the search and on the graph view.

During these activities, positive and negative feedback were received and are here reported.

The first issue that was confirmed by two users concerned the fact that documents stored in the Knowledge Base were difficult to read due to the non-descriptive titles used for the major part

of the documents. Users suggest to have titles that are comprehensible and directly linked to the actual content of the document to facilitate the consultation.

It is also suggested that documents should be sorted according to their quality; a shorter list of high-quality materials should be preferred to a long list of documents of lower quality. An additional modification requested is to make evident when a document has already been opened (e.g., using a different colour) and also add some key-words in the same line of the title allowing for a better comprehension of the document.

Furthermore, attendees discussed the utility of information related to the document that is presented by the system after a search for a specific word is performed. Particularly, one of the users confirmed the relevance of the summary and of the information on the author, source and data associated to each document.

On the other side, two users stated that the graph view is not something that could be of their interest nor applicable to their work. Indeed, such function seems more useful for people engaged in the background activities. Attendee 1 added that the graph view could theoretically be useful as a kind of mind map to help think about topics that were not taken into account. During the exercise performed in the workshop, however, the topics emerged from the graph view were not of practical help to think of other topics.

In the same way, also the classification of the topics according to their relevance within the documents seems to do not be very appealing for the users.

Following the visualisation of the documents, the possibility was discussed to edit results of the search (e.g. edit the summary). Attendee 1 stated that he would not use the edit function to avoid changing a document uploaded by someone else, as well as to reduce the workload associated with uploading a document.

In this sense, what emerged clearly from all users is that this kind of system will be used if it is a real way to improve the time-efficiency of their working routine.

Then, the case in which the user who performs the search cannot have access to the document due to restrictions was discussed. In that case, the SecInCoRe procedure is that the system will give the user the email address of the document's author, so that a request for the document can be directly addressed to the author.

Such a function was very much appreciated by the users, because this will increase the chance to obtain documents from people that are already not part of your network, increasing exchange but also collaboration. Moreover, Attendee 1 stated that he would be glad to share his document if the users who received the information agreed to share their own results or achievements. This mechanism could also be good to enhance the storage of the document of the system while also sustaining collaborative practices and networking.

The main feedback on functionalities related to the Taxonomy and to the Search Function provided by SecInCoRe is summarized in the table below.

In the questionnaire, attendees were asked to think about the different types of search that were used during the day (search based on keywords; filters based on categories; graph-based search), and consider how useful they would be in their standard work practice[4].

	Attendee 1	Attendee 2	Attendee 3
Keywords-based search	1	1	2
Filtering based on categories	2	2	1
Graph-based view	3	3	3

Table 22. Ranking the Search Functions

As it is possible to see in Table 22, two users agreed in ranking the keywords search as the most useful, while the third user preferred the filtering. At the same time, the three attendees agree that the less relevant function is the graph-based view.

Then, attendees were asked to rank the different types of search according to how useful would they be when exploring a topic with which they are not familiar[5]. In this case, two users confirmed their selections assigning the same score to the previous question, so the keywords based search remains the most useful. One user, on the other hand, assigned a higher score to the graph view, which seems more relevant when searching for new topics rather than when searching for already familiar terms.

	Attendee 1	Attendee 2	Attendee 3
Keywords-based search	1	1	2
Filtering based on categories	3	2	1
Graph-based view	2	3	3

[4] The rank is in order of usefulness from 1 to 3, where 1 is the most useful and 3 is the least useful.

[5] The rank is in order of usefulness from 1 to 3, where 1 is the most useful and 3 is the least useful.

Table 23. Ranking Search Functions in order to explore new topics

5.3.3 Knowledge Base

Exploring a past disaster case stored in the Knowledge Base, two users agreed that having access to similar information stored in a common format for different cases is extremely useful. Two users asserted that they would use the past disaster database to collect information, instead of just using Google or asking a colleague.

Looking in detail at the information stored for one past disaster case, one user asserted that he would prefer an additional amount of information stored in the template.

Discussing the general amount of information stored in the Knowledge Base and searchable through the Semantic Search, users expressed their concern about having some sources of information that are not directly related to emergency services. For example, a newspaper article was retrieved during the search. Users seem willing to trust a system based on information generated by emergency services, but they are not confident in having also sources that are not so trustworthy.

6 What stakeholders engagement means for SecInCoRe and how it was performed

The aim of the chapter is to discuss stakeholders' engagement in relation to the SecInCoRe activities performed so far in order to have a clear idea of positive and negative aspects and consequently improve further activities, that will be described and analysed in D5.5.

Stakeholder engagement is at the base of the several activities within the project. Particularly, this engagement is defined in the forms of domain analysis, design and development workshops, and in validation and evaluation activities. This plan implies the participation of a group of experts in their field of operation that can contribute to the construction of a trusted environment for participation, contribution, and problem solving. What is gained from these activities is an alignment of the concepts and framework created by the SecInCoRe consortium to stakeholder routine and guidelines. This has to be done in an environment that is user-friendly and will encourage stakeholders' participation and continuous contribution.

Indeed, this has been invaluable in terms of identifying the current issues affecting responder organisations throughout Europe and expanding the research into why and how these organisations exchange information currently, the problems they face as they move forward, and how they might wish to do so in the future. Having end-users involved in the development of the project and throughout its lifetime should ensure that the project is developing in an ultimately useful way and not simply following technological development for the sake of it. It has also meant developing tangible outputs that can be engaged and interacted with by the stakeholders in order to be able to see how their actions are influenced by technology, how what they say and what they do align (which are never exact matches), and provide an opportunity to learn more about how stakeholder practice meets, or does not meet, consortium expectations. Finding this balance between user input and collaborative technological interaction is necessary for maintaining credibility of all parties involved.

The project has employed so far a wide variety of stakeholders from across Europe and from a number of fields of expertise: police, fire, rescue, civil protection, health, coastguard, volunteer agencies (Red Cross) and military organisations (counter-terrorism and explosive ordnance disposal). The interactions began in the form of supporting the building of disaster case studies were and defining datasets through interviews and questionnaires. Several interactive and collaborative design workshops followed (plenary and six stakeholder/AB workshops, with a third AB-specific workshop due to take place in M34 of the project). In particular, two close working relationships have developed: in the UK between Lancaster University and the Lancashire Local Resilience Forum, (a formal structure within the UK's emergency response structure); and in Germany with the Dortmund Fire Department. In addition, stakeholders have also been represented within the Advisory Board structure since the project commenced. In addition, smaller numbers of the AB have taken part in dedicated development meetings for specific issues. More information about the meetings is contained in the First and Second Reports on Advisory Board activities, namely in D1.4 and D1.6.

Apart from meetings with AB members and first responders, representatives from the relevant industrial or technology sector have also taken part in research questionnaires and interviews conducted by the SecInCoRe team. For example, interaction with stakeholders from the industry sector took place at events such as the B-APCO meeting in 2015 at Manchester, as the feedback from the people in the development was considered valuable. At the Border Surveillance and Search & Rescue event in Crete organised by the Centre for Security Studies

(KEMEA), a questionnaire was prepared and distributed in the participants' folder, collected at the end of the event; during the event there were interviews with operational and field practitioners regarding the operational models and data most valuable during their daily tasks and emergency cases; the feedback was analysed and included in deliverables of WP2 and WP3. Input regarding crisis management models were included in WP4 deliverables.

6.1 Main successes from stakeholder engagement

As a whole, interaction with the stakeholders has proved an invaluable resource and helped the project progress. Engagement was particularly good at the beginning of the project due to an initial enthusiasm for the goal of the project. The active participation at the initial stages of stakeholders with great expertise in their respective areas helped the project form a solid database of the disaster events that form the foundation of this work. Extensive conversations and interviews allowed for the definition of the datasets which have set the ground for the taxonomy and ontology. Last but not least, the stakeholders' involvement (all from their respective areas of expertise) has been crucial for the evolution of the SecInCoRe consortium's conceptual design and to its shaping, through participation in interviews and to the conceptual workshops. Indeed, stakeholders have assisted the project by defining their needs and concerns in modern emergency and crisis management and providing the consortium with information whenever required. The more collaborative engagements have also produced opportunities in shifts in definition of user needs that resulted from direct engagement with SecInCoRe CIS concepts as well as shifts in concept design within the consortium – a two-way process.

6.2 Main challenges in engaging stakeholders

Several challenges regarding stakeholder engagement have also emerged. First of all, identifying and then attracting the right level of stakeholder is always challenging. Theoretically, strategic-level and financial managers would be the ones to approach, however, strategic-level managers are usually too heavily engaged in the management of their own organisations to get involved in speculative 'proof-of-concept' projects and financial managers will lose interest when they discover that there is nothing at the end of a project which can be assessed for production viability or budgeted for. Secondly, public safety organisations are increasingly having to manage decreasing budgets and this makes it difficult to justify involvement in a project where there is no clear, short-term realisable value for those organisations; even the incentive of paying for time and attendance costs is reducing in impact as a result of the increased opportunity costs from losing members of staff for periods of time, either at meetings or whilst engaged on project activities. In addition, diaries are filled often many months in advance – often long before project consortia (who need to demonstrate concrete and meaningful progress to the invitees) are ready to announce meeting dates and this can impact on getting a meaningful group of external attendees together. This impacts very much on the ability of stakeholders to attend and participate to activities. Despite this, SecInCoRe has been fortunate in having a group of dedicated AB members who do make every effort to attend key meetings

Going in detail, apart from difficulties of the synchronisation and coordination of getting stakeholders that are very active in their field (such as active officers, managers, academics) from different countries and disciplines to one place for a meeting, probably the more

challenging task that has been experienced in the SecInCoRe project is the projection of a clear objective of the project, hence the requirement of multiple conceptual workshops.

Since this project addressed the development of a new concept for a Common Information Space it demanded the extra effort in the refinement of the concept and the definition through procedures that required clarification and modification through the evolution and progress of the project, which has slowed down the development of the tangible and interactive elements of stakeholder engagement further engagement and feedback. This lengthy conceptualising process has led to comments from the AB members asking for a practical demonstration of some elements of the project concept. While some of the early interactive engagements stumbled on the surface as a result of the lack of an interface designer on the project, the consortium is working on improvement based on these experiences for further demonstrations. This is planned at the next AB workshop event in February 2017.

6.3 Lessons learned and plans for further involvement

In conclusion, it is possible to state that the concepts and the main promoting factor for next activities will be the availability of a system that stakeholders can work with, even at basic level, but that it would demonstrate and make visible underlying ideas of the SecInCoRe consortium, highlight the novelties of this system, pulling the focus away from the lack of interface and instead highlighting developments such as the ELSI framework, the fast yet insightful provision of the information and conclusions from lessons learnt, the concepts for building a trusted and user-friendly CIS environment, and the innovations where interaction and communication amongst them is possible in a seamless way.

The aim in the remaining months will be to organise a final AB Workshop with a clear focus on practical demonstration, in order to maximise the potential for end-user evaluation and feedback.

In summary, during the remaining months of the project, stakeholders will be engaged during the next Demonstration Cases as already explained in the previous chapter, at the Joint Projects Event, and at the ELSI conference; and at the third AB workshop. It still remains to be clarified whether external stakeholders will take part to the final review process.

7 Next steps and planning for next Demonstration Cases

7.1 Lessons learned on the validation strategy

The validation strategy has been tested in three Pilot Demonstration Cases; they have been crucial to understand how Demonstration Cases should be organised to better communicate SecInCoRe to end-users and stakeholders and to gather useful feedback for validation purposes. In this final chapter, we summarize the lessons learned in previous Pilot Demonstration Cases that will be applied to all future validation and evaluation activities. We also present some reflections on persisting issues that consortium partners would need to address to more fully convey the relevance and potentialities of the project to stakeholders, and to extend the scope of validation and evaluation activities to aspects of the CIS concept that have not yet been validated.

Regarding the general organisation of the meetings, previous experiences suggests that to gather detailed and reliable feedback on validation activity it would be preferable to involve in each Demonstration Case only a small group of end-users. Our experience in previous Pilot Cases suggests in fact that it is difficult to perform detailed validation activities with a large group of users, particularly because end-users of interest to SecInCoRe are generally very busy and validation workshops are consequently constrained within strict timeframes. For this reason, validation workshop with larger groups do not leave enough time for face-to-face interviews, which provide instead an opportunity to gain a more in-depth understanding of individual perspectives and reactions to SecInCoRe demonstrations and of their linkage with end-users' current practices. We suggest therefore to organise several smaller Demonstration Cases rather than fewer, larger Demonstration Cases - even if this entails more efforts in terms of preparation and could be more time consuming.

Beyond issues of scale, we also observed that it is preferable to organise separate workshops dedicated to a specific topic rather than include too many topics for discussion in a single workshop. The reason is twofold: first, in this way, discussions can be more focused and can proceed to a greater level of detail; second, this leads to a more careful selection of the end-users or stakeholders according to the specific topic that will be addresses. Since, in the case of SecInCoRe, different topics must be validated in each case, organizing the discussion around a single thread would allow Demonstration Case organizers to select and to invite users with skills and expertise that are more aligned with the focus of the validation.

An additional crucial element identified in previous activities is related to the use of a Demonstrator to validate concepts and outputs. Using a technical Demonstrator that can be adapted to the scope of the validation increases end-users' understanding of the aims of the validation activity and improves their capacity to relate the demonstrated activities to their current practices, in this way providing concrete and relevant feedbacks. Such lessons are partly based on the observation of the activities performed, partially on direct suggestions of the participants. Participants' suggestions and detailed feedback has been very useful for technical improvements of the demonstrator. Similar comments also emerged during the Paderborn case; comments and suggestions are now leading the refinement of the demonstrator that will be shown to the end-users in future Demonstration Cases.

7.2 Reflection on issues that shoud be addressed in future Demonstrations

Although the lessons gathered in Pilot Cases have helped refine the validation methodology and the practical organization of Demonstration Cases, some issues of a more conceptual nature remain to be addressed to: (a) improve the quality of data collected from end-users through validation and evaluation activities; (b) extend the scope of validation and evaluation to components of the CIS concept that have until now been only marginally included in Demonstration Cases.

The reflections here presented are based on a critical elaboration of the statements and impressions collected from end-users in different validation activities in the light of our knowledge of the projects' aims and of its still untapped potentialities. Our main concern is to highlight the obstacles that limit the capacity of end-users to envision the possible outcomes and impacts of SecInCoRe – hence, constrain the possibility to collect data and feedback from end-users on the medium- and long-term relevance of the project. The reflections here presented are primarily addressed to consortium partners in charge of the technical and conceptual development of different aspects of the CIS.

The premise for the observations that follow is that a Demonstration Case for a socio-technical system such as SecInCoRe can only be a simulation. Unless end-users and stakeholders (at the individual, organisational and wider societal level) claim ownership of the system and shape its functioning through day-to-day interactions in a real-life setting, the social aspects of a CIS and the social and organisational context in which a CIS may be operating must be 'imagined' by end-users on the basis of: (a) the limited social setting in which Demonstration Cases take place; (b) the contextual elements provided by the SecInCoRe team, in either a technical or conceptual form. In this regard, we believe that several and often minor improvements in the organization of Demonstration Cases and in the functioning of Demonstration Implementations could help end-users better contextualise the experiences taking place in a Demonstration Case. This would enhance their ability to provide feedback and assessments projected towards the potential future outcomes and impacts of SecInCoRe rather than remain focused on the (necessarily limited) capabilities of the demonstrators they have to opportunity to interact with in the limited timespan of a Demonstration Case.

Starting from this assumption, we provide below some inputs and elements for the teams involved in the development of technical and conceptual elements.

Particularly, we recommend that a thorough discussion have to be undertaken among the implementation and development teams on the points below highlighted to harmonise their aims and to foster cooperation on the design of future Demonstrations. Once that the teams will reach a mutual agreement on the plans and strategies to address the issues reported below, Demonstration Cases will be organised accordingly. Particularly, the workflow will be organised around Demonstration Case Templates offering the tools to organise conceptual and technical components and to adapt it to any advancements in the demonstrators.

First of all, we suggest that greater attention to details of what is presented to end-users should be used in each and every step of a Demonstration Case. It is in fact clear from users' reactions and suggestions that they make use of all the elements presented during a Demonstration Case to extrapolate conclusions on how a fully-developed system would work in their routines and organisational settings. For example, in the lack of specific indications concerning the managing authority of a fully-functional CIS or the lack of a clear quality control on the

documents that emerge from the search function (see for example the comments above on the presence of dubious sources or articles from the mainstream press). Perhaps a reconsideration and a preliminary quality vetting of the documents accessed through the Semantic Search is needed to ensure that end-users do no reach unjustified conclusions on the inherent weakness of the system.Second, although the development of a refined User Interface (UI) and a focus on end-users' experiences with the actual Demonstrator are not necessarily primary objectives for the project, any obstacles to a smooth end-user experience during a Demonstration Case may send wrong signals on the solidity of the concept. For this reason, according to the available time and resources further enhancement responding to end-users' request could be addressed to help end-users focus on the potentialities of the concepts rather than on the weaknesses of the demonstrator. This is particularly relevant with regard to the perceived incapacity of the system to facilitate the browsing, skimming and exploration of the long list of documents produced by the search. It would perhaps be useful to present users with a fewer number of document whose tagging, titles and summaries have been reviewed by team members prior to a Demonstration Case to convey a birds-eye view of the documents' content. This would simulate the experience of a fine-tuned tagging and content extraction function.

Third, the Scenario prepared for a Demonstration Case should provide more details on the (fictional) organisational context and on the managing authority behind the activities practiced in a Demonstration Case. This would help users overcome their doubts on the actual reliability and trustfulness of a future system based on the SecInCoRe concept. Although different sustainability and management models are possible for SecInCoRe, leaving the possible structure of the managing authority entirely open to end-users' interpretations diverts their attention away from the actual focus of the demonstration and directs it to issues that are in most cases beyond the scope of the actual activities undertaken with them.

Finally, and perhaps most importantly, the current disconnect between the ELSI/ collaboration principles underlying the SecInCoRe concept and the actual practices performed by end-users in Demonstration Cases makes it difficult to validate key elements of collaborative practices (such as the stability of a collaboration network, the definition and pursuing of shared goals, sense-making, articulation work, interaction mechanisms and their relation to the politics of information sharing and control, configuring awareness). The fact that ELSI are currently presented as theoretical principles and guidelines, rather than being visible in the actual practices taking place during a Demonstration Case, can explain the reaction of most end-users who see them as abstract design principles that can be only addressed to designers and managers of the system. Furthermore, the disconnect between their concrete daily practices and the form in which ELSI are presented can also justify their feeling that they would place too heavy a burden on their day-to-day operations. It is clear that end-users are not assisted in their efforts to appreciate the relevance of ELSI for their work and cannot assess the relevance of the work made on this aspect within SecInCoRe.

The integration of three crucial aspects of the CEIS in the recently deployed version of the OpenAtrium platform (identity management, collaboration and communication functionalities and Semantic Search) provides however the potential to include collaboration activities in future Demonstration Cases. We strongly advise that this potentiality should be exploited in future Demonstration Cases, and that the possibilities for making ELSI guidelines and principles more visible to end-users through the integrated OpenAtrium platform should be further developed.

7.3 Plans for the upcoming months

At the moment of writing, a timeline containing all validation and evaluation activities that have to be performed by the end of the project has been shared and agreed with all partners. For each of the activities, projects partners that are more involved with the output that will be validated will support the work of validation and evaluation. Currently, the plan about the validation and evaluation activities is to have three sessions dedicated to validation and three sessions on evaluation.

More in detail, the validation will be performed on the components that can be shown with the use of a demonstrator and will be performed with end-users; on the other side, the evaluation will be more at a conceptual level and will be organised with high level stakeholders engaged in the field.

In this sense the validation will be organised to validate the following components:

- Knowledge Base and Inventory
- Taxonomy, Ontology and Semantic Search

To validate such project's output, two Demonstration Cases will be organized with Italian Fire Brigades and the Italian Civil Protection.

Regarding the evaluation activity, the conceptual project's outputs that will be evaluated will be:

- CIS concept
- Collaborative practices and ELSI

For the ELSI evaluation, a dedicated workshop at the Computer Privacy and Data Protection (CPDP) Conference with a selected community of users strongly engaged on the issues related to data protection and privacy will be performed. While for the CIS concept will be organized a dedicated activity with members of the Advisory Board and another activity with selected stakeholders that will attend the Joint Event.

The timeline for next activities is reported in Figure 16.

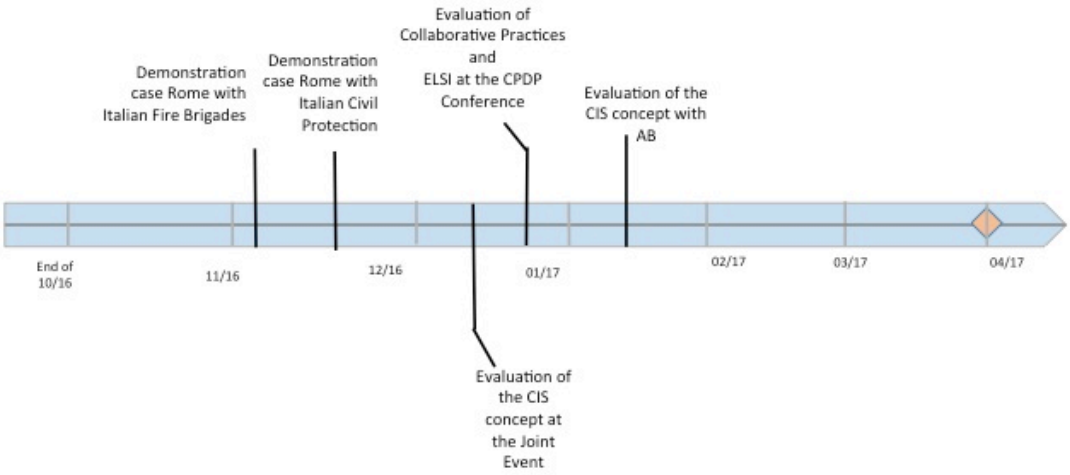


Figure 16. Timeline for validation and evaluation activities

8 Literature index

Bannon, L. and Bødker, S. (1997). Constructing Common Information Spaces. In ECSCW. Retrieved from http://www.ul.ie/~idc/library/papersreports/LiamBannon/ECSCW.htm

Kuhnert, M., Wietfeld, C., Paterour, O., Georgiev, A., Petersen, K., Büscher, M., Pottebaum, J. (2015). Next Generation, Secure Cloud-based Pan-European Information System for Enhanced Disaster Awareness“. In (L. Palen, M. Buscher, T. Comes,and A. Hughes, eds.) Proceedings of the The 12th International Conference on Information Systems for Crisis Response and Management (ISCRAM), Kristiansand.

Pottebaum J., Kuhnert M., Schäfer C., Behnke D., Büscher M., Petersen K., and Wietfeld C. (2016). Common Information Space for Collaborative Emergency Management. In Proceedings of the IEEE International Symposium on Technologies for Homeland Security 2016, Boston.

Rolland, K., Hepso, V., & Monteiro, E. (2006). Conceptualizing Common Information Spaces Across Heterogeneous Contexts: Mutable Mobiles and Sideeffects of Integration. CSCW ’06 Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work, 493–500.Sage Publications. ISBN 0-7619-2553-8

Schmidt, K., & Bannon, L. J. (1992). Taking CSCW seriously. Computer Supported Cooperative Work, 1(1), 7–40. http://doi.org/10.1007/BF00752449

Yin, R. K. (2003). Case study research, design and methods, 3rd ed. Newbury Park:

9 Appendices

9.1 Templates from the preparation of validation activities

9.1.1 CBRNE training exercise preparation with the FDDO, Dortmund Pilot Case

Name	Date	Reason For Changes	Version
SDR and IC	01.06.2016	Collating information from UPB slides on FDDO story; requesting clarifications and integrations	V1

Demonstration Case Identification

Demonstration Case ID (to be assigned by T6 ECO):	DC1	Demonstration Case Version (to be assigned by T6 ECO)	V1
Demonstration Case Name:	CBRNE training exercise preparation with the FDDO		
Person/Unit in Charge:	UPB	Last Updated By:	Simona De Rosa and Ivan Cucco
Date Created:	01.06.2016	Date Last Updated:	16.06.2016

General Information on the Demonstration Case

Demonstration Case Name: CBRNE Training exercise preparation
Short description of the Demonstration Case (to be completed by T6 ECO)
The Fire Department of Dortmund (FDDO) needs to prepare a CBRNE training exercise and uses SecInCoRe to get internet access, information and contact. This story is being constructed for June the review meeting. The aim of the story is to show that SecInCoRe provides: Simple access to the network for collaborative planning activities The possibility to find the right information and contacts to solve difficulties in the planning

process

Reduce the efforts/costs for authoring of realistic scenarios (including preparation for the dynamics of such an exercise) by selection of IT support tools, direct or indirect content retrieval

The concepts / components and functionalities that will be mobilized and shown through this story are:

Inventory

Taxonomy

Search

NEC

The added values of the system highlighted by this story-based demonstration are:

Capacity to easily obtain safe network access

Access information from other organizations that is not in the public domain

Get the information in a structured way

Obtain contact details to solve difficulties in the planning process

Which members of the SecInCoRe Team contributed to the documentation of this version of the Demonstration Case?

Responsible: UPB (Torben, Jens, Christina)

Planned: Technical contribution: TUDO (Daniel, Alex)

Planned: Content contribution: KEMEA, BAPCO (Yiannis, Paul)

Collating information in the template: T6 ECO (Simona De Rosa and Ivan Cucco)

Please list all the stakeholders / end-users that contributed content or provided input for the Demonstration Case Template (they helped construct stories, identify aims, define use cases etc)

Name	Position, department and organization
Torben Sauerland	UPB
Jens Pottebaum	UPB
Christina Schäfer	UPB
FDDO Staff (Got the exercise details a time ago, hard to say who gave it to us)	FDDO/IFR

FDDO

One exercise planner

FD Bremerhaven

Tabea Schwandt (see if to integrate in one or both stories)

Demonstration Case Scenario

The demonstration scenario is narrative describing a hypothetical but realistic situation (ideally co-designed by stakeholders and SecInCoRe team members) that provides an agreed-upon starting point for participants to (a) define the overall aims they want to achieve during the Demonstration Case; (b) identify the challenges they will have to overcome to achieve these aims. Feel free to choose the most appropriate format for the narrative, but please provide as many details as possible on the following points:

The starting situation and how it relates to stakeholders' current practices

What are stakeholders trying to achieve in this demonstration scenario

What do stakeholders need to achieve their aims

Who participated in defining the scenario, and which were the main steps in the construction of the scenario (meetings, workshops, conversations etc)

Were the stakeholders who contributed to the definition of this scenario already familiar with the SecInCoRe concept?

The starting situation and how it relates to stakeholders' current practices

Among its activities FDDO uses to plan big training exercises.

An example of the current practice is shown by Exercise "Stein der Weisen" that is a large-scale exercise of a CBRNE incident (02.04.2011). The exercise foresees that several districts are involved and there is a strong collaboration with various units and in various fields. Other details are:

Observations in the field and in command cars ELW1 and ELW3

One of the exercise objectives: Validation of a concept for CBRNE detection

High dynamics: Exercise control means improvisation; decision makers are free in their decisions (constructive learning)

For this scenario, FDDO is planning a new CBRNE training exercise similar to "Stein der Weisen" and uses SecInCoRe to get internet access, information and contacts. The new training exercise should start in a few weeks and so the new exercise planner leads the preparation following instruction provided by the Head of the FDDO.

What are stakeholders trying to achieve in this demonstration scenario

The aims and challenges identified for this scenario are:

According to the instructions given to the exercise planner by the Head of the FDDO, a new but realistic scenario should be used in this new training exercise to:

Enhance the variety of participants

The exercise should be based on one of the past disasters (participants can find past disasters in the SecInCoRe Inventory)

The exercise should be supported by information systems where necessary

The exercise should last a few days, because the Head of the FDDO want to know how the FDDO can treat long time CBRNE events

Inter-organisational cooperation is one of the main objectives; the Head of FDDO has not however instructed the exercise planner about the organizations that have to be involved (so identifying them is one of the challenges)

The prerequisites for this scenario (plan a training exercise similar to CBRNE using SecInCoRe) are:

FEU (Federation of the European Union Fire Officer Associations) owns a CIS and many European and national organizations participates in it

What do stakeholders need to do to achieve their aims?

To achieve the aims of planning an exercise with the desired characteristics, the exercise planner proceeds through several actions and steps:

She starts the exercise planning by reviewing the last CBRNE exercise

After she is informed about the last exercise, she needs inspiration about a new / extended scenario which can last for a few days (so she should identify other cases that are relevant for planning)

She prepares the scenario and a first draft for the exercise

He should evaluate, if support by an information system is helpful and finds an important one

She contacts the Bundeswehr DEKON and the THW and invites them to plan the exercise together in Dortmund

Additionally she invites BBK staff she knows, which coordinates the CBRNE detection units in Germany

The guests arrive at the FDDO and need internet and CIS access

They discuss about the different aims and capabilities of their units

The FDDO exercise planner needs to get an idea what the Bundeswehr DEKON is able to do

They discuss about the difficulties with heavy suits and respiratory masks in a CBRNE case and find results from a EU project which helps solving the difficulties

They discuss further and prepare the new training exercise

They store the result at the "public" part of their storage

The resulting .pdf is automatically inserted into SecInCoRe

Added Value:

Get easy and safe network access

Get non-public information from other organizations

Get the information in a structured way

Get in contact with responsibles

Zero scenario: The information is stored internally at the organizations and has to be send to interested people. They have to know who could be a good person to contact.

SecInCoRe System Components needed for the Demonstration Case

Please describe all the components of the SecInCoRe system that stakeholders will interact with during this Demonstration Case. Please include both technical implementations (prototypes - demonstrator implementations) and conceptual representations (delivered through presentations, booths, diagrams etc). For each component, please indicate the tools that you think will have to be used during the Demonstration Case such as:

Mock-ups (pre-designed demonstrations that mimic functions or possible uses of the SecInCoRe system)

Demonstrator implementations (prototypes) for end-user interaction

Conceptual tools (e.g., booths where team members introduce specific concepts / components and discuss them with end-users)

The SecInCoRe components that will be show through this story are:

The search will give access to distributed data and parts of the Inventory.

To refine the search requests parts of our Taxonomy is used

To get internet access the NEC is used

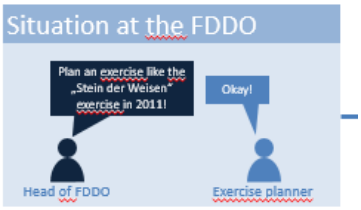
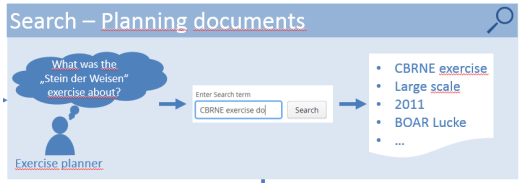
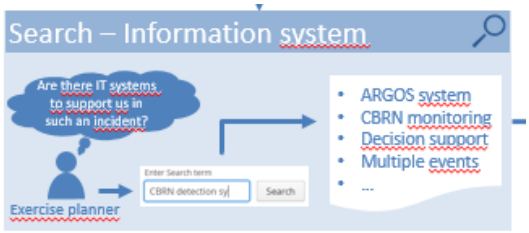
Timeframe and roadmap for the Demonstration Case

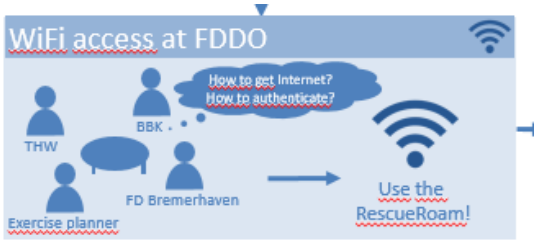
Please explain for how long stakeholders will be involved in the Demonstration Case and provide indicative start and ending dates. If possible, please provide details on any planned activities or interactions between SecInCoRe team members and stakeholders. Please keep track of all interactions between SecInCore team has with the involved stakeholders and about the

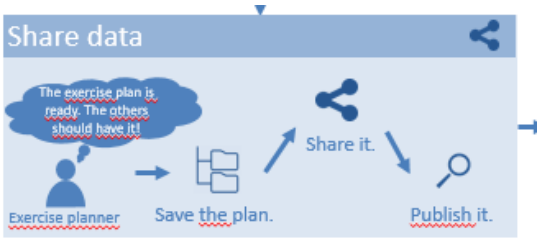
outcome of such interactions

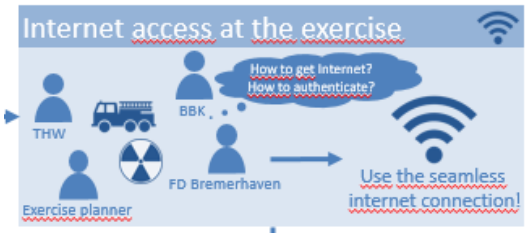
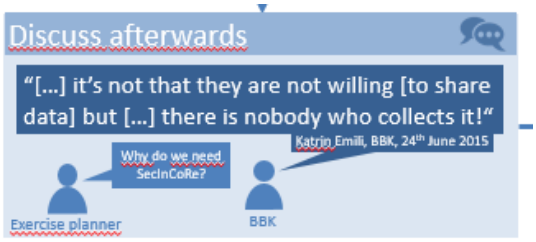
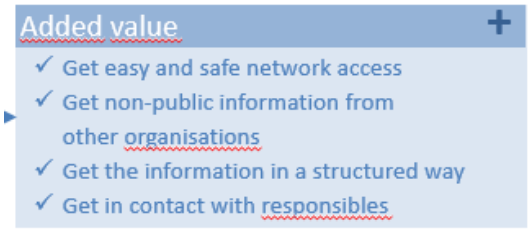
The FDDO people will mainly comment/ maybe interact a bit but will not be crucial to tell the story.

Use Cases associated with the Demonstration Case

Poster	Story telling	Screen
	The Fire Department (FDDO) is planning a large-scale CBRNE exercise similar the „Stein der Weisen" exercise in 2011. To plan the exercise, SecInCoRe components are used by the exercise planner.	blank
	The exercise planner is new at the FDDO He needs to get an overview of the „Stein der Weisen" exercise ----- He searches for "CBRNE exercise dortmund" He finds the "Stein der Weisen" exercise documents and get an overview about the exercise	Search for "CBRNE exercise dortmund Resultlist Open "Übungsbefehl" Open a presentation with photos
	Last time IT was hardly used in the exercise The head of the FDDO wants to include information system support in the exercise The exercise planner is wondering which IT system could help in this scenario ---- He searches for "CBRN detection system" Get too many results	Search for "CBRN detection system" Resultlist Use filters Open ARGOS presentation

	Refine his search by setting the filters	
	The head of the FDDO wants the exercise to care with a long term CBRNE incident and to include additional participants The exercise planner needs inspiration about a new scenario to use as a basis --- Searches for "CBRNE long term" Find a document about the Sarin incident in Tokyo => Use this incident to adapt it for DO Look at some other search results Find a document about an exercise where THW special CBRNE unit was involved Use the contact data of the document to get in touch with the THW	Search for "CBRNE Long term" Resultlist Open "Sarin" document Back to result list open THW document Write an e-mail to the THW
	He invites the THW special recovery unit and the Federal Office of Civil Protection and Disaster Assistance (BBK) to discuss a combined exercise They arrive at the FDDO and need internet access -- Explanation from Daniel	Blank. NEC Demo

	They start to discusss on difficulties within a CBRNE incident, especially with the respiratory protection They are curious, if there are new solutions to combine heavy suits with respiratory masks --- They search for CBRN respiratory protection They get too much results They use the filters They find an interesting deliverable of the EU project IfReact It explains new solutions for respiratory protection in CBRNE case	Search REsultlist Use filters Open IFReact Deliverable
	The exercise planner prepares the new training exercise after the meeting The resulting draft is shared with all participants The folder is password protected. They discuss if the document is public or remain intern. They decide to share it. When finishing the document it is made searchable in SecInCoRe. The concept plans an expiration date to define how long the document is valid.	File is saved in folder Demonstrator – Share view isd opened The Folder is shared with the group It is password protected The Folder is shared with SecInCoRe The document is searched and found

	After a month of preparation, they start the exercise When the different units are at the exercise locations, they use the seamless internet connection and get internet and CIS access using different channels (LTE, WiFi, etc) -- Explanation from Daniel	Blank. NEC Demo.
	At the exercise, the exercise planner discusses with staff from the BBK , about the advantages of SecInCoRe Katrin Emili from the BBK remembers her comment on the need for a concept like SecInCoRe:XX SecInCoRe addresses this issue by creating a socio-technical system	Blank.
	Explain the added values as described	Blank.

Prerequisites list:

TODOs for FDDO Story

Story I

Search for „CBRNE exercise Dortmund“ results in at least 5 documents. “Übungsbefehl” ist eines davon.

4 Dokumente hochladen, checken ob da.

"Übungsbefehl"

Author: Fire Department Dortmund (Mailto Link to sauerland@cik.upb.de)

Preview Text: The „Stein der Weisen" exercise deals with a big CBRNE incident in Dortmund.

Topics: Training Exercise, CBRNE

Date: 02.04.2011

Source: Fire Department Dortmund

Story II

Search for „CBRN detection system" gives at least 30 results.

ARGOS ist eines davon

Filter auf "Information Systems – Type – Decision Making" ergibt nur noch ARGOS als Resultat

ARGOS

Author: PDC-ARGOS – mailto: sauerland

Preview Text: Handling muliple events, Monitoring radioctivity, Datapresentation (N, R), Dispersion Calculations (R, N, C and B), Modelling (R and N), FoodDose Calculations , Urban Dose Calculation

, Countermeasures R, GIS functionalities, Data Publication

Topics: CBRN, Information System

Date: 1.10.2009

Source: SecInCoRe Inventory

Story III

Search for „CBRNE long term" gives at least 40 results

Filter to past incident leads to Document B plus Document C as results

Sarin paper

Author: St Luke's International Hospital – mailto: sauerland

Preview Text: In the morning of March 20, 1995, a terrorist attack by a religiously motivated cult resulted in the release of a toxic gaseous substance in five subway cars on three separate subway lines. The attack occurred during the Monday morning rush hour, when it was anticipated that commuter traffic would be at its peak. These chemical agent releases were timed to occur at a subway convergence point underneath the Japanese National Government's ministry offices. As a result of the attack, 11 commuters were killed and more than 5,000 persons required emergency medical evaluation.

Topics: CBRNE, Incident

Date: 1.4.1996

Source: Universiy of Paderborn – C.I.K.

Stärke Nachweis SEB ABC

Author: THW special recovery unit (mailto Link to: sauerland@cik.upb.de)

Preview Text: The Special Unit for Salvage ABC (SEB ABC) is in case of need temporarily compiled from locally units. It is a special unit to treat with CBRNE incidents.

Topics: CBRNE, THW

Date: 01.07.2014

Source: THW - Referat E1

Story IV

Daniel

Story V

Search for “CBRN respiratory protection“ leads at least to 40 results

Filter to „Datasets – Operational Information - Resources - Material“ leads to:

Deliverable of IFReact

Author: IFReact – Mailto libk zu sauerland

Preview Text: CBRN protective garments for need to provide protection protective clothing with innovative respiratory protection. There is still no protective suit which at the same time offers optimal protection and optimal equipment will include, besides protective clothing with an integrated respiratory protection, a full compatibility of the protective suit and respiratory protection is one of the main goals

Topics: CBRNE, Triage

Date: 10.11.2014

Source: University of Paderborn

Story VI

Upload a document via the seafile client and share the document with a group

The result document has to be crawlt in the search and found serarching for “CBRNE exercise”

document with a few lines of text /Headers tagged in “Datasets- Planninginformation- Scenario Documentation – Training exercise”

Author: Fie Department Dortmund, THW, BBK– Mailto libk zu sauerland

Preview Text: A long term CBRN exercise based on a Sarin incident in the area of Dortmund Germany. The exercise is planned by the Fire Department Dortmund, the THW and the BBK.

Topics: CBRNE, long term exercise

Date: 23.06.2016

Source: Fire Department Dortmund

Story VII

Daniel

Story VIII

-Presentation of the Demonstration Case during the Review Meeting

Use this section to explain how you think results and/or activities related to this Demonstration Case will be presented during the Review Meeting. Examples may include:

demonstrations of interactions between end-users and demonstration implementations (prototypes) during the review meeting

storytelling (documenting and narrating the key moments and evolution of a Demonstration Case through video, audio etc involving end-users

visual tools such as graphs, posters etc

booths and presentations

other?

For each activity that you envision during the Review Meeting, please also describe with as much detail as possible at this stage:

which stakeholders will be involved in the activity

the needs for interactive functions / capabilities technically implemented in demonstrators / prototypes

rooms / physical space

number (an possibily names) of SecInCoRe team members involved in the activity

needs related to documents / Knowledge Base

Current plan:

One of us will tell the story using the Poster. When Live Action is required, it should be done on a big screen/projector (probably by us, commented by some participants).

Physical equipment / hardware (e.g., laptops, whiteboards, post-its etc)

1 Table

1 Big screen

1 Flipchart/wall (Poster)

How much time you think should be devoted to the activity: 30 minutes

Introduction (Stein der Weisen) – 1 Min.

Story- Prerequisites – 2 Min.

Story I – 2 Min.

Story II – 2 Min.

Story III - 3 Min.

Story IV – 4 Min.

Story V – 2 Min.

Story VI – 2 Min. Story VII – 1Min Added value – 1 Min. Questions – 5 Min.

9.1.2 Pandemic Plan Revisions, Dortmund Pilot Case

Demonstration Case Identification

Demonstration Case ID (to be assigned by T6 ECO):		Demonstration Case Version (to be assigned by T6 ECO)	
Demonstration Case Name:	Pandemic Plan Revisions		
Person in Charge:	Katrina Petersen	Last Updated By:	Simona De Rosa, Katrina Petersen
Date Created:	1 June 2016	Date Last Updated:	15 June 2016

General Information on the Demonstration Case

Demonstration Case Name: Pandemic Plan Revision
Short description of the Demonstration Case (to be completed by T6 ECO)

Concepts/Components mobilised through the story: ELSI aware interactions Within system (e.g. privacy, security) With other stakeholders (e.g. inclusiveness and diversity) With individual document/data (e.g. access rights) Taxonomy concept support for searching in new topics/issues support for identification of knowledge gaps support for finding relevant information, quickly (e.g. provide a mechanism by which users can support for identification of potential new partners support towards configuring awareness of other perspectives (e.g. awareness of other data-gathering and risk-analysis structures) support towards overcoming language barriers Meta-data concept Expression of access rights Find contact/author Support towards overcoming language barriers support for determining relevance of information, quickly support for determining data quality in relation to one's needs Identification of access rights and necessary information to request change Ability to contact the originator of data/other stakeholders
Which members of the SecInCoRe Team contributed to the documentation of this version of the Demonstration Case?
Katrina Petersen, Monika Buscher, Paul Hirst
Please list all the stakeholders / end-users that contributed content or provided input for the Demonstration Case Template (they helped construct stories, identify aims, define use cases etc.)

Name	Position, department and organization
Katrina Petersen	Research Associate, Lancaster University
Monika Buscher	Professor, Lancaster University
Ed Saville	Lancashire Local Resilience Forum Pandemic Management Group
Collette Taylor	Lancashire Local Resilience Forum Pandemic Management Group
Mark Bartlett	Lancashire Local Resilience Forum Pandemic Management Group

Demonstration Case Scenario

The demonstration scenario is narrative describing a hypothetical but realistic situation (ideally co-designed by stakeholders and SecInCoRe team members) that provides an agreed-upon starting point for participants to (a) define the overall aims they want to achieve during the Demonstration Case; (b) identify the challenges they will have to overcome to achieve these aims. Feel free to choose the most appropriate format for the narrative, but please provide as many details as possible on the following points:

The starting situation and how it relates to stakeholders' current practices

What are stakeholders trying to achieve in this demonstration scenario

What do stakeholders need to achieve their aims

Who participated in defining the scenario, and which were the main steps in the construction of the scenario (meetings, workshops, conversations etc.)

Were the stakeholders who contributed to the definition of this scenario already familiar with the SecInCoRe concept?

Background:

The Scenario was initiated by stakeholders familiar with SecInCoRe with the Lancaster AB workshop and the issues within are derived from the ELSI guidelines, concepts as expressed in the deliverables, and the follow up notes from the workshop.

Starting Situation:

[Introductory Slide] Brief Explanation of the LRF, co-design and how the case came to be.

The Lancashire Local Resilience Forum (LRF) wants to improve their community resilience plans in the context of pandemic planning. To do so, they need to consider specific issues around cultural diversity and excess deaths

--Pandemics are a main risk hazard for most EU member states (the United Kingdom and Norway assess influenza pandemics as posing the highest overall risk of all hazards addressed) thus a very relevant issue through which to examine SecInCoRe's potential.

"Pandemics are considered one of the most severe threats with potential important human impacts on health and indirect socio-economic impacts as a consequence of the affected manpower running vital social and economic services…The overall uncertainty in measuring the level of impact and likelihood of pandemics make it a prominent hazard central to many NRAs." (p. 28)

European commission (2014). "Commission staff working document: Overview of natural and man-made disaster risks in the EU." Brussels, 8.4.2014. SWD(2014) 134 final.

Stakeholder's Current Practices:

This is based on current activities taking place within the LRF, who are revising their pandemic plans to address the challenges identified during the 2009 H1N1 Flu academic. One issue that arose in 2009 was the need to have plans that better prepare for the potential for 'excess deaths'. While in 2009 the deaths were limited and the issue did not arise, the gap for future planning became clear.

At this time, the management of mass fatalities in the context of a pandemic incident is not resolved. This is in part due to lack of central guidance at national level. It is argued that the reason for this may be based on the fact that the issue is an emotive one: difficult to address in the absence of an incident, but where solutions (e.g. mass burials) to a real problem during an incident may find public acceptance more readily when they actually exist. In the meantime, the LRF can only develop plan structures rather than detail, based on relationships with religious and community groups, relevant service industries (funeral directors, transport and refrigerated storage companies) and other public safety organisations. One way to progress the matter further might be to look for those countries or organisations who might have already solved the issue or provided information which could be used to suggest solutions to higher government levels. where fact, their methods for dealing with this are very ad hoc, often through already established connections with religious groups.

The LRF is currently working towards participation in a national pandemic influenza exercise entitled CYGNUS which is planned for October 2016. As part of this, the LRF are planning to test their revised plan and community resilience mechanism, of which this is a part.

In the demo, stakeholders are trying to achieve:

The LRF wants to revise already existing plans to address needs that were identified after the 2009 H1N1 pandemic. They want their plan to provide tools for supporting decision-making around excess death / mass fatalities during pandemics.

The LRF wants to define more clearly when they might need new partnerships to address these concerns, to identify and expand data sets and overall informational resources to support such work, and to establish in advance various scales of communication / data sharing practices so

that come the need to activate the plan, the networks are already there to support it.

The LRF wants to improve toolsets to identify potential vulnerabilities that can lead to excess deaths in order to improve their plan. This can range from new data sources, more informed questions to be asking of the data, and new partners/networks to support this.

To achieve their aims, stakeholders need:

Access to lessons learnt from others who have faced similar situations

Ways of finding relevant information, quickly (including summaries)

Tools to help identify relevant new partners based on current issues

Tools to highlight gaps in knowledge, such as search results that provide unexpected results.

Support in achieving more social tacit practices, specifically configuring awareness and articulation work. Tacit Practices are those which we do but cannot articulate or get lost when we explain things because they are so ingrained. 'Configuring awareness' and 'Articulation Work' (see D2.4 2.1.3 for more details about this) refer to the nods, contextual information, references, exchanges done do make sure everyone is on the same page, understand the variations in perspectives in a room, and understand how the work they are doing fits in with the work others are doing.

Support for ELSI sensitive engagement with information (such as access restrictions (unpublished research, lessons learnt that are not yet public), awareness of different data gathering structures.

Mechanisms by which the diverse stakeholders can become familiar or can engage with each other's different infrastructures, languages used, methods, etc., in relation to the knowledge being shared via the search results and follow-up interactions.

Mechanism for explaining motivations for data to be included (in order to be clear about the goals of the data gathering and the power play being enacted in engaging with the data).

Ability to find and contact the originator of the data.

Enable different (and modifiable, and partial) classifications of data, so that some organisations can see their own data for comparison with a wider data set but not share it with the wider collaborative community.

Mechanism to assure data quality is attended to (especially if it is a new partnership to help determine overall if a document/information is of high enough quality to use when the originator is previously unknown).

Mechanisms for ensuring privacy and security

The Story:

The LRF need to revise present pandemic plans to better prepare for the management of excess death / mass fatalities. In doing so, they know they need to develop tools to be more aware of: preventative measures; issues that can add to the death toll, beyond simply tracking the disease vector and overall number of those affected; management and disposal of bodies; public information; public perception (both negative and positive); and so on……

They realise they do not even know:

where to begin searching for cultural or local statistics in relation to the 2009 pandemic (e.g. they are unsure where to find numbers of deaths by ethnicity or class, etc.); or

how to actively track what issues might make individuals or a community at higher risk (e.g. what individual and community details should they be tracking in order to best foresee a vulnerability).

These are both beyond any internal experience they or their typical contacts have. They go looking for new resources (documents, data, people). So, they turn to SecInCoRe in order to try to find some ideas as to how to address their issues.

Their aim is not to develop a specific plan but to try to best develop a plan for data interoperability by

identifying for the issues around which they will need to respond

establishing in advance the network they need in order to get/share data on those issues

Use Case 1: Initial search to identify issues of concern

[click to slide 2]

They start their search by looking for ‘excess death’.

[click on search box]

[click search (this will switch to slide 3)]

Show: ‘Excess Death’ being typed in

The results are too large and a bit all over the place, so they go to the filters to refine their search, but are unsure of which to do.

[click on ‘data sets’ filter (this will switch to slide 4)]

[click on ‘planning information’ filter (this will switch to slide 5)]

[click on ‘lessons learned’ filter (this will switch to slide 6)]

Show: oversized results list and filter menu, changes as the filters change.

So, they switch to graph view to see how the search term appears in context to help better determine a more limited set of issues to work with.

verbally state: they realise part of the problem is that they know they have a gap but don’t know what it is to search for to help fit the gap. They hope seeing what issues are tagged and

connected in relation to their search terms might help them navigate the unknowns and start to point to areas that will help fill clarify and fill the gap.

[click on 'graphs' tab (this will switch to slide 7)]

show: screen switching to larger graph/constellation view.

[note: this is co-designed – it is built based on the pandemic specific taxonomies created during our workshop as well as the issues raised during the follow up meeting with the LRF]

They click on a few of the related nodes to get a more detailed, zoomed in, Taxonomy

[click on 'vulnerability' bubble]

[click on 'community care' bubble]

[click on 'demographics' bubble]

[click once more to finalise selection]

[once expanded click one more to get new detailed nodes (this leads to slide 8)]

show: the selected nodes enlarging

once selection is finalised, the nodes will expand on the screen with the unselected nodes fading away. New, more detailed nodes will appear.

From this they start to collect a list of issues and articulate questions about what exacerbates deaths during a pandemic that they previously could not. They are gathering confounding factors related to pandemic deaths but that are not just about the viruses themselves. They look at the Taxonomy/tags around the topic and start to see what kinds of issues have arisen elsewhere so that they can start to consider these same issues for themselves. And from there begin to make a list.

Use Case 2: Exploring potential relevancy of unexpected issue.

Look one of the unexpected nodes to continue to fill their gap in knowledge about issues that exacerbate pandemic deaths other than the virus itself/determine relevancy of data and/or documents. The Taxonomy relationships helps provide a contextual frame within which to evaluate the different issues, concerns, tags, and documents/datasets that come up. This supports a user in better understanding how otherwise unfamiliar data fits into their own practices and risk analysis procedures. It is not intended to give a definite answer, but it is intended to provide key support and make the process of engaging with new data and stakeholders more efficient and effective.

They find many expected categories (religion, cultural issues, transport infrastructure,

environmental concerns). But then also find 'isolation' is connected to these issues, a category previous not considered beyond isolating to prevent spread, not isolation in relation to excess deaths. They identify this as an additional subject for further investigation and to incorporate in their planning.

[click on 'isolation' bubble – it turns red]

[click a second time on bubble, it moves to centre while others disappear]

[click once more to get new constellation (this switches to slide 9)]

Mouse clicks: now see 'isolation' at centre with a range of shapes and colours referencing the type of supporting material within SecInCoRe.

Blue = issues/tags/topics (as had been the case in the previous constellations shown in this same presentation)

Pink = Lessons Learned

Green = Case Studies

Note: these two categories have consistently been highlighted in the co-design workshops as being of great interest, added value, and supporting needs of our users.

Orange: data sets

Blue: Documents

[note: might need a quick aside here about how these are not uploaded nor linked, but SecInCoRe will have a 'portal' to their meta data – should confirm this, though]

As an issue related to data gathering, isolation is new for both their excess death and pandemic plans and they are uncertain it relates, but since they don't know which issues to consider, they want to examine it further. They pull up the H1N1 case study to better understand how these issues might be relevant for pandemic planning.

[click on '2009 H1N1 Pandemic' trapezoid – it enlarges]

[click again to switch to detail page (this switched to slide 10)]

Show the details page for the case study. It has:

--a snapshot of the document

--meta data (which is co-designed – derived in part from what has been found in WP3 but also from what's been requested and asked of documents in the workshops)

--related documents (in a Taxonomy to see the documents with most similar tags)

--related Images (from the documents or related to it, also similarly tagged – this was also something that has come up in the co-design workshops and interviews, how images can be a quick way to understand the context and scope of information, faster than words in many cases – it does some of the articulation work)

--related stakeholders (to see which stakeholders have written documents that are closely tagged, which is a way to start seeing possible new partnerships – again, a sort of articulation work since different stakeholders automatically imply specific goals/aims for the information within)

From here they are able to start to do some quick overview research related to specific issues (isolation as a confounding factor in excess deaths during pandemics) to better understand how to being to approach building that issue into their plans.

[click 'back' button at bottom of screen (this switched to slide 11)]

The next step, now that they've identified this issue as relevant is to start to pull up the lessons learnt to see how other regions/countries have dealt with the problem.

[click on 'data gathering' pink rectangle – it enlarges]

[click again to get extracted lessons learned (this switches to slide 12)]

Show 'extracted' lessons learned for data gathering result screen. The left column is the documents. The right column is the lessons learned that have been tagged (as lessons learned and as their relevant issues) when the documents became part of SecInCoRe.

Notice that the first three all point to a data gathering gap. At three different scales of data gathering it is noted that data around migrants is missing. These are groups that are often isolated (by there status as migrants) from many of the social services and community care networks, but yet also provide a mobile vector for pandemics.

(note: these are real quotes from real documents, all except the first which is a real quote, but from a US document -- KP tweaked it to be UK)

LRF finds that consistently in the lessons learnt there may be no adequate stats collected or collated around this issue. That being so, there is the opportunity for the LRF now to identify that issue to regional and national organisations, who can then consider changing their stats processes accordingly.

[click 'back' button at bottom of screen (this switched to slide 13)]

They go back to their search, now, to start to see what else they can find in the data sets to help inform their planning.

[click on 'data Flash Euro-barometer 287: Influenza H1N1' orange rectangle – it enlarges]

[click again to get the details page (this switches to slide 14)]

They then go to another data set page to explore it, too. The LRF can do this many times as needed to get a range of data from a range of sources all pooled together here. (we are skipping going back and forth between the search results/Taxonomy and details page, just going from details page to details page now because what's important is the contextual data here).

[click again to get another data sets details page (this switches to slide 15)]

then notice is that many data sets are connected to a specific author for which they are unfamiliar. 'The European Observatory on Health Systems and Policies'.

Point to how this stays the same in the stakeholder section. I've even left it in the same position to make it stand out in the transition between these two.

Since they are not familiar with them, and they is not a typical public emergency response agency (and not a regional one at that), they would like to determine more about the data being provided. On one account, the author is a stakeholder in SecInCoRe: that gives the data one stamp of approval since users would not use it unless the contributors were legitimate. However, that does not tell the LRF if this particular group's data is relevant and appropriate for their needs. So, they go back to the meta data of these documents in order to try to suss out some more information about the data collection practices.

Point to meta data section and the categories within. (note, this is also co-designed…derived from WP2, WP3, WP6, as well as the discussion in the co-design workshops). If you could scroll down you would also see:

kind of organisation, expiry date, controller, collaborators, is it tested, access rights, gathered via what means.

Use Case 3: Encountering a Language Barrier

[stay on slide 15]

The initial results come from all over Europe, meaning many documents that are not in English

Point to how these results are in French, but the LRF does not read French. And they know: 1) plugging into google translate won't work because google translate doesn't work that well to begin with, and translation is more than simply a foreign language issue but a Taxonomy issues. Even on the most basic level, what 'first responder' means in the UK is not the same as in Germany; 2) if it is a data set, as is this case, that's not easily translated using an automated system. So, instead using the details page data it is possible to see how this document fits in with others you can contextualise and then determine if it is worth the effort to follow up on. In many cases, this simply involves contacting the author for a conversation to get the relevant material. They can contact the authors, through the SecInCoRe system (as already seen in FDDO example) to find out more about the contents of the document and that particular issue without requiring a translation or asking the author if they are willing/able to practically check a translation for accuracy.

In this case, the document has many of the same images as the previous one, and almost all the same related documents. The meta data, which is in English, also points to relevancy.

Use Case 4: Negotiating Access Rights

Going back to the general search results, the LRF continues to explore the documents within. Except that they arrive at one for which they can only see the meta-data and it's related tags.

[click to switch to slide 16]

In some cases, they can quickly rule it out as irrelevant. But here it looks potentially useful.

Show the summary details within the list clearly demarcating access rights: none. No images. No related stakholders. Only meta data.

So, they want to find out more about why the document is restricted

[click 'restricted access', it will blink]

[click again to get pop up (which will switch to slide 17)]

Click "restricted access" and get a pop up window that points to the appropriate ELSI guideline regarding the specific restrictions in this case: 'data minimisaton'. The guidelines also offer support in how best to approach requesting access. (there is a scroll bar there to show how you should be able to scroll down to see entire guidelines page)

Close that pop up.

[click the ‘x’ in the upper right corner, it will close (will switch to slide 18)]

Now that you are aware of the access rights and think it is acceptable/legal for you to gain access, you want to draft an email to the author requesting so.

[Click on the authors name to then get a new pop up to send an email through the system.]

Inside the pop up it not only anonymises the emails/contacts, but is also automatically sets up the subject line as well as offers key advice about what to include in order to have the best chances to gain access. [this last part was also co-designed – it came from the workshops where people described what they do when they ask for data or what they want to see when they are asked in order to not just pass it over with an automatic ‘no’]

The email is sent.

[Click send and the pop up will close]

the author provide the rights. Now, when you click on the details page, you will get the full picture.

[Click ‘details’ tab again to refresh again]

Show the expanded detail page, highlighting how the results changed from the previous list.

Use Case ‘Next Steps’: Explore potential for New Partnership. There will also be a poster that reinforces what can be said here..

End the demonstration discussing the more collaborative aspects that remain too conceptual to show at this point. This is mostly how this same background/contextual information that is helping the users best engage with the variety of data provided can also be used with other stakeholders within the CIS.

SecInCoRe System Components needed for the Demonstration Case

Please describe all the components of the SecInCoRe system that stakeholders will interact with during this Demonstration Case. Please include both technical implementations (prototypes - demonstrator implementations) and conceptual representations (delivered through

presentations, booths, diagrams etc). For each component, please indicate the tools that you think will have to be used during the Demonstration Case such as:

Mock-ups (pre-designed demonstrations that mimic functions or possible uses of the SecInCoRe system)

Demonstrator implementations (prototypes) for end-user interaction

Conceptual tools (e.g., booths where team members introduce specific concepts / components and discuss them with end-users)

Mock-ups:

Show: words being typed in 'management of mass fatalities' or "excess death data"

Show oversized results list and filter menu…have mouse wander over and explore a couple different options, but none are providing what they want.

show screen switching to larger graph/constellation view.

Show: the mouse selects 4 related nodes and then get the zoomed in results. The results include the remainder of the excess death column (body management, funeral practices, religious requirements, death certification, death statistics (subbed by categories – national, regional, ethnicity, class), and hospitals, regions without service, evidence, environmental health, business continuity issues, isolation.

Mouse clicks: now see 'isolation' at centre with issues in blue: living alone, single family home, no living family, neighbourhood support network, connectivity, community care. Also see in green case studies appear: European heat wave, Chicago heat wave. See in orange lessons learned from specific disasters.

Show two case studies being clicked on to be opened/viewed.

Go to details page on second case study, that shows contextual and meta data. Show triangle that makes clear that documents that are tagged with these two terms are often also tagged with XXXX and/or XXXX.

Back to isolation constellation. Click on lessons learnt – (have many be about "no data, but there is a need")

Back to search result screen. Open up the summary data show the different types of things that can appear for the meta data.

Show a few of the results with summaries showing at the same time, all with author X listed as the author or among co-authors.

Show a return to the search result screen and a close up look at the detailed meta data for the document that contains information about: Author, kind of organisation, when originally made, when last updated, expiry date, controller, collaborators, is it tested, access rights, purpose, gathered via what means.

Show results of documents with summaries in many languages. Show that the meta data is still in English

Show a graph that places the documents in their taxonomical relationship.

Show one document that is clearly overlapped in relation to some English ones but has one

other taxonomical connection that is important to the search that the English documents don't have.

Show the summary view with the specifics for that document. Click on author and open up email/communication system for directly sending request.

Show the summary details within the list clearly demarcating access rights: none.

Click "access rights: none" and get a pop up window that points to the appropriate ELSI guideline regarding the specific restrictions in this case. The guidelines also offer support in how best to approach requesting access.

Show the letter being written taken into specific account the points raised in the guideline that popped up.

Show some sort of "access granted" result.

Show the expanded list, highlighting how the results changed from the previous list.

Conceptual Displays (for review only):

ELSI Booth with 3 posters and 1 computer

Poster 1) Constructing a common information space

One major aspect of developing trust is developing a sense of "shared", "sameness", or "common" in how data is engaged with. While getting everyone involved to have the exact same understanding of a piece of data is impossible, it is possible to focus on purpose and legitimacy that encourage all to see the actors as on equal grounds.

be an expert instead of a novice in a partly-new practice (one's ability to act as an expert is based on the ability to take new knowledge/experience and frame it within a previously established frame of analysis – explain up SecInCoRe can help do this).

configuring awareness/articulation work: explain how SecInCoRe supports these actions (that typically require being in the same space) in distributed ways (at a distance).

Poster 2) ELSI registers

The 5 registers on which ELSI can be found, with example, from the ELSI white paper, to help explain how we understand ELSI a why it is important for design to think at different scales.

Poster 3) ELSI Guidelines

Explains the guidelines, their purpose, and how they are being made

Explains the live, lived, living nature of them.

Computer: With OA and the (very rough) guidelines on them.

Timeframe and roadmap for the Demonstration Case

Please explain for how long stakeholders will be involved in the Demonstration Case and provide indicative start and ending dates. If possible, please provide details on any planned activities or interactions between SecInCoRe team members and stakeholders. Please keep track of all interactions between SecInCoRe team has with the involved stakeholders and about the outcome of such interactions

Involvement started in February 2016. Several large and small meetings with LRF have taken place. Co-design workshop 3-4 May 2016. Follow up meeting with LRF 6 June 2016 to further develop case. To be continued until end of project.

Use Cases associated with the Demonstration Case

A Use Case details a sub-tasks or activity that stakeholders need or should be able to perform in order to achieve the aims or confront the challenges identified in the Demonstration Case. The activities / tasks defined in Use Cases do not necessarily need to follow a pre-determined linear progression; they may also represent potentialities that end-users may or may not decide to exploit during the Demonstration Case, or adapt to their emerging needs. For each Use Case, please indicate:

Which is the specific goal that end-users can accomplish (e.g, find relevant documents; identify the author(s) or otherwise assess the reliability of a document; securely log in etc)

A (ideally user-generated) definition of what would qualify a task as successfully accomplished

An (as detailed as possible) break-down of the intermediate steps that end-users would have to go through to complete a sub-task

A list of the prerequisites and assumptions (covering both end-users and the status of technical and conceptual SecInCoRe demonstrators) that must be fulfilled to complete each sub-task

ELSI guidelines in action

contextual embedding of guidelines

provides confidence in data privacy and security

stakeholder diversity

encourages critical/reflexive thinking about information/data sharing/access decisions.

Provides tools for data quality assessment

Negotiating Access Rights

search results that display different access rights, including documents that might be shareable but only after author contact, such as: grey papers, lessons learnt not made public; full access rights documents; documents for which they can only see meta-data. The mock up would encourage a personal author interaction that would then change access rights and then the next search would display different access rights / level of information to the results.

Encountering a Language Barrier

search results that show summaries of the ways a term appears and of the content itself if the document in a different language so they know if it is worth the trouble to follow up on. Have the taxonomical display make it clearly visible that the document in another language is relevant based on its tags and relationships to other concepts. Use this as a way to demonstrate how the Taxonomy produces relevant results/new partnership/new contacts/act as a translation mechanism.

Identify issues of concern + Exploring potential relevancy of unexpected issue

search results that rely on taxonomical use that provides unexpected results that help the users highlight gaps in their plan they had not previously identified but are not relevant because of

their search issues. Use this as a way to demonstrate how the Taxonomy highlight gaps/links between different categories/issues/topics by connecting a vast body of knowledge via relationships between terms, documents, and data.

Exploration of data quality for new stakeholder:

Find data from a new organization that doesn't clearly/cleanly fit into previous understanding of trusted agencies. SecInCoRe supports working though/finding out whether it is reliable by including meta data about authorship, different expertise categories. Also, as part of a CIS/search make visible what types of expertise could be beneficial and why.

Support for contributing documents and data/data sets:

Participants discover that they have relevant material. How do they add it in a way that it has meta-data and this is exploited, including meta data extraction or input mechanisms and follow up searches

Presentation of the Demonstration Case during the Review Meeting

Use this section to explain how you think results and/or activities related to this Demonstration Case will be presented during the Review Meeting. Examples may include:

demonstrations of interactions between end-users and demonstration implementations (prototypes) during the review meeting

storytelling (documenting and narrating the key moments and evolution of a Demonstration Case through video, audio etc involving end-users

visual tools such as graphs, posters etc

booths and presentations

other?

For each activity that you envision during the Review Meeting, please also describe with as much detail as possible at this stage:

which stakeholders will be involved in the activity

how much time you think should be devoted to the activity

the needs for interactive functions / capabilities technically implemented in demonstrators / prototypes

physical equipment / hardware (e.g., laptops, whiteboards, post-its etc.)

rooms / physical space

number (and possibly names) of SecInCoRe team members involved in the activity

needs related to documents / Knowledge Base

What is written above in section 2 basically covers this.

25 minutes is the estimate. We will aim to solidify this by Wednesday.

Right now, no outside stakeholder involvement is planned. It is primarily Paul storytelling

Equipment needed:

Screen, Keyboard, Mouse. We do not want a laptop, but a keyboard that is hooked up to the big screen/projection so eyes are looking their and not all trying to look over someone's shoulders. (Paul) Booth/Tables for conceptual components, 3 posters printed, 1 or 2 laptops with internet access (Katrina)

9.1.3 Search Function for plans revision, Second Lancaster Workshop

Demonstration Case Name: LRF Workshop
Short description of the Demonstration Case (to be completed by T6 ECO)
To test/challenge/validate our assumptions of practice and added value that are built into the system and concept at present. The workshop has been structured around two main points relative to the overall SecInCoRe concept: 1) Test the ability to demonstrate in interactive form the semantic framework and Knowledge Based concepts, building on the mock up demonstration from the second year review. 2) Explore one major theme of the ELSI guidelines: transparency. This case is set up to use it as a tool to explore both our Ontology in practice with domain experts as well as a way to probe potential approaches to ELSI guidelines. Concepts/Components mobilised through the story: ELSI aware interactions Within system (specifically a focus on transparency) Taxonomy concept support for searching in new topics/issues

support for identification of knowledge gaps

support for finding relevant information, quickly

support towards configuring awareness of other perspectives (e.g. awareness of other data-gathering and risk-analysis structures)

Meta-data concept

support towards overcoming language barriers

support for determining relevance of information, quickly, including useful and accurate keywords and tags

support for determining data quality in relation to one's needs

Which members of the SecInCoRe Team contributed to the documentation of this version of the Demonstration Case?

T6

ULANC

Please list all the stakeholders / end-users that contributed content or provided input for the Demonstration Case Template (they helped construct stories, identify aims, define use cases etc)

Name	Position, department and organization
Ed Saville	Lancashire Local Resilience Forum Pandemic Management Group
Mark Bartlett	Lancashire Local Resilience Forum Pandemic Management Group
Simona De Rosa	T6 Ecosystems
Katrina Petersen	Research Associate, Lancaster University
Ivan Cucco	T6 Ecosystems
Sarah Becklake	Research Associate, Lancaster University

Demonstration Case Scenario

The demonstration scenario is narrative describing a hypothetical but realistic situation (ideally co-designed by stakeholders and SecInCoRe team members) that provides an agreed-upon starting point for participants to (a) define the overall aims they want to achieve during the Demonstration Case; (b) identify the challenges they will have to overcome to achieve these aims. Feel free to choose the most appropriate format for the narrative, but please provide as many details as possible on the following points:

The starting situation and how it relates to stakeholders' current practices

What are stakeholders trying to achieve in this demonstration scenario

What do stakeholders need to achieve their aims

Who participated in defining the scenario, and which were the main steps in the construction of the scenario (meetings, workshops, conversations etc)

Were the stakeholders who contributed to the definition of this scenario already familiar with the SecInCoRe concept?

Starting Situation and Stakeholder Current Practices:

The Scenario is a follow up on the demo-case initiated by stakeholders on pandemic planning that lead to the search mock up used in the second year review. Some of the ideas that this mock up helped develop have since become part of the Reference Implementation for the semantic framework and Knowledge Base. This workshop is intended to be a similar follow up for the stakeholders practices in relation to the design decisions in order to develop the overall concepts to greater precision.

As a whole, this demonstration series is based on the need for the Lancashire Local Resilience Forum (LRF) to improve their community resilience plans in the context of pandemic planning. To do so, they need to consider specific issues around cultural diversity and excess deaths. Moreover, many of the critiques from previous plans are vague and do not offer clear paths forward for revisions, and thus they would appreciate a system that supports their research practices in ways that helps them both identify what the gaps are "what they don't' know that they know they don't know" and help them fill them using other agencies' previous experiences.

The LRF is currently working towards participation in a national pandemic influenza exercise entitled CYGNUS which is planned for October 2016. As part of this, the LRF are planning to test their revised plan and community resilience mechanism, of which this is a part.

Note: Pandemics are a main risk hazard for most EU member states (the

United Kingdom and Norway assess influenza pandemics as posing the highest overall risk of all hazards addressed) thus a very relevant issue through which to examine SecInCoRe's potential.

In the demo, stakeholders are trying to achieve:

The LRF wants to revise already existing plans to address needs that were identified after the 2009 H1N1 pandemic. They want their plan to provide tools for supporting decision-making around excess death / mass fatalities during pandemics.

The LRF wants to define more clearly when they might need new partnerships to address these concerns, to identify and expand data sets and overall informational resources to support such work, and to establish in advance various scales of communication / data sharing practices so that come the need to activate the plan, the networks are already there to support it.

The LRF wants to improve toolsets to identify potential vulnerabilities that can lead to excess deaths in order to improve their plan. This can range from new data sources, more informed questions to be asking of the data, and new partners/networks to support this.

To achieve their aims, stakeholders need:

Access to lessons learnt from others who have faced similar situations

Ways of finding relevant information, quickly (including summaries)

Tools to help identify relevant new partners based on current issues

Tools to highlight gaps in knowledge, such as search results that provide unexpected insights/topics/themes.

Support in achieving more collaborative practices, specifically configuring awareness and articulation work done do make sure everyone is on the same page, understand the variations in perspectives in a room, and understand how the work they are doing fits in with the work others are doing.

Support for ELSI reflexive engagement with information.

Mechanisms by which the diverse stakeholders can become familiar or can engage with each other's different infrastructures, languages used, methods, etc., in relation to search results and follow-up interactions.

Mechanism for explaining motivations for data to be included (in order to be clear about the goals of the data gathering and the power play being enacted in engaging with the data).

Ability to find and contact the originator of the data.

Enable different (and modifiable, and partial) classifications of data, so that some organisations can see their own data for comparison with a wider data set but not share it with the wider collaborative community.

Mechanism to assure data quality is attended to (especially if it is a new partnership to help determine overall if a document/information is of high enough quality to use when the originator is previously unknown).

Mechanisms for ensuring privacy and security.

Who participated in defining the scenario and which were the main steps?

This particular scenario was constructed primarily through telco meetings between ULANC and UPB.

Were the stakeholders who contributed to the definition of this scenario already familiar with the SecInCoRe concept?

Yes.

The Case for the workshop:

This case is not a narrative, per se, but an experiment in Reference Implementation engagement in order to better develop and articular the concepts behind them.

Introduction to the system and what's behind-the-scenes

Aim: to give a big picture about what our system does and how it does it. This does not mean show the code or engineering, but does mean offering some insight into the backstage intermediary steps that make the tagging and mapping onto the Ontology possible. This will provide us:

the opportunity to explore, along side users, how our system's derivation of tags and positioning in the Ontology (the context of risk analysis) matches our users expectations.

The opportunity to do an ELSI assessment to see where transparency (in the social and legal sense) might be beneficial within the system's classification (see D2.2 for why).

some answers the question: How to make our system that is understandable to the general users? How do we make it so that they can interact with it in a strategic way? What kind of knowledge of the inner-workings do they need? Do they want?

Big Picture Concept in very plain speak

Provide a reminder of rationale and aim and a quick bite about what all the different parts of project are in very brief terms and a few sentences about how they fit together to reach that aim. No more detail than that.

Background for this: when we last met with the LRF we did not go over the "tool kit" idea or that this will be open source, etc. We really just focused on the mock up I made that drew on the workshop in the spring and discussed how the mock up and our previous discussions ended right before we would really explore or show how our concept would help support new partnerships or collaborative practices. So, revisiting the big picture would be good background context for them.

Demonstrate the system at present – what it does

Background: ULANC hasn't presented anything new, beyond mock ups, to the LRF since the spring meeting. It would be good to quickly walk them through the changes in the demonstrator since then. It would also be good to link in the updates to the RescueRoam and OA platforms to the Search Functions here, even if just verbally/visually for the rescueroam. This would be:

1) good practice for us for November to make a coherent;

2) give them what they need to be able to think about the search demonstrator in the larger context of the project concept. Whatever we do, we cannot repeat what we've done, though. This should instead be us explaining the links between parts (which we didn't do for them before) and new developments since spring.

Semantic and Contextual Search, how it works behind-the-scenes

The goal here is to go back over the search demonstrator (that they will be exploring hands on in the following activity and needing a good knowledge of for the last activity), but in a way that then shows them the middle steps that the system is doing for them between uploading a document to how it is placed with the Ontology. This involves, ideally (working with UPB to see what's possible):

providing the extracted data for two sample documents

explaining how this is different form the keyword generator that makes the keywords, etc, on the details page.

explaining/showing how it is 'translated' to the topics/relationships in the Ontology (since, for instance, not all topics are necessarily words that appear in the documents, so some interpretation work is going on).

The goal is not about teaching them engineering or the logic, but about making visible the meta-data/tagging production in order to best discuss the ELSI related to it, set up the potential for understanding how the graph view provides context, and to test our own assumptions about the categories/Taxonomy.

Activity 2: Explore Graph View

Aim: To explore whether the Ontology is coherent with domain knowledge, and how it fulfills the goal of contextual reasoning/analysis. The activity aims to do this on three levels of the Ontology, basic facts, meanings, and rules.

Explore document facts

Have the users upload documents they are familiar with and see how the details and positioning with Ontology works for them. Try this with a few different documents.

Do the keywords make sense?

Are any not representative of the document?

Are any difficult to interpret (e.g. don't know what it would mean because too broad)? If so, what could be done to help?

Explore meaning

Once the document is situated in the Ontology, explore how it is situated in the larger connections.

Would you make different connections to the document? Why?

Explore Rules

Does the logic make sense as moving around Ontology?

What does this suggest about how the relationships our Ontology describes?

What kinds of new and unexpected questions are you able to derive from this view?

What surprises might you find? Are there good surprises?

Discussion about the possibility of doing meta-data instead of a document

Based on what's been seen this morning, what is the minimum level of detail necessary in order for this to happen?

Could we actually make this work, balancing human vs computer generated tags??

Governance Discussion

How are the standards for these keywords governed? Is that being done by the APIs? Our Ontology? Users? If so, what should be set in place to make this acceptable and proper for our users?

Activity 3: Issues around Catalog vs Library

Based on what has been seen, a quick debate about issues raised regarding library vs. catalogue, liability issues in regards to duplicate documents, concerns about data-mining, and the like. ULANC could take notes about the various issues raised on both sides of the coin during discussion which would help us in our ELSI guideline writing.

Aim: Collect the range of issues that arise in relation to these various ways of managing documents and meta-data to determine what the best way to produce meta data in relation to the goals and needs above, now that we have some concrete examples/instantiations to work with rather than just abstract conversations.

Activity 4: ELSI Guideline: Transparency

Aim: Take a very early version of the background supporting material that would accompany a guideline on transparency and work through the issues, in consideration of the day's discussion and experimentation with RIs in order to better determine how to write a guidelines and towards what audience they would be most productively focused.

Read and discuss one-pager on transparency

The one-pager explains why it is valuable, what it does, why not always a cultural good.

Presentation on transparency and classification systems

Talk about ideal often letting trends and connections to be seen but lets a facial structure = criminal. Otherwise have particular so lots of nuanced detail, but then can't make connections between, which is the present problem we are having. It's not about seeing that a system is "designed right" but about figuring out how much you need to know to have the ability to ask questions to support the goals and aims of implementing the system.

Discussion activity

Split into two groups: users and designers.

How much transparency of the Ontology do you need to be able to know when a change is necessary to meet your cultural understanding or expand your

cultural awareness to better support collaborations? What kind of transparency (if any) would be useful for a user? How can designers consider transparency in order to better support the use of the system?

SecInCoRe System Components needed for the Demonstration Case

Please describe all the components of the SecInCoRe system that stakeholders will interact with during this Demonstration Case. Please include both technical implementations (prototypes - demonstrator implementations) and conceptual representations (delivered through presentations, booths, diagrams etc). For each component, please indicate the tools that you think will have to be used during the Demonstration Case such as:

Mock-ups (pre-designed demonstrations that mimic functions or possible uses of the SecInCoRe system)

Demonstrator implementations (prototypes) for end-user interaction

Conceptual tools (e.g., booths where team members introduce specific concepts / components and discuss them with end-users)

Reference Implementation:

Detailed Search Results with keywords and tags for each entry

Graphic Search that connects to Knowledge Base and Ontology

Interactive Ontology

Mock up:

Background activity that supports the search including process for derivation of keywords and tags

One-page background material on the ELSI: transparency

Timeframe and roadmap for the Demonstration Case

Please explain for how long stakeholders will be involved in the Demonstration Case and provide indicative start and ending dates. If possible, please provide details on any planned activities or interactions between SecInCoRe team members and stakeholders. Please keep track of all interactions between SecInCore team has with the involved stakeholders and about the outcome of such interactions

This is to be conducted at a one-day workshop on 11 October 2016.

The planning started in September 2016 and was ongoing until the week prior to the 11th because of the need for the functioning Reference

Implementations. There were many meetings between ULANC and UPB to discuss priorities in the Reference Implementation to support this demo-case as well as to explain the design decisions being made within the RI to make it ready in time.

Use Cases associated with the Demonstration Case

A Use Case details a sub-tasks or activity that stakeholders need or should be able to perform in order to achieve the aims or confront the challenges identified in the Demonstration Case. The activities / tasks defined in Use Cases do not necessarily need to follow a pre-determined linear progression; they may also represent potentialities that end-users may or may not decide to exploit during the Demonstration Case, or adapt to their emerging needs. For each Use Case, please indicate:

Which is the specific goal that end-users can accomplish (e.g, find relevant documents; identify the author(s) or otherwise assess the reliability of a document; securely log in etc)

A (ideally user-generated) definition of what would qualify a task as successfully accomplished

An (as detailed as possible) break-down of the intermediate steps that end-users would have to go through to complete a sub-task

A list of the prerequisites and assumptions (covering both end-users and the status of technical and conceptual SecInCoRe demonstrators) that must be fulfilled to complete each sub-task

Specific goals that end-users can accomplish:

Find potentially relevant documents.

Assess if document is of value to questions being asked based on:

the keywords in the details page

the tags within the Ontology/graphic search

the abstract provided

the English language metadata for non-English documents

Find useful other material by navigating the Ontology as presented in the graphic search. This means the tags also have to be of substantially significant meaning for the user and their search, not just, for example, general categories that would be relevant to most emergency documents.

Upload a document they are familiar with and have it appear in the search as expected (with user-deemed appropriate keywords, tags, and abstract).
Intermediate steps that end-users would have to go through to complete a sub-task
enter search term
get results that can be searched via text filtes
see details about a given document that includes an English language abstract/summary, relevant keywords, author, date last revised, source
see the same document as situated in the graph view Ontology
click on the document in the Ontology to get more details about how it is connected to second-degree tags, not just first degree tags.
navigate around the Ontology to see other potentially relevant issues because of their relation to this document
requested (but was not done in time): be able to see what other document are connected to the same tags by clicking on a tag.
Prerequisites and assumptions (covering both end-users and the status of technical and conceptual SecInCoRe demonstrators) that must be fulfilled to complete each sub-task
The Ontology is of detailed enough nature to provide tags that are not relevant all the time for the domain.
Abstract derivation that is accurate
Production of keywords that is relevant
Production of domain relevant tags that are relevant
A clear understanding/explanation of how the keywords and tags are derived and related to each other in order to best offer feedback.
Presentation of the Demonstration Case during the Review Meeting
Use this section to explain how you think results and/or activities related to this Demonstration Case will be presented during the Review Meeting. Examples may include:
demonstrations of interactions between end-users and demonstration implementations (prototypes) during the review meeting
storytelling (documenting and narrating the key moments and evolution of a Demonstration Case through video, audio etc involving end-users

visual tools such as graphs, posters etc
booths and presentations
other?
For each activity that you envision during the Review Meeting, please also describe with as much detail as possible at this stage:
which stakeholders will be involved in the activity
how much time you think should be devoted to the activity
the needs for interactive functions / capabilities technically implemented in demonstrators / prototypes
physical equipment / hardware (e.g., laptops, whiteboards, post-its etc)
rooms / physical space
number (an possibily names) of SecInCoRe team members involved in the activity
needs related to documents / Knowledge Base

9.1.4 Paderborn Demonstration Case

Demonstration Case Name:
Short description of the Demonstration Case (*to be completed by T6 ECO)*
Please leave empty at this stage. A brief summary of the demonstration will be prepared by T6 ECO according to a common format and will be validated by partners in charge of the Demonstration Case
Which members of the SecInCoRe Team contributed to the documentation of this version of the Demonstration Case?
UPB
Please list all the stakeholders / end-users that contributed content or provided input for the Demonstration Case Template (they helped construct stories, identify aims, define use cases etc)

Name	Position, department and organization
Detlev Harries	Fire department Dortmund
Grzegorz Wenarski	CNBOP
Marco Sickmann	Fire Department Paderborn

1. Demonstration Case Scenario

A preparation of a training exercise requires several steps. An organization team needs to build up and decide about participants in the training exercise. Aims of the training exercise have to become evident. One important point is the evaluation of a training scenario. Here SecInCoRe comes in and support the inspection of past events and therefore the decision about a dedicated scenario.

Important is to include relevant past disasters in the Knowledge Base based on a first indication of a required scenario.

First needs of this Demonstration Case based on discussions with Detlev Harries in November 2015. Further work before the review meeting especially with the ATF strengthen the need for such a case.

The case itself was based on this scenario:

CIS' are created by your governments, which are connected within a CIS, created by the FEU (Collection of national CIS's), all EU- Fire Brigades and related institutions are in and have inserted their data.

Now BASF is building a new chemical plant in your region.

Most dangerous substances that are known are:

- Ammonium Nitrat
- Vinylchlorid

Based on previous risk analysis, a dedicated training exercise taken the explosion of a chemical plant into account should take place. You are responsible to organise such a

training exercise, to be prepared for possible related incidents. As one reference scenario the incident of Toulouse was mentioned for the Training exercise.

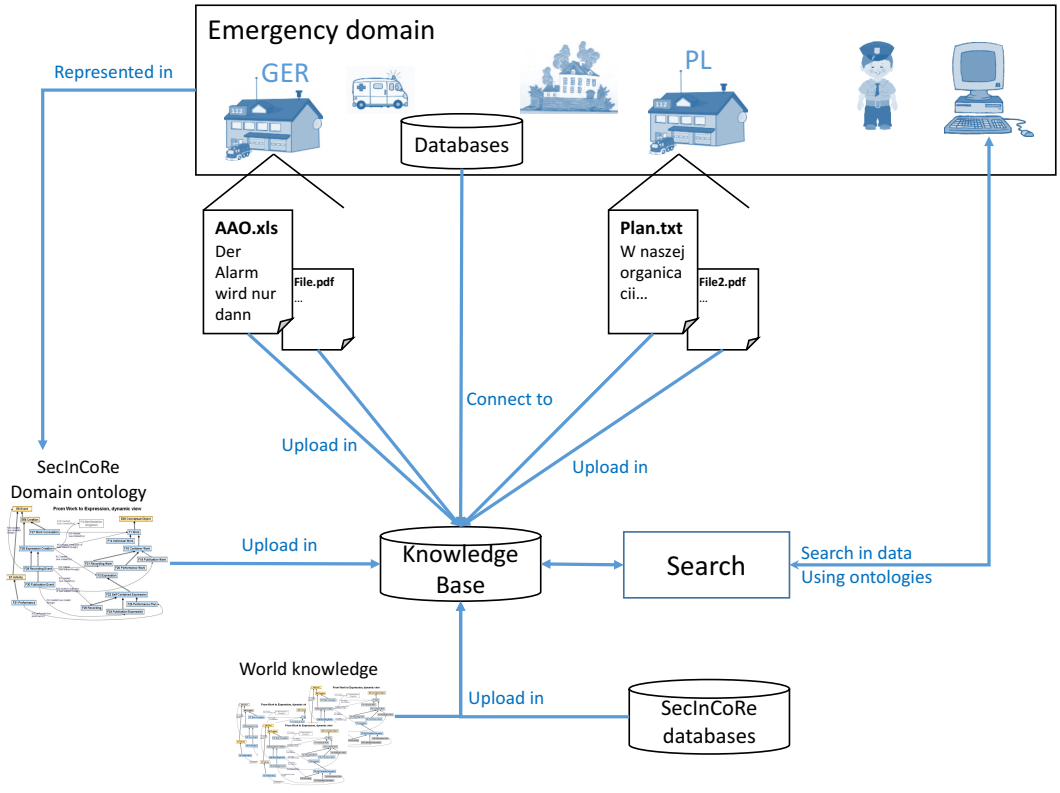
Based on that scenario, several steps has to be performed by the participants (see use case section)

2. SecInCoRe System Components needed for the Demonstration Case

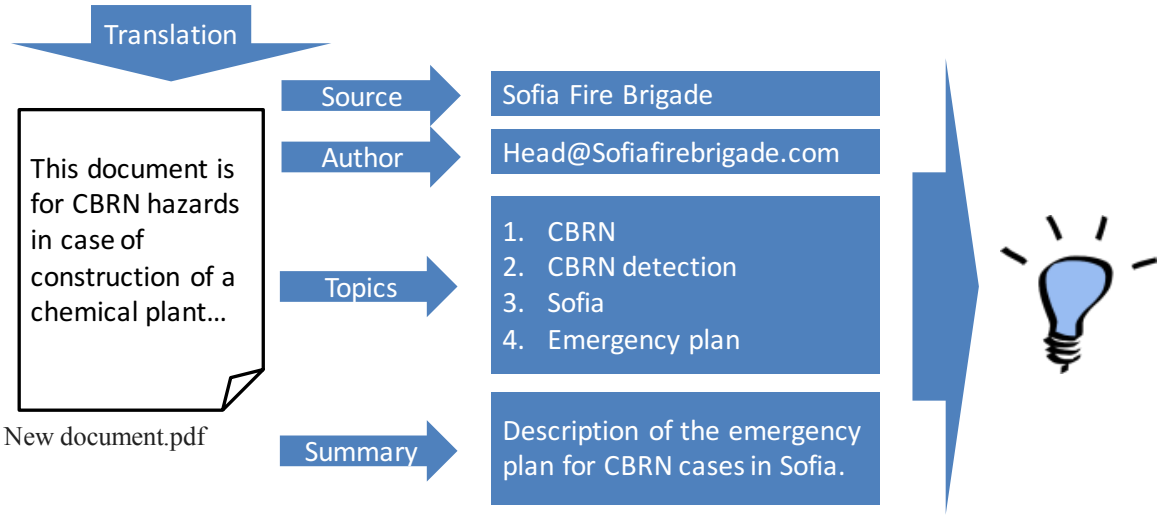
The Reference Implementation of the SecInCoRe Semantic Search was used in this Demonstration Case, including the functionality of Topic and Abstract extraction and Translation. Changes with regard to the demonstrator implementation of the Semantic Search was made by providing more / specific content in relation to CBRN scenarios.

To embed the demonstrator in the proper conceptual framework, the following slides are used:

Search concept overview:



How to care with unstructured/ multi-lingual data:

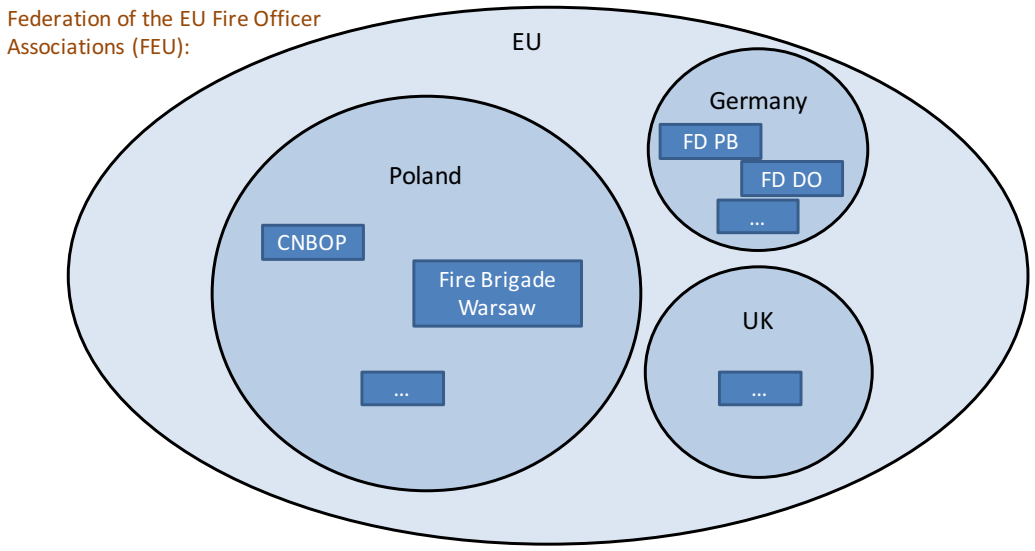


Hosting the CIS I:

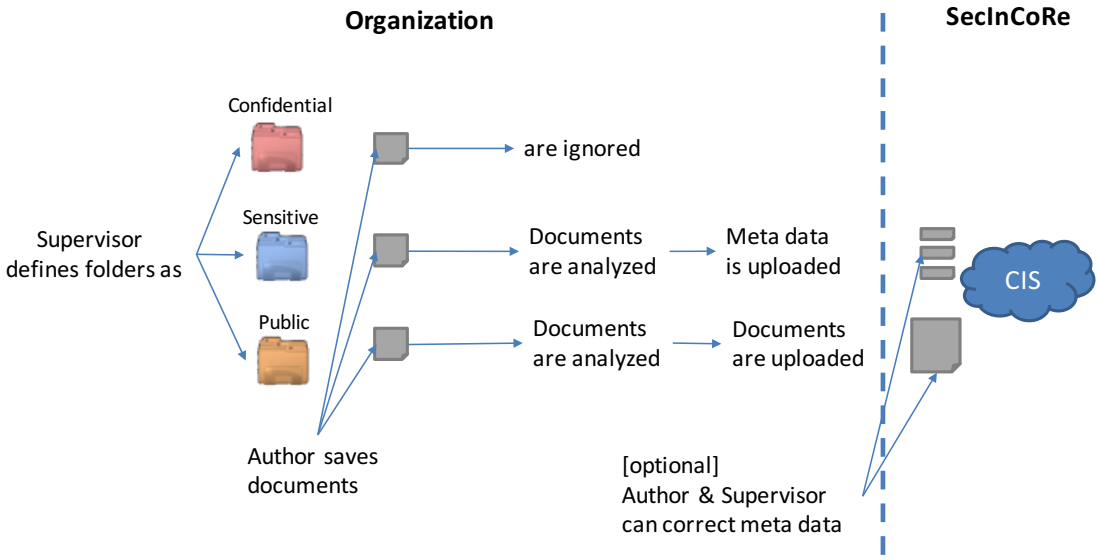
- Who should host the system, who will be the managing authority?

- The managing authority has to be
  - on a national level or lower
  - governmental institution
- National systems could be connected

Hosting the CIS II:



Crawling of data:



3. Timeframe and roadmap for the Demonstration Case

The Activity runs on the 25th of October, full day.

Agenda:

9.00 – 9.15	*Welcome Coffee*
9.15 – 9.30	Welcome
9.30 – 10.00	Introduction to SecInCoRe
10.00 – 10.45	*Concept of Semantic Search*
10.45 – 11.00	*Coffee Break*
11:00– 12:00	*Guest Session*
12:00-13:00	*Lunch*
13:00-13:15	*Case introduction*
13:15-14:45	*Experience SecInCoRe*
14:45-15:15	*Coffee Break*
15.15 – 16.15	*Validation activity*
16:15 - 16:30	*Open discussion*

4. Use Cases associated with the Demonstration Case

Concept presentation	
General questions? Would your organisation participate? What changes would be needed to do so? Tagging: automatic vs. single doc. Manual? Catalogue vs. library?	Aim: Direct feedback to the concepts, not directly shown in the demonstrator.
Play Guest Session	
Discussion?	
Case description CIS' are created by your governments, which are connected within a CIS, created by the FEU (Collection of national CIS's), all EU- Fire Brigades and related institutions are in and have inserted their data. Now BASF is building a new chemical plant in your region. Most dangerous substances that are known are: • Ammonium Nitrat • Vinylchlorid Based on previous risk analysis, a dedicated training exercise taken the explosion of a chemical plant into account should take place. You are responsible to organise such a training exercise, to be prepared for possible related incidents. As one reference scenario the incident of Toulouse was mentioned for the Training exercise.	
Managing authority ok? Scenario realistic?	Aim: Get feedback about the constellation of the described case
Experience Demonstrator	

- Short introduction of the demonstrator

KB – Past disasters, Lessons Learned

- Search for a similar CBRN incident in Europe
- They find the Toulouse incident from the KB
- Look at lessons learnt
- Are they helpful? Other display needed?
- If addition: add

Backup: We give them a "lessons learnt", they add them.

Useful? Changes necessary? Would you add past disasters? Would you add Lessons Learned?	Aim: Get feedback about the use and scope of the past disaster database and related information.

Semantic analysis – topic, abstract, translation

- Search for similar incidents.
- Find German document of a CBRN plant accident e.g. "Bitterfeld"
- Possible Backup: Recycling farm in Bochum, incident Dormagen Bayer
- Look at translation/topics/abstract
- What document do you find interesting?
- They contact the author via mail and plan a call to get more information?

Useful? Do you get a clue of the document? Would you contact authors with the information you get?	Aim: Discuss validity of topics and abstracts of search results

Semantic analysis – Ontology, filters, graph view

- You want to get more information about related topics/ documents
- They search/ filter and find related interesting documents
- They open a document in the graph view
- Get an overview of the thematic categorization
- They take a look at the whole Ontology

Categorization useful? What has to be different? Detail level ok? Graph view is for "research resaons". Would you need/ appreciate it, as a standard user?	Aim: Discuss usefulness of other representations of search results
ELSI – restricted document • Search for Ludwigshafen emergency plan • Find restricted document of the Fire Brigade Ludwigshafen(faked) • Look at topics/topic ranking/abstract • You find this interesting! • They don't get access • They contact the author via E-Mail • They get the document back (from other participant/SecInCoRe Team) (faked)	
Would you contact the author? Would you send information to another author, if he requests the document?	Aim: Insights about possibilities to make new partnerships based on the existing version of the Semantic Search
KB-IS • Finding IT support to evolving CBRN scenarios • Search for information system, to support evolving CBRN scenario used to integrate in training purposes • Find the Argos System • => Story what they would do with that	
Is it useful to not only get information about possible related information, but also relevant products?	

5. Presentation *of the Demonstration Case during the Review Meeting*

6. Any other comments related to the Demonstration Case?

*9.2 **Questionnaires used for data collection***

Secure Dynamic Cloud for
Information, Communication and Resource Interoperability
based on Pan-European Disaster Inventory

Validation Activity

Ivan Cucco, Simona De Rosa
T6 Ecosystems

October 25th, 2016

Work Package 5

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

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

Authors

T6 Ecosystems

Ivan Cucco

Email: i.cucco@t-6.it

Simona De Rosa
Email: s.derosa@t-6.it

Introduction to the survey

As part of SecInCoRe, T6 Ecosystems is conducting a survey addressed to the SecInCoRe's stakeholders in order to validate projects' concepts and outputs shown during the activity organised in Paderborn .

We estimate that the survey will take about 15 minutes to be completed.

Please answer all questions from your viewpoint, ticking the appropriate answer(s) or providing your answer in the designated space.

In case some questions are not clear, or show aspects you think are not relevant, please list us your suggestions/opinions to help us improving the questionnaire. Feel free to add comments after the text of the question where you think they need to be improved.

Thank you for the time you dedicate to this survey!

In case you need any support or clarification please ask to Ivan Cucco and Simona De Rosa during the interview that will follow shortly.

Workshop Participant Background Information

Please fill out the questions below to help us gather some information about you, your experience, and background knowledge, both in your expertise and about collaborative design. Such information helps us better evaluate the results of the workshop.

Name and Surname_____

Institution/Organisation_____

Position_____

1. What is your previous experience in disaster management (e.g. in mitigation, preparedness, response, recovery, and/or business continuity)? Is risk management a core duty for your current position?

2. Do you have any previous experience in the use of technologies for information exchange and multi-agency collaboration? If so, please describe:

- what collaborative IT systems you have previously used;
- for what purposes you have used them (e.g., to find/share documents; to communicate with other agencies / colleagues / experts; to identify good practices …);
- how frequently you use them (e.g., they are part of your regular work routine; they are used only in special occasions…)?

3. What kind of experience do you have in cross borders operations, planning and training activities? Could you please list the countries with which you have previously collaborated?

4. What kind of previous experience do you have in operation with multi-agency collaboration?

For each of the questions below, please tick the box that best characterizes how you feel about the statement:

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree	Do not know
A CIS built according to SecInCoRe concepts and specification would improve my working routines compared to other systems that you are currently using or you have used in the past	□	□	□	□	□	□
A CIS built according to SecInCoRe concepts and specification would help you increase your collaborations and establish new partnerships	□	□	□	□	□	□
A CIS built according to SecInCoRe concepts and specification would make your work more time-efficient by helping you find relevant information more quickly	□	□	□	□	□	□

Taxonomy and Ontology

Please think about the different types of search you used during the day (search based on keywords; filters based on categories; graph-based search), and consider how useful they would be in your standard work practice. The rank them in order of usefulness from 1 to 3, where 1 is the most useful to you and 3 is the least useful to you.

	Rank
Keywords-based search	___

Filtering based on categories	___
Graph-based view	___

Now please rank the different types of search according to how useful they would be to you when you are exploring a topic with which you are not familiar. Rank them in order of usefulness from 1 to 3, where 1 is the most useful to you and 3 is the least useful.

	Rank
Keywords-based search	___
Filtering based on categories	___
Graph-based view	___

Observation, focus groups and interview scripts

Interview script

Paderborn, 25 October 2016

INTRODUCTION

This is the last activity for the day. We are interested in hearing your opinion on a number of elements of SecInCoRe that you have experienced today. Please feel free to stop the interview at any time; we hope you do not mind if the interview is recorded.

PART I – RECALL POSITIVE / NEGATIVE MOMENTS FROM THE WORKSHOP

We would like to start by asking you to tell us about the moment during the workshop that you found interesting. It may be for positive or negative reasons: maybe something unexpected happened, or something particularly relevant to your work; or it was irritating or you thought that it was not particularly relevant or usefu to your work. Please tell us what happened and why you think that moment was particularly important.

Possible probes:

How does this XXX relate to your practice?

Why is this new / unfamiliar?

Can you imagine a situation at work in which you would apply this [technique / tool / strategy / type of collaboration]? Please describe it.

PART II – DISCUSS A KEY EVENT IDENTIFIED BY THE INTERVIEWER

Note: the event must be the same for both interviewers; we will decide on it during the lunch break. Ideally, it would focus on an ELSI-related aspect (one of the events that we have identified as an example of increased understanding facilitated by the system design (e.g., the

graph view or the emergence of categories from the Taxonomy). Or conversely, a case in which it was clear that different perspectives were not meeting.

What I found particularly interesting during the workshop, was to notice how [brief description of the event]. In that case I had the impression that the [graph view, the use of categories...] helped overcome some differences between the participants. Did you notice the same, and would you agree with my reconstruction of that specific event?

Possible probes:

Favouring mutual understanding is actually one of the key objectives of the SecInCoRe concept. Do you think the system as it is does a good job in this direction, and how could this be improved?

Does something similar [misunderstanding, or the need to bridge different ways of working or categorizing] happen often during your work? Can you tell me about a case in which this has happened recently? How did you solve the problem, and do you think a system like SecInCoRe would have helped?

PART III – FOCAL TOPICS

Taxonomy / Ontology

Considering the presentations and the experiences you have had with the demonstrator, do you think the Taxonomy-based categories, filters and keywords could be useful for performing a search of cases in your daily practice? What are their main advantages and disadvantages compared to your current practice?

Tell the user that you want to perform a search with them on either [to be decided beforehand]:

A topic of their interest

A topic that has already emerged during the workshop [the same for both interviewers]

Look at the results together, and invite the user to:

look at the categories listed in the filter view

open a document, and look at the categories to which it has been assigned

open the graph view and explore the surrounding Taxonomy categories

Are you familiar with most of the terms listed in the categories, filters or graph view? Do you feel you know what types of documents you would find filed under each of them?

Ask the user to identify in the filter view a term with which they are familiar, and a term with which they are NOT familiar. Write the terms.

Did you find any surprising or unexpected connections between document or between categories during your interaction with the Search Function? Could you please describe a case in which it happened and why you found it surprising?

Possible probes:

Did you at any time follow an unexpected path (based on the categories or graph view, and did it lead you to new information?

Please give the details.

Knowledge Base / Inventory

Ask the participant to open the KB page in the demonstrator, and allow them a couple of minutes to skim through the content (ask them to choose the category they are most interested in).

Are you familiar with most of the sources, or do you find listed many new sources that you were not aware of? Please give an example of each. Do you think that the collection of sources included in the KB provide an added value compared to your current access to similar collections / catalogues?

Invite the participant to navigate again the KB page to search for something using the available filters.

Do you think the navigation system for the KB is useful and effective? Is it easy to find what you are interested in?

CIS Concept

Explain that, as it has probably already emerged during the workshop, building trust and favouring collaboration is one of the key objectives of SecInCoRe. Highlight how you are aware that, for sensitive work such as theirs, entirely trusting an online system is not easy. Recall any doubts or comments they made on the point of trust during the workshop.

At the end of this workshop, do you think that plans and options concerning the process for establishing and releasing credential is clear enough and could provide a sufficient level of trust?

PART IV – OTHER ISSUES

Is there any other issue that you would like to discuss and has not been discussed during the workshop?

Other tools used to collect data (e.g., system logs)

9.3 Figures from the Second Lancaster Workshop