



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

Deliverable 4.1

Requirement Report

Final Version

Maike Kuhnert¹, Jens Pottebaum², Steffen Schneider², Monika Buscher³, Katrina Petersen³,
Katja Firus⁴, Andrea Nicolai⁴, Olivier Paterour⁵, ⁶Alexander Georgiev, Ioannis Danilidis⁷

¹Technical University Dortmund/CNI, ²University of Paderborn/C.I.K., ³Lancaster University,
⁴T6 Ecosystems, ⁵Airbus Defence and Space, ⁶CloudSigma, Center for Security Studies⁷

March 2015

Work Package 4

Project Coordinator

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

7th Framework Programme

for Research and Technological Development

COOPERATION

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





Distribution level	Public
Due date	13/03/2015
Sent to coordinator	12/03/2015
No. of document	D4.1
Name	<i>Requirement Report</i>
Type	<i>Report</i>
Status & Version	<i>Final Version 1.0</i>
No. of pages	58
Work package	4
Responsible	TUDO
Further contributors	UPB ULANC T6 ECO ADS CS KEMEA
Authors	Maike Kuhnert, TUDO Jens Pottebaum, UPB Steffen Schneider, UPB Monika Buscher, ULANC Katrina Petersen, ULANC Katja Firus, T6 Andrea Nicolai, T6 Olivier Paterour, ADS Alexander Georgiev, CS Ioannis Danilidis, KEMEA
Keywords	<i>Requirement Life Cycle, Quality Requirements, Functional Requirements, Requirement Analysis</i>






History	Version	Date	Author	Comment
	V0.1	19/12/2014	TUDO, MK	Initial version
	V0.2	09/01/2015	TUDO, MK	Input UPB, Input TUDO
	V0.3		TUDO, MK	Input ADS, Input TUDO
	V0.4	22/01/2015	TUDO, MK	Peer reviewed by CS
	V0.5	27/01/2015	TUDO, MK	Include reviews from CS,ULANC, ADS and Input from TUDO
	V0.6	06/02/2015	TUDO, MK	Input ULANC, KEMEA, TUDO
	V0.7	09/02/2015	TUDO, MK	Preparation for Review
	V0.9	10/02/2015	TUDO, MK	Version for QA Review
	V0.91	18/02/2015	TUDO, MK	Version for Monitoring Review, based on Review by CS and T6 and further input from T6 and TUDO
	V0.95	09/03/2015	TUDO, MK	Input SecInCoRe stories (UPB), Input Rome Workshop
	V0.99	12/03/2015	TUDO, MK	Final Version send to coordinator
	V1.0	13/03/2015	UPB	Final Edits and submission

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





Authors

	University of Paderborn C.I.K.	Jens Pottebaum Email: pottebaum@cik.upb.de Steffen Schneider Email: st.schneider@cik.upb.de
	TU Dortmund CNI	Maike Kuhnert Email: maike.kuhnert@tu-dortmund.de
	Mobilities.Lab Centre for Mobilities Research Department of Sociology Lancaster University LA1 4YD UK	Monika Buscher Email: m.buscher@lancaster.ac.uk Katrina Petersen Email: k.petersen@lancaster.ac.uk
	T6 Ecosystems	Katja Firus Email: k.firus@t-6.it Andrea Nicolai Email: a.nicolai@t-6.it
	Airbus Defence and Space	Olivier Paterour Email: Olivier.Paterour@airbus.com
	CloudSigma	Alexander Georgiev Email: alexander.georgiev@cloudsigma.com
	Center for Security Studies (KEMEA) P.Kanellopoulou 4 1101 77 Athens Greece	Ioannis Danilidis Email: yanniz@gmail.com



Reviewers

	T6	Antonella Passani Email: a.passani@t-6.it Simona De Rosa Email: s.derosa@t-6.it
	CloudSigma	Alexander Georgiev Email: alexander.georgiev@cloudsigma.com



Executive summary

The deliverable scopes out the requirement definition of SecInCoRe. The objective of this deliverable, “the requirement report” is to first give an overview of the requirements context in the SecInCoRe project and to, secondly, derive functional and qualitative requirements that can be transferred into technical requirements in the ongoing work in WP4. The requirements are identified against the existing background and experiences in the consortium and are supplemented with first feedback from end users during the co-design workshop on 9th and 10th December 2014 in Manchester. Further, the initiative overview and the requirements are linked to T2.2, T2.3. and WP3. Besides setting up requirements, the report gives instructions how to handle requirements during the project and within validation activities. Therefore the document has a strong relationship to the validation activities defined in D5.2 [9]. In addition, the document presents a guideline for how to define technical requirements and to work in a collaborative manner on these requirements. The document ends with a first requirements analysis based on the presented early demonstrator [8].

All in all this report is divided into 9 chapters:

- Chapter **one** gives an introduction by describing purpose, validity, the relation to other SecInCoRe documents and the target audience. Furthermore, the reader can find the glossary as well as a list of figures and tables in this chapter.
- An initial SecInCoRe overview is presented in chapter **two**. This overview is indispensable for the further understanding of the document. Setting up a “Common Information Space” bundled with a pan-European disaster inventory leads to a need for a cloud based emergency information and a network enabled communication system. The cloud emergency information system consists of two parts – the inventory and a knowledge base (T4.1) that is in effect a technical implementation of the inventory. Both are running in the cloud so that access could be realized from anywhere having just a running internet connection. The network enabled communication system (T4.5) focuses on the latter part. Establishing secure local communications (see section 2.2.1) and the stable communication with the cloud based solution is the main objective in this task. Section 2.3 describes SecInCoRe’s potential users. The novel approach that SecInCoRe suggests is that not only police authorities and first responders are the intended end-users of the system. Researchers and other users are considered and therefore the possible benefit of SecInCoRe is manifold. This possible benefit is outlined in section 2.4 with a link to D5.2 [9].
- Initial use cases and requirement categories are defined in chapter **three**. Giving detailed information about initial use cases and possible accessible data sets should simplify the understanding of the following requirement definition. One main use case is the retrieval of information for individual purposes for every kind of user in mind. Besides the development of innovative solutions for emergency organizations, political awareness and the harmonisation of European disaster response present additional use cases and objectives of SecInCoRe.



- For validation activities and the follow up of the requirement definition, the SecInCoRe requirement life cycle is defined in chapter **four**. This life cycle is defined in strong interaction with the validation life cycle to guarantee consistency through the whole project.
- Chapter **five** starts with the definition of quality requirements. Quality requirements are related to user satisfaction. The terms Quality of Service (QoS) and Quality of Experience (QoE) are adapted from the field of communication network to SecInCoRe. The original meaning of QoS and QoE describes the user satisfaction in communication networks. Further, quality requirements from the system point of view are defined. This is mainly related to interfaces and data processing.
- In addition to quality requirements, chapter **six** defines functional requirements from a user and system point of view. Functional requirements are related to services that should be available. These services are manifold and are dependent on the user and the system components. Typical functional requirements are for example search capabilities with several keywords. Further, having ethical, legal and social issues (ELSI) in mind, services for requesting ELSI guidelines are important for nearly every user of SecInCoRe.
- Chapter **seven** presents a guideline for the transfer to technical requirements and gives a scheme for the uniform description of technical requirements. A consistent description is important for the consideration of these requirements in validation activities. The technical requirements have been and will be defined in the following activities in WP4, most notably T4.4, T4.5 and T4.6.
- Chapter **eight** delineates the collaborative requirement within SecInCoRe using the project management tool JIRA. This tool allows us to adapt the work flow of items and enables role management to manage the requirements. The work flow is adjusted to the requirement life cycle defined in chapter four.
- The document ends with chapter **nine**, giving a first analysis of requirements addressed within the development of the early demonstrator. This analysis shows that having requirements in mind during the development and design process of supporting technology for end users leads to efficient and process aware solutions. These solutions have to be further adapted to the individual needs, but these needs are identified in a feedback round in direct discussions with end users. This iterative process is also part of the SecInCoRe validation process.

This document composes a first bridge between SecInCoRe user requirements and technical innovative solutions that are the focus of WP4, bringing information to the user at incident scenes, commando post, universities and other places.



Table of contents

1	Introduction	7
1.1	Purpose of this document.....	7
1.2	Validity of this document.....	7
1.3	Relation to other documents.....	7
1.4	Contribution of this document.....	8
1.5	Target audience	8
1.6	Glossary	8
1.7	List of figures	10
1.8	List of tables	10
2	SecInCoRe Overview	11
2.1	Cloud Emergency Information System	12
2.1.1	<i>Pan European Inventory</i>	<i>14</i>
2.1.2	<i>Knowledge Base</i>	<i>15</i>
2.2	Network enabled communication system	15
2.2.1	<i>Secure local communications</i>	<i>17</i>
2.2.2	<i>Communication with Cloud Emergency Information System</i>	<i>19</i>
2.3	End User and Stakeholder Perspective.....	21
2.4	Possible Benefit of SecInCoRe	22
3	Requirement Categories and Initial Use Cases.....	24
3.1	Requirement Categories.....	24
3.2	Initial Use Cases of CEIS	24
3.2.1	<i>Entering of information for individual, organisation and group purposes</i>	<i>27</i>
3.2.2	<i>Retrieval of information by individual and groups.....</i>	<i>27</i>
3.2.3	<i>Search inventory content for information</i>	<i>31</i>
3.2.4	<i>Identify gaps in the provisioning of data and information systems</i>	<i>33</i>
3.2.5	<i>Harmonise European disaster response.....</i>	<i>33</i>
4	Requirement Life Cycle.....	35
5	Quality Requirements	37
5.1	Requirements derived in interaction with users	37
5.1.1	<i>Police authorities, crisis organisations and first responders.....</i>	<i>37</i>
5.1.2	<i>Politics, industry, research and volunteers.....</i>	<i>37</i>



5.2	Requirements from system point of view	38
5.2.1	<i>Communication and cooperation between organisations.....</i>	38
5.2.2	<i>Inventory base</i>	38
5.2.3	<i>Cloud Platform and Cloud Services</i>	38
5.2.4	<i>Data protection.....</i>	39
6	Functional Requirements	40
6.1	Requirements derived from interaction with users.....	40
6.1.1	<i>Police authorities, crisis organisations and first responders.....</i>	40
6.1.2	<i>Politics, industry, research and volunteers.....</i>	40
6.2	Requirements from system point of view	41
6.2.1	<i>Inventory base</i>	41
6.2.2	<i>Cloud Platform and Cloud Services</i>	41
6.2.3	<i>Communication and cooperation between organisations.....</i>	41
6.2.4	<i>Data protection.....</i>	41
7	Transfer to technical requirements.....	42
8	Collaborative Requirement Management	45
9	First Requirement Analysis	47
9.1	CIK-Framework	47
9.2	Inventory.....	47
9.3	Process-oriented network deployment	48
10	Literature index	50



1 Introduction

1.1 Purpose of this document

This document presents a first holistic SecInCoRe overview with the objective to set up requirements for the ongoing development activities in other Tasks. Considering these defined requirements will lead to impact in various fields. Therefore this document reports the qualitative and functional requirements for the proposed SecInCoRe innovation. Both kinds of requirements are needed to design and develop valid services achieving high user acceptance. The requirements are derived in interaction with T2.2, T3.3, WP3 and WP4 to derive holistic system requirements [3]. Therefore, the document contributes to all of the SecInCoRe main objectives [3, p. 9-10 Part B]. There are requirements regarding the design of the inventory (see Obj. 1), the design of the secure knowledge base and the communication system (see Obj. 2) and the integration in first responder organisations (see Obj. 3). Further requirements are elements of the evaluation and validation activities (see Obj. 4).

1.2 Validity of this document

This report describes the current collection of requirements, but due to the ongoing evolution of processes and technology, new requirements will emerge over the duration of the project. Several additional perspectives are considered related to a high number of possible users as well as various technology choices, and as a consequence, these reviews could raise new requirements for SecInCoRe. Therefore there is no claim to be comprehensive at this stage. As additional requirements emerge or existing ones turn out to be more complex or insignificant, these changes will be considered directly in the related work package (e.g., T4.5). Thus this document copes with the SecInCoRe overview and the initial set of associated requirements.

1.3 Relation to other documents

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

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

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

- [4] D2.1 Overview of disaster events
- [5] D2.2 ELSI guidelines for collaborative design and database of representative emergency and disaster events in Europe
- [6] D3.1 Inventory Framework
- [7] D3.2 First publication of inventory results
- [8] D5.1 Common information space for internal use



[9] D5.2 Early setup of evaluation model for internal use cases

The outputs described in this document build the basis for further activities in WP4 and are therefore related to the following documents directly:

[10] D4.2 System Views and Concept of Operations (CONOPS)

[11] D4.3 Network enabled communication system concept and common

[12] D4.4 Report on Interoperability Aspects

1.4 Contribution of this document

This document clearly states the requirements to the SecInCoRe ‘Common Information Space’. It gives a holistic and inventory driven overview of system requirements. Requirements are derived by interacting with end users, from a system point of view and based on existing knowledge in the project. Requirements are two-fold: functional and qualitative. Functional means required functionality for supporting existing process, while qualitative requirements are measurable, for example the scalability and availability of the system.

Further work in WP4 will be based on the requirement definition to develop on the one hand a modular system architecture for enabling the CIS and on the other hand a design of a secure network enabled communication system concept for seamless emergency communication. The transfer to technical requirements is key for efficient innovative technology enhancement for the use in emergency scenes. To guarantee a common understanding, a scheme for the description of those is presented. A first requirements analysis based on D5.1, the early demonstrator shows how requirements are considered from the beginning of the SecInCoRe project.

1.5 Target audience

This deliverable is public and therefore available to all interested parties. Therefore the document is written as generally intelligible as possible. This document forms the basis for the validation process of user needs related to SecInCoRe evolutions. According to [3] user needs are mainly derived from existing background and user from the field of first responders, police authorities, researchers in this scientific field as well as policy-makers, politicians, publics and companies involved.

1.6 Glossary

Abbreviation	Expression	Explanation
CEIS	Cloud Emergency Information Space	See section 2.1
CIS	Common Information Space	See section 2
CONOPS	Concept of Operations	
COW	Cell on the Wheel	Cell on the wheel for ad hoc deployment



Abbreviation	Expression	Explanation
		at incident scenes
CPM	The Community Mechanism for Civil Protection	Facilitates co-operation in civil protection assistance interventions in the event of major emergencies which may require urgent response actions. It is a tool that enhances community co-operation in civil protection matters and was established by the Council Decision of 23 October 2001, updated 8 November 2007. In accordance with the principle of subsidiarity, it can provide added-value to European civil protection assistance by making support available on request of the affected country.
CSCW	Computer Supported Cooperative Work	
D2D	Device to Device	LTE/3GPP
DMO	Direct Mode Operation	Related to TETRA
DOW	Description of Work	
ELSI	Ethical, legal, social issues	
KB	Knowledge Base	See section 2.1.2
LTE	Long Term Evolution	4G mobile communication standard
NEC	Network enabled Communication	See section 2.2
NOW	Network on the Wheel	Network on the wheel for ad hoc deployment at incident scenes
ProSe	Proximity Service	LTE/3GPP
QoE	Quality of Experience	



Abbreviation	Expression	Explanation
QoS	Quality of Service	
SDS	Short Data Services	
WAN	Wide Area Network	
WLAN	Wireless Local Area Network	
WMNs	Wireless Mesh Networks	

1.7 List of figures

Figure 2-1 SecInCoRe Overview	11
Figure 2-2 Cloud Emergency Information System (CEIS)	13
Figure 2-3 Network enabled communication (NEC).....	16
Figure 2-4 Communication via Mesh and 5G/4G/3G/2G or satellite from incident scenes with decision maker at a faraway location.....	17
Figure 2-5 Intelligent hose coupling for one-the-fly network set up	18
Figure 2-6 Stakeholders and users of SecInCoRe.....	21
Figure 4-1 Requirements circle and validation activities	36
Figure 8-1 Example workflow in JIRA	45
Figure 8-2 Planned and unplanned requirements in JIRA	46
Figure 9-1 Inventory content of the early demonstrator [10]	47

1.8 List of tables

Table 1: Initial use cases for first responders and police authorities	25
Table 2: Initial use cases for example other users.....	26
Table 3: Initial use case “Retrieving” for end user.....	28
Table 4: Initial use case “Retrieving” for example other users	29
Table 5: Initial use case “Searching” for end users	31
Table 6: Initial use case “Searching” for example other users	32
Table 7: Requirement scheme for technical requirement	43

2 SecInCoRe Overview

This chapter gives a short overview about the proposed SecInCoRe innovation. This includes a Common Information Space (CIS), bridging between organisations and technology. The CIS contains a pan-European Inventory, a Knowledge Base (KB) and a Cloud Emergency Information System (CEIS), which are providing information about past and current disaster.

The Network Enabled Communication System (NEC) is divided into secure local communication (e.g., to access the CEIS) and internal communication within the CIS (see chapter 2.2.1). Furthermore, this chapter describes a first end user perspective and gives a first impression of possible benefits resulting from SecInCoRe.

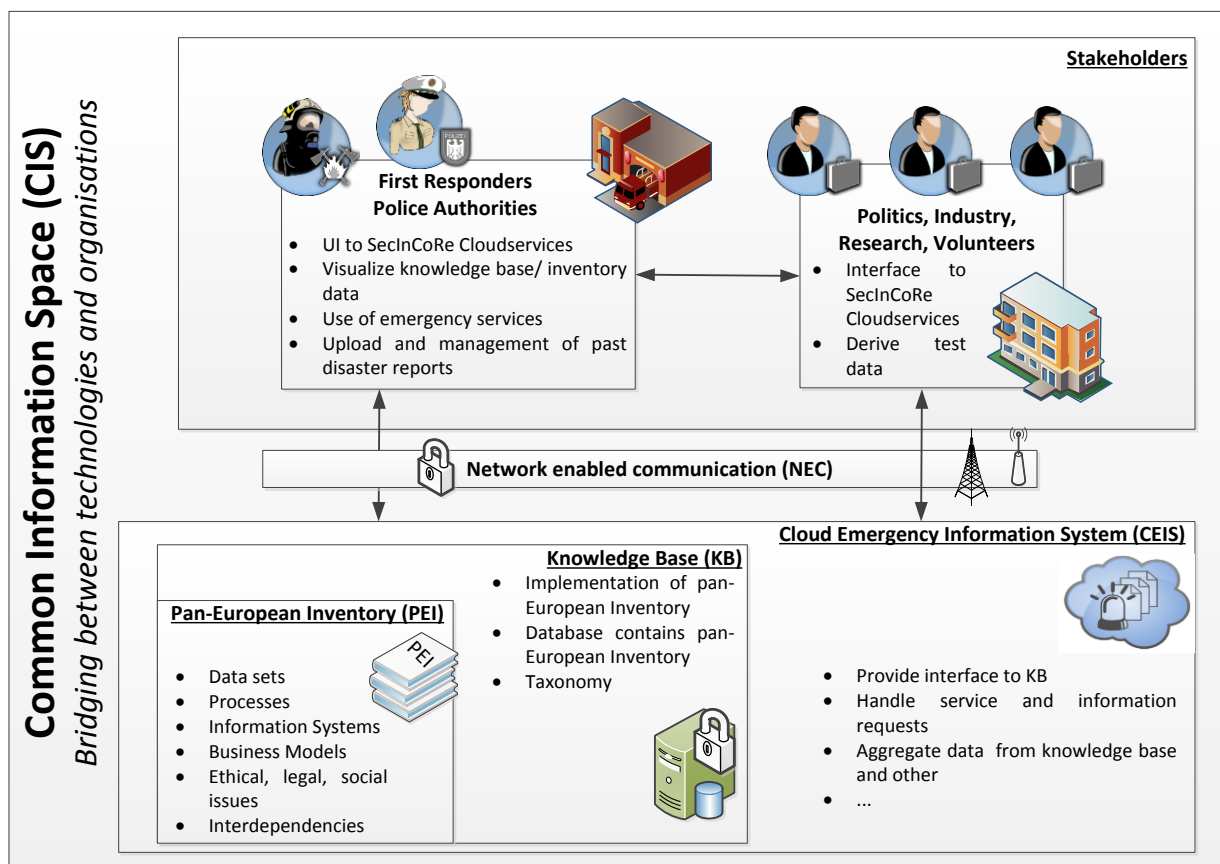


Figure 2-1 SecInCoRe Overview

Figure 2-1 highlights first the Common Information Space (CIS) that will enhance the interoperability between various rescue organizations, its used technologies, different countries and end users in the CIS. The creation of such a virtual room or space concept is one key objective of SecInCoRe. However, the term “Common Information Space” could have several meanings depending on the knowledge and the view and practices of each individual.

In the literature a definition from a “Computer Supported Cooperative Work” (CSCW) perspective is as follows: A common information space is negotiated and established by the actors involved [BB97]; it is not merely a space somehow ‘filled’ with information created for them to interact within. It is a ‘mechanism of interaction’ [BB01] that

facilitates the work necessary for translation, negotiation and agreement (at least temporary, local, and bounded to use), it supports interpretation, making sense and making meaning in relation to the objects within the CIS [SB92]. To do so, it must provide interpretive context to integrate activities that are happening on different ontological foundations in order for the various groups involved to continually assess and reassess the validity of the information produced [BB97]. This context provides such things as the situational context for the production and the conceptual frame of reference of the originator (how did they get the information? Why? To what end will they use it?). For a CIS to be enacted, it must facilitate expression and communication of alternative perspectives within a common problem domain. Simultaneously with this openness, it needs to enable boundaries and limits that allow for the creation of trust and translation between communities [SB92]. This also means that when the actions are distributed, so too are the centres of activity within a CIS [BB01]. The shared vision from a CIS emerges as a common objective, informal interactions, and the rhythms of work that produce and use the information [BB01]. Mechanisms that can support 'configuring awareness' [HSH+02] within a distributed team are also needed. These support practices of noticing and understanding other members' degree of awareness of information within the CIS and provide means to draw their attention to specific items when needed.

But a CIS will only work if those involved are mutually dependent on each other's work such that there is an allocation of accountability, which is more than just the need to share each other's resources [SB92]. Moreover, it cannot replace the human mediators and social networking for the development and maintenance of trust [BB97]. Nor does the virtual 'space' replace the physical places of action; rather the physical places in some ways overlays and in some cases may dictate information needs and uses [SB92].

The following sections will describe the subparts of this space in more detail in order to delineate the SecInCoRe approach. This knowledge is required to better understand the main content of this document, the requirement definition, the transformation to technical requirements and its analysis.

2.1 Cloud Emergency Information System

The Cloud Emergency Information System, as depicted in Figure 2-2, enables access to the knowledge base and handles service and information requests. Furthermore, aggregation of data from external services with the knowledge base is supported. Aggregation services' will be designed in line with ELSI guidelines and be constructed in a way that allow users to make themselves aware of risks of re-identification, data controller and accountability issues, and social sorting risks. External services are for example dynamic weather data and are in general openly accessible. Access to the database inventory is role-based, allowing the access and filtering of data according to the user's role and permissions, providing different level-of-detail of datasets. Role-management is in general very problematic and a lot of aspects has to be considered, like users having several roles, organisation based role than an individual role, tracking of activities of individuals.

The application subsystem provides a graphical user interface for displaying information that is transmitted via a secure gateway. Provisioning of information is based on web services that allow the user to handle diverse services via an

application store. The information could be used offline using a secure device (see section 2.2.1 and 2.2.2, see with D5.1 [8]).

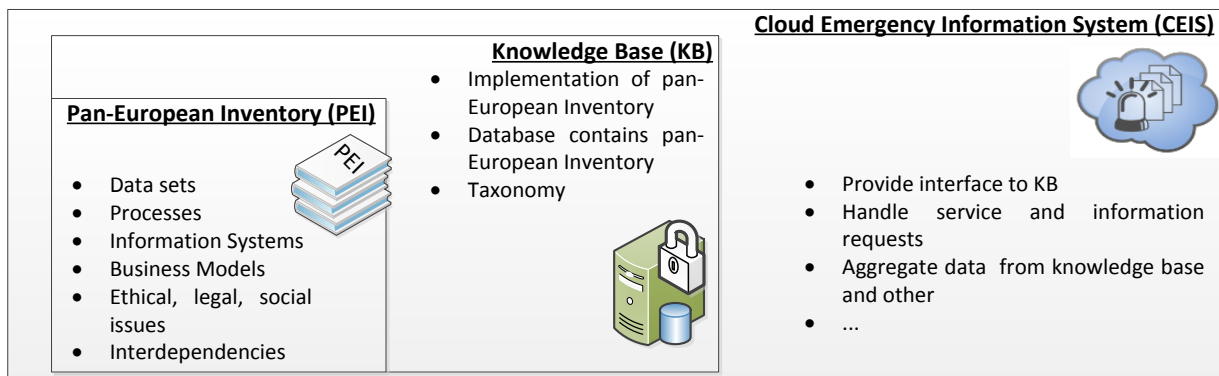


Figure 2-2 Cloud Emergency Information System (CEIS)

The main difference between the three parts are as follows: the inventory includes links to data sets, for example about processes, information systems, business models, ELSI, interdependencies and other materials. The knowledge base consists of a technology based implementation of the inventory and provides a database containing the inventory and taxonomy. The CEIS in the end handles service requests and gathers and combines data from external source to further enhance the information about disaster scenes. The data from external sources has been processed and is available for public or for the SecInCoRe case. The latter promises an ELSI aware handling of the gathered data.

The gathering and combining of data from external sources constitutes data processing, which, if it includes sensitive or personal data, is subject to data protection restrictions. A key question in this context is 'Who is the data controller?' This is a difficult question, because the data controllers for each of the external sources are presumably those who gathered it, and they gathered it for a specified purpose, which may be different here. There is legitimate ground to gather and combine data from multiple external sources for the potentially different purpose of disaster preparedness or response without the data subjects' informed consent if this is necessary for the responders to carry out their work in the public interest. However, participants in the CEIS may be reluctant to commit to such sharing and make their datasets available due to uncertainties about the legal situation. SecInCore addresses this challenge with multiple measures.

Technical measures should support transparency and clarify such uncertainties. For example a user or organisation could decide on its own if their data, parts of it are encrypted or not. Using device based encryption and network coding technologies enables the secure use of even unsecured communication channels. Within the cloud the data is stored securely, in addition if data is encrypted this is a further level of security.

However, technical support for controlled data processing in the CEIS is not enough. There also needs to be social, organisational and policy innovation to enable lawful and ethically and socially appropriate sharing. SecInCoRe contributes to such efforts through enabling experimentation with the potential of a CEIS and the development of ELSI guidelines.



2.1.1 Pan European Inventory

The description is based on [5]. For further information, please refer to it. This section presents an overview with the information needed for the rest of the document.

The usefulness of an inventory of past disaster events rests on a basic assumption: that societies can learn from past disasters. However, we approach it from the perspective that simply having more data available does not equate to more knowledge. Like technology, information ‘is at once a strategic resource and a social construct’ [J94]. Information does not easily move across organizational and cultural boundaries and it changes as it moves. The goal with SecInCoRe’s inventory is to make a system that can support professional practices of information management, information sharing and sense-making. In this light, the design of an inventory aims to create something more than a database that anyone can access, but a gateway to information that also accommodates, actively supports and informs a variety of practices, information needs, and command structures. The inventory also aims to be a system to foreground ELSI, issues at the heart of why disaster plans and response are accepted and trusted by the affected public. We want it to encourage decision-making that openly acknowledges ELSI.

There are various different private and public disaster inventories already in existence. Private disaster inventories include MunichRE’s *NatCatSERVICE* and SwissRE’s *CatNet*. Worldwide in content and focused on natural hazards, these inventories are primarily used for insurance risk assessment. Public inventories include *CRED EM-DAT* and *CRED CE-DAT* maintained by the Epidemiology of Disasters at the University of Louvain and the World Health Organization (WHO). Worldwide and open access, they focus on natural and technical hazards and are searchable by the general public. They aim to support humanitarian practice such as disaster preparedness, vulnerability assessment and priority setting. They draw on a range of sources—UN agencies, NGOs, insurance companies, research institutes, and press agencies—the output is quantitative. Slightly less global, *DesInventar* focuses on Latin America, Africa, and Asia, and is designed to generate inventories of damage, losses and in general the effects of disasters. It also focuses on natural disasters and is publically searchable. Within the EU, *eMars* is an inventory that aims to facilitate the collection and exchange of lessons learned from industrial accidents aimed at prevention and mitigation of future disasters. EU member states are legally required to report incidents to this inventory. The inventory, publically searchable, produces statistics and quantitative information. Also within the EU, there are a range of national disaster inventories, such as *ZEMA* (see: <http://www.infosis.uba.de/index.php/de/site/12981/zema/index.html>) in Germany and *ARIA* (see: <http://www.aria.developpement-durable.gouv.fr/about-us/the-aria-database/?lang=en>) in France. These provide a mix of quantitative data and short descriptions of what happened.

SecInCoRe’s inventory draws on features from many of these inventories, combining them into a single EU-scale collection of publicly available information. It may contain some summaries of past disasters, excerpts from publicly available information, but mainly contain LINKS to literature, as well as data sets, information systems, ICS, and similar. It also crucially holds links to data sets, command systems including information management processes, information systems and business models.



The inventory aims to enhance the collaboration among European countries to drive the sharing of data and other information in a way that is circumspect to ELSI opportunities and challenges. Most importantly, it will highlight the ELSI issues in disaster response in ways that make pathways possible and help people address conflicts in EU collaborations.

2.1.2 Knowledge Base

First of all the Knowledge Base (KB) is a technical implementation of the inventory to enable IT-based access to the inventory. In addition, the KB is coupled to other services in the cloud based emergency system (e.g., mapping of inventory information to a map, resource availability services) and further external services (e.g. weather services, satellite image provider, etc.). Accessing inventory content is realised by the KB that provides at least the access of authorized persons to pure, non-processed and non-filtered inventory content (e.g. raw data, but anonymised). Access means that no data is stored on personal devices, but for processing several services has to be defined in the KB. If needed and ELSI compliant data could be stored by agreeing a specific policy that also includes the deletion of data, after a specific time, this schedule will be developed during the further work in the project, depending on the user needs. The KB is not responsible for the handling of external, this will be done in the CEIS directly. The definition of services and how to handle the information content will be focussed in the ongoing work in WP3/WP4. The KB base allows us to further develop secure cloud services relying on the inventory content (see T4.5).

A taxonomy defines a uniform method for the classification of data sets according to specific criteria. SecInCoRe intends to derive a taxonomy for data set classification to enable the efficient and accurate integration of new disaster information to the inventory. Moreover, this taxonomy enables the efficient development of search engines for the inventory that will be provided via an individual web service.

2.2 *Network enabled communication system*

The network enabled communication system has two main use cases (see Figure 2-3):

- Firstly for enhancing secure local communications, for example a fire fighter transmitting data to their fire engine. This communication is mainly required for efficient response at the incident scene (e.g., communication between first responders inside and outside of buildings) (See section 2.2.1)
- Secondly the communication with the CEIS and a wide area network (e.g., Internet). This communication is needed for the transmission of information about the incident scene to further organizations that could include personal data (e.g. video) (See section 2.2.2). We are aware of transmitting personal data and the challenge to track the information flow, where it is stored, how it is processed and when this information will be deleted, this is even more important when the disaster scene is over and post processing will start.

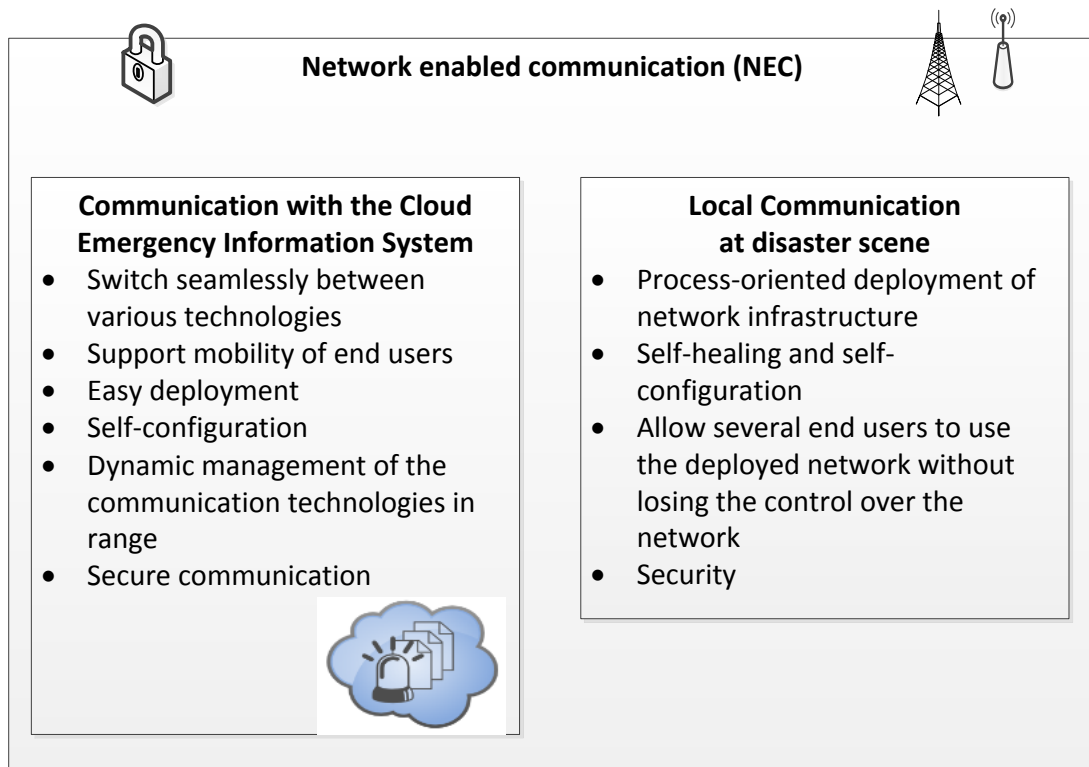


Figure 2-3 Network enabled communication (NEC)

Figure 2-4 presents an example of NEC, where both use cases are covered: communication between a fire fighter, his fire engine and a remotely located decision maker. Instead of using a wired connection between fire engine and cloud, LTE or 4G/5G is an alternative solution. LTE has the advantage of supporting the mobility of its users and offering high data rates, but in emergency cases the possibility exists that this infrastructure could be broken. Therefore the development of highly reliable, self-healing and self-configuring secure networks is indispensable for the creation of a network enabled communication in crisis management. The use of secure networks is part of section 2.2.1 and T4.5, where further studies and research will be made on this topic. In addition, we are aware that networks can be unsecure and there has to be a further security mechanism to guarantee the secure transmission of information and personal data.

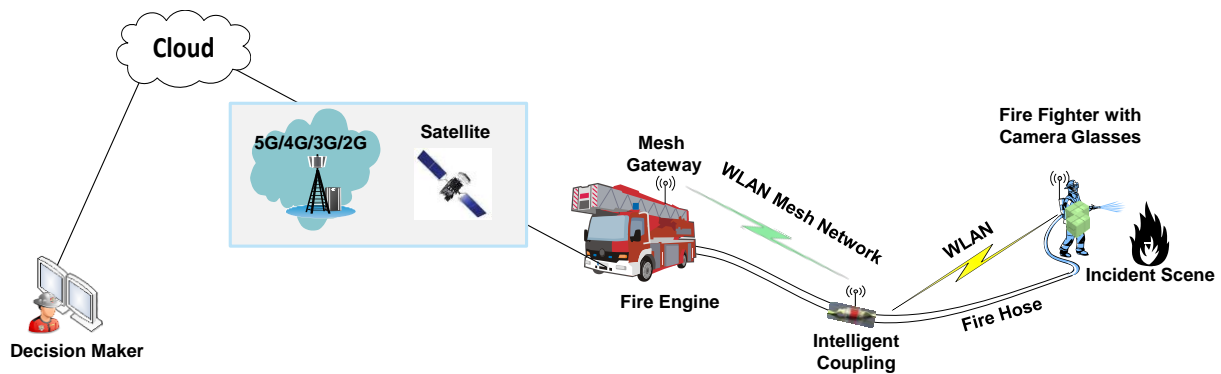


Figure 2-4 Communication via Mesh and 5G/4G/3G/2G or satellite from incident scenes with decision maker at a faraway location.

2.2.1 Secure local communications

Two use cases are the main focus of SecInCoRe when dealing with secure local communications. The first is when network communications are working but there is a need to interoperate between different organisations, (e.g., in case they have different operational management), users (e.g., first responders and volunteers), countries and technologies (e.g., Tetra, TetraPol, cellular Network like 4G/3G/2G, WLAN and further). The second is in case of network communications failure, when ad-hoc networks or backup networks such as “Cell on the Wheel” (COW) or “Network on the Wheel” (NOW), or Satellite can be used.

Handling disrupted communications infrastructures by setting up new networks or rebuilding broken ones is a key challenge during crisis situations. Secure wireless mesh networking can provide reliable high performance and low cost ad hoc disaster networks.

The surveys in [SVC13], [S13] and [NKJ08] present a comprehensive analysis of the security in WMNs. They point out that several attacks are common in wireless networks such as jamming at the physical layer, and these can be mitigated by conventional security mechanisms, while some attacks are specific to WMNs. The latter mainly includes attacks on the core service of the mesh backbone (i.e., routing), such as the wormhole and blackhole attacks, and user-related attacks, such as attacks on the user privacy with respect to data content, traffic flows, and location. The security of the routing functionality is addressed via PASER [SGB+14]. For privacy preservation and other user-related security services in WMNs, several approaches have been proposed in [LMH+12], [RYL+10], [WXC08], [WL06], [ZF06], which can be applied in combination with PASER. The security of the links between users and mesh access points are typically secured via the standardized mechanisms in the IEEE 802.11i or the IEEE 802.11s.

This technology has already received attention from various rescue organizations [WSW12] but the main problem - how to place mesh nodes efficiently in crisis situations, is as yet not standardized or integrated into current processes. The integration of wireless relays in fire hose couplings (see Figure 2-5) enables the on-the-fly network deployment by ‘piggy-backing’ on existing necessary practices to

establish a water supply. One main advantage to this approach is that there is no special training needed to set up or manage this network. With this solution, it is possible to cover the entire incident scene, even in mixed indoor and outdoor scenarios. A disadvantage is that hoses are not always required and/or there may be legacy equipment used in combination with new equipment and that may interrupt connectivity. Consideration of this highlights ELSI of technology dependence, which can be addressed by measures that support graceful augmentation that is redundancies between old and new systems and practices that retain organizational memory of 'traditional' ways of communicating [J07].

Local communications services provided by fixed network infrastructure also offer access to WAN services, such as voice (one to one and one to many communications) as well as NarrowBand data services.

Public Safety networks such as Tetra and TetraPol offer different solutions to provide local communications services in addition to the native capabilities provided by a fixed network infrastructure with its base stations.

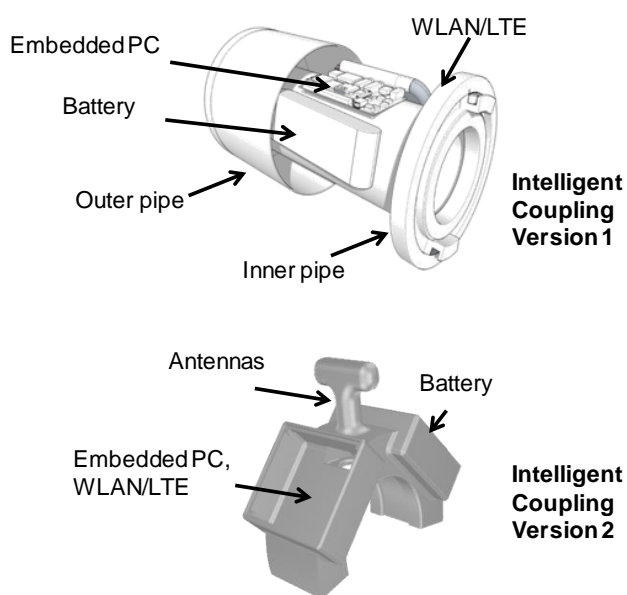


Figure 2-5 Intelligent hose coupling for one-the-fly network set up

These solutions rely mainly on the direct terminal to terminal communications known as Direct Mode Operation (DMO) in Tetra standards, Proximity Services (ProSe) or sometimes Device to Device (D2D) in LTE/3GPP standards. DMO provides the ability for radio terminals to communicate directly with each other over a limited distance of typically no further than 1000 m (like Walkie-Talkies) whether or not a Wide Area Network (WAN) is available.

This mode can be used to provide communications when WAN is not available and to extend the network services to terminals just beyond the available WAN coverage.

Services in this mode are mainly voice services and short data services (SDS).

Different types of communications are possible:

- direct call (one to one)
- group communications (one to many)
- Simultaneous connection to the WAN and to the direct terminal to terminal communications – called ‘Dual Watch’ in TETRA
- Network range extension for direct communications – called ‘Repeater’ in TETRA, ‘UE to UE relay’ in 3GPP
- WAN network range extension – called ‘Gateway’ in TETRA, ‘UE to Network relay’ in 3GPP

2.2.2 Communication with Cloud Emergency Information System

There is a strong need for **scalable** solutions that are able to connect autonomously deployed mesh networks with wide area networks and cloud infrastructures, like the Cloud Emergency Information System. For this purpose, local WiFi, 3/4G, satellite networks and even cache based approaches for spontaneous transmissions of non-time critical collected data are possible solutions. Only IP networks can provide cloud access. Enhanced mobility support and reliability can be achieved by providing seamless data roaming between these communication networks. For example - if one technology fails, the switch to another technology can be realised autonomously. The end-users at the incident scene do not have to care about how they are connected with each other and their control room. We are aware of cost implications for users, but for development processes we will assume the same costs for every network, because mobile data plan availability, we are further carrying out further research on that part. All networks are able to store data, but using end-to-end encryption leads to an efficient solution to overcome this problem.

Communication means not only the technological part of what devices or technologies are used or combined for communication. Moreover, the content of communication (e.g., information, datasets) and the kind of communication (e.g., protocols, information flows) have to be inspected and approved, especially related to the CEIS.

It was quickly evident, that an information system should not just manage the production of information from data. Even the managing of information flows in **scalable** ways should be a central focus of any useful information system. Information flows are even more important when several users are connected to the system. The response experts argued that the greater the circle of actors in any information sharing system, the greater the need to delimit accessibility and to guarantee added value for the different roles and responsibilities [5].

One effect of increasing the range of data sources is a need to create clearer rules for data perimeters. It starts with two questions: How far down the response chain does data need to go? How broad in range does the data need to be? It also involves managing on multiple planes of information sharing at once: sharing between strategic and tactical sections, sharing between agencies or with private companies, sharing in different phases of crisis management, managing public understanding, media messages, and social media trends. Multiple ELSI may arise in this complex data environment. By mapping information flows and data types that are circulating through



the CEIS, it is possible to support human judgement and accountability. Information flows will be derived in the further development within WP4, this will help to identify where data protection arises.

Sharing also needs to be scalable spatially, temporally, and practically so that it can be **basic** enough to be part of daily practice, **durable**¹ enough to work on international responses, and **adaptable** enough to incorporate new practices or technologies as situations call for. To work, SecInCoRe needs to design something, be it a technology or an organizational system that considers **everyday** incidents and **infrequent** ones, the **small** and the **large**, the **routine** and the **exceptional**.

¹ This requires, for example, tools that enable configuring awareness in distributed, hybrid physical and virtual spaces that allow people to make visible who is seeing what, and who is accessing what.

2.3 End User and Stakeholder Perspective

Different terminology is used to describe the potential users of the SecInCoRe CIS. Firstly there are first responders, police authorities, rescue/crisis organisations and related personnel that should reap benefits by using the CIS before, during and after a crisis situation. This group is normally described as end users or stakeholders. In the SecInCoRe case this group is even broader (see Figure 2-6). There is a second group beyond rescue organisations consisting of policy-makers and politicians, industry (e.g., information system provider), researchers, members of the public and volunteers.

To address the complex ELSI opportunities and challenges arising from SecInCoRe innovation it is important to enable broad-based participation in the inventory and understanding and debate about the potential of the KB, NEC, CEIS and CIS. This is facilitated through the SecInCoRe ELSI aware co-design approach (see D2.2 [5] for more detail).

SecInCoRe will create a common information space to enhance the communication and interoperability between these two end-user groups and within the groups. Special consideration of user needs should be paid to the second group of users, which is the requirement for a novel approach in crisis management.

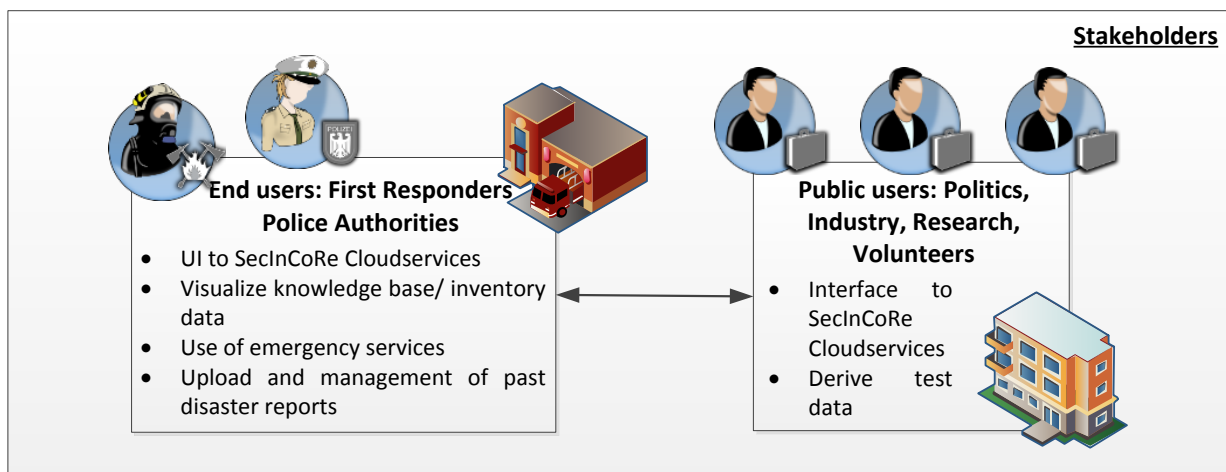


Figure 2-6 Stakeholders and users of SecInCoRe

Using this definition of stakeholder, SecInCoRe considers the following users. Please note that each group and even every single user can act independently. The number and kind of users or user groups will vary over time, depending on the individual needs and the information and service availability. For a further analysis of SecInCoRe stakeholders, please see D5.2 [9].

- Operation command (first responders/police authorities)
- Trainer (first responders/police authorities)
- Information manager (first responders/police authorities)
- Procurement manager, procurement legislation (first responders/police authorities)



- Policy Makers and Politicians
- Standardization bodies
- Information system producer and provider
- Researchers
- Volunteers and Members of the Public

2.4 Possible Benefit of SecInCoRe

To complete the figure of SecInCoRe innovation and the SecInCoRe tool description we will sketch a few benefits in this section. The complete overview will be handled in WP5 its deliverables D5.2 [9] and the following.

The benefits of SecInCoRe are manifold and a result of the interdisciplinary consortium working together in an intertwined manner on solutions regarding ELSI and technological potential. Rethinking technology through ELSI and vice versa facilitates sophisticated, creative and ambitious development and design that seeks to understand how technologies can be made appropriate to complex individual, social and societal needs. SecInCoRe's main areas of positive impact are: the social, the economic, the security and the environmental spheres. In fact, besides creating benefits for first responders and other rescue organisations, there will be a positive impact in the research community and for information system producers.

SecInCoRe will evolve the current state-of-the-art of many aspects of the emergency system; the main benefits will be both social and economic. At the current phase of the project it is not possible to describe the expected benefits in detail. However, it is possible to give a first qualitative overview of where benefits of the project are expected to occur.

Having social benefit in mind, the innovation pursued by the SecInCoRe project seeks to facilitate more informed, more agile, broad-based and coordinated emergency response. The inventorying of experiences from past disasters, data sets, command systems, information management processes, information systems and business models (as described in D2.1 and D3.2), and the facilitation of common information space formation and secure and dynamic information sharing can enable better preparedness, which is at the heart of nurturing resilient societies in a 21st Century that has been labelled the 'century of disasters'. Moreover, SecInCoRe enables better engagement with the public by enhanced integration of multiple data sets and integration of information practices amongst affected populations and volunteers.

Based on the above issues, economic benefits arise by enabling more economical emergency planning, response and recovery. This is enabled by learning from past methods, experiences and enhanced information awareness in disaster management.

Technological innovation by flexible networking infrastructures and flexible security leads to supporting technology usable for every user and information at the right place at the right time. Please note that SecInCoRe does not develop a new technology, it focuses on the efficient interoperability between existing technology and its improvement.

Combining information systems, technological solutions with ELSI through value sensitive or ELSI aware co-design (as described in D2.2) is a powerful and novel



approach developed in SecInCoRe. There are a whole host of positive and negative ELSI, as we have outlined, and there is currently significant confusion over legal regulation relating to data protection, big data analytics and information sharing as well as their ethical and societal implications [A07][G13][B-W13]. Even when known, it is difficult to address issues such as transformed accountabilities and liabilities for responders, demands for privacy preserving data sharing, and dangers of social sorting and preventative security measures in practice. In addition, there is a lack of trusted innovative technological support for human practices of reasoning, collaborating, noticing and managing ethical, legal and societal issues arising in the appropriation of common information spaces and infrastructures. SecInCoRe maps ELSI in relation to IT innovation in crisis response (see D2.2) and carries out privacy impact assessment, ethical impact assessment and a range of more integrated methods of value sensitive design, along with privacy by design methods [C01], [CH02], [C12] and [L01] and other forms of technological innovation that respond constructively to the opportunities and challenges.

Moreover, SecInCoRe intends to develop guidelines for efficient interoperable practices between organisations by bridged uses of the CIS. At the same time, the CIS will improve the politics of cooperation and resource sharing among different countries (as agreed in the European Civil Protection Mechanism (CPM)¹) thanks to better crisis management thought the sharing of management plans and resource information.

A more comprehensive overview of main benefits will be provided in deliverable 5.2 [9].

¹ The Civil Protection Mechanism facilitates co-operation and resource sharing between EU member states in disaster management. In accordance with the principle of subsidiarity, it can provide added-value to European civil protection assistance by making support available on request of the affected country. EU Civil Protection Legislation ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_legislation_en.pdf

3 Requirement Categories and Initial Use Cases

There exists a huge variety of requirements related to crisis management, interoperability and processes of rescue organisations. This document will only focus on the requirements that are relevant for the development of the SecInCoRe project. Firstly, the requirements are separated into quality and functional requirements derived from engagements with users and those identified in relation to the architecture of the system. Quality requirements are related to the Quality of Service (QoS)¹ and the Quality of Experience (QoE)² the user or the system is going to work with (see Chapter 5). Functional requirements are related to special services and functions that are identified in interaction with users and the various system components (see Chapter 6).

3.1 Requirement Categories

Based on existing knowledge in the project related to crisis management and initial interviews with end users, the following categories of requirements have been derived:

- **ELSI:** Identification and incorporation throughout the design of relevant ELSI in order to develop a deeper understanding of the socio-technological context in which the SecInCoRe project is to make a productive, ethically, legally and socially circumspect, innovative and useful contribution to collaborative and cross-border disaster response
- **Security:** Services should not compromise the current security architecture. Additional integrated security solutions have to be developed.
- **Operative:** All solutions and services must regard the current operative state-of-the-art and should be able to integrate with as little effort as possible.
- **Regulatory:** All solutions must work with regard to national regulatory aspects.
- **Technical:** The technology that is selected and used must fit the use case and shall be usable under extreme conditions (e.g., weather, light). The technology shall further be usable without the requirement of being an expert. The developed solutions should consider and build on existing technology as much as possible.

3.2 Initial Use Cases of CEIS

In this section initial use cases relevant for the CEIS are outlined. Please note that the provisioning of information is not linked to initiating actions from users. For all use cases we assume that the information will be provided by the CEIS. The use cases are

¹ Quality of Service (QoS) describes in general the overall performance of a communication network (e.g., computer network) from user's point of view. Typical performance measures are error rates, bandwidth, throughput, transmission delay, availability. Transmission of data with specific requirements are coupled to QoS requirements. Using this definition the original use case of a communication network can be adapted to new applications. For this reason, we use this term for the description of qualitative requirements for the SecInCoRe project.

² Quality of Experience (QoE) describes in general a measure of user's experience with a communication service (e.g., web browsing, video call). QoE focusses on the overall experience and therefore this measure is more holistic than QoS.

useful to help identify in which situations specific data may be beneficial. The use cases do not describe how access to the information should be realised (manually, semi-automatic, automatic, what technology is used, etc.). Moreover no information about the presentation of information (e.g., how they are displayed) will be described in the initial use cases.

The following sections describe possible available data sets for proposed users of SecInCoRe. The sections outline first what can be provided today, based on the first inventory as collected in D2.1 [4], D3.1 [6] and D3.2 [7]. There are data sets, command systems including information management processes, information systems and business models. Followed by a conclusion describing an objective of future provisioning of data sets.

Table 1 lists use cases for end users, like first responders and police authorities and other rescue organisations. Table 2 lists additional use cases that occur by other users. Besides the entering and the retrieval of information for individual purposes and the ability to search for inventory content, the improvement of regulations and public-private partnerships as well as the harmonization of European disaster response are additional use cases. The latter are mainly driven by politics and standardisation groups. Having these use cases in mind, ELSI issues and especially guidelines are of high importance for this group.

Table 2 summarize the initial use cases for end users and examples of other users. The main difference between these two user groups are the specific impact of information the individual user groups can access and use for their own purpose. As described in Table 1, the main use case for end users is to enter and retrieve information for the individual use case and to search for inventory content. Using the CEIS will therefore enhance the information awareness in disaster management.

Table 1: Initial use cases for first responders and police authorities

Use Case	End users: First Responder, Police Authority			
	Operation command	Trainer	Information manager	Procurement manager, legislation
Entering information to the knowledge base ¹	Adding expert information about own processes and use cases			
Retrieve information for individual purpose from inventory content	decision support	configuration, validation of simulations, training scenarios	adaption procurement	configuration, validation of simulations, benchmarking scenarios

¹ We assume that the users are willing to share these information within a certain community.



				adaption procurement
Search inventory content	yes			

Table 2 lists additional use cases that occur by other users. Besides the entering and the retrieval of information for individual purposes and the ability to search for inventory content, the improvement of regulations and public-private partnerships as well as the harmonization of European disaster response are additional use cases. The latter are mainly driven by politics and standardisation groups. Having these use cases in mind, ELSI issues and especially guidelines are of high importance for this group.

Table 2: Initial use cases for example other users

	Users		
Use Case	Political and standardisation bodies	Industry: Information system producer	Research
Entering information to the knowledge base ¹	Adding expert information about own processes and use cases		
Retrieve information for individual purpose from inventory content	adaption legislation	prepare for customised demonstrations	analysis / validation
	identify gaps in the provisioning of data and information systems, request new innovative services	development of innovative services	build new research project approaches up on existing projects instead of building yet another solution from scratch
Search inventory content	yes	yes	yes
Improve of procurement regulations and Public-Private-Partnerships	yes	n.a.	n.a.

¹ We assume that the users are willing to share these information within a certain community.



Harmonise European disaster response	yes	n.a.	n.a.
--------------------------------------	-----	------	------

The following sections describe the initial use case in more detail by giving an overview about used information and data sets. These are mainly derived from WP2 and WP3.

3.2.1 Entering of information for individual, organisation and group purposes

The inventory stays alive by entering information from the broad range of stakeholders. Therefore an initial use case is to add data and make them available for other CIS users, and/or use the CIS for accessing this information at several places or use it firstly within an organisation to provide data to several groups within the own organisation.

A great challenge is to convince users to share their data. This document collects a first setup of requirements that are the basis for user driven design of such an inventory. Users will only share their data if this is secured and it could be guaranteed that no misuse will be done with this data.

3.2.2 Retrieval of information by individual and groups

The most relevant use case is the retrieval of information for individual organisation or group purposes. Here a group could be even interdisciplinary. Retrieval of information means the access to unfiltered pure data that has to be processed by the user on their own for their individual purpose. This can lead to cases where data can be used for purposes other than those it was collected for. This require either informed consent or an exceptional legitimation. SecInCoRe is aware of this issue. For example the inventory itself will not hold such data. If such data is requested via the CEIS, the purpose has to be stated. ELSI guidelines could be made available that will explain explicitly how and when this data can be used for other purposes than the intended one.

The retrieval is based on the defined data sets and does not cover any searching or filtering capabilities. Table 3 presents an overview for end users, Table 4 for example of other users. There are various use cases: past disaster, data sets, command systems, information management processes, information systems as well as business models and ELSI are of interest for these user groups. The processing of the retrieved information is manifold. End users are more interested in disaster preparedness, recovery and response. Research organisations on the other hand process the information in a simulation environment or perform other studies in order to develop innovative solutions for future crisis response. In addition, political organisations are for example interested in the ELSI information or crisis management models they can gather from the inventory. Furthermore, research organizations are interested in building new research projects. They are able to retrieve information to assist in building new project approaches on top of existing projects, instead of building yet another solution from scratch. Here the focus is on inventory content based on and about research projects.



These tables do not claim to give a complete overview. They are just presenting the current results and will be extended as SecInCoRe progresses.

Table 3: Initial use case “Retrieving” for end user

		End User: First Responder, Police Authority			
Retrieve information for individual purpose from inventory content		Operation command	Trainer	Information manager	Procurement manager, legislation
Past disaster	procedure, development	x	x		x
	lessons learned, best practices	x	x		x
Data sets	used databases	x	x	x	x
	available databases	x	x	x	x
	data quality		x		x
	demanded information			x	
Command systems	specific processes	x	x		x
	deviations from processes		x		x
	hierarchy	x	x		x
Information management processes	procedures, information flows			x	
Information systems	open platforms (e.g. providing access to open data)	x			
	interfaces applicable to share resources during response	x			
	to be considered/included		x		x
	prospective use of available information systems		x		x
	information provided, demanded by the system			x	



Business models	PPP	x	x		x
	digital volunteers	x			
	data procurement			x	
	procurement processes				x ¹
ELSI	implications with regard to all categories of artefacts	x	x		x
	guidelines	x		x	
	esp. legal constraints			x	

Table 4: Initial use case “Retrieving” for example other users

		Users		
Retrieve information for individual purpose from inventory content		Politics, standardisation bodies	Information system producer	Research
Past disaster	procedure, development			x ²
	lessons learned, best practices			x ³
Data sets	used/available databases		x ⁴	x ⁵
	demanded information		x	x ⁶
Command systems	specific processes			x
	deviations from processes			
	hierarchy			x
Information management processes	procedures, information flows		x	
Information systems	open platforms (e.g. providing access to open data)			

¹ In the case of retrieving information for adaption procurement from inventory content

² data source for test and simulation data

³ data source for test and simulation data

⁴ benchmarking/testing with realistic data

⁵ data source, identification of information demands

⁶ data source, identification of information demands



	interfaces applicable to share resources during response			
	most common IT systems in the context of a (potential) customer		x ¹	
	prospective use of available information systems			
	benchmarks			x
Business models	PPP responsibilities	x		
	digital volunteers			
	overview procurement options (e.g., licensing)			
	procurement rules and processes	x	x	
	lessons learned			x
ELSI	data from interviews, workshops			x
	guidelines	x	x	x
	esp. legal constraints	x		

¹ identification of market situations

3.2.3 Search inventory content for information

The second initial use case is to search the inventory for specific information. Searching in contrast to just retrieval means to combine different data sets, enable filtering options and mapping of different searches. Here the same information categories as before are of main interest: past disaster, data sets, command systems, information management processes, information systems, business models and ELSI. Table 5 gives an overview for end users, table 6 for example of other users. The operation command is able to search the inventory for example for past disaster at a distinct location, or sorted by the type of incident. A procurement manager can start a specific search for recommend practices or business models. The benefit for every user is different, but the objective remains to provide valuable information for every user.

In further studies in WP4, especially T4.6 Design of secure cloud services, we will investigate research in the field of searching mechanisms. One key challenge is to search in the CEIS that links to external info and not holding all the data.

Table 5: Initial use case “Searching” for end users

		End User: First Responder, Police Authority			
Search inventory content for information		Operation command	Trainer	Information manager	Procurement manager, legislation ¹
Past disaster	actual location	x			
	type of geographical surroundings	x			
	type of incident	x	x		
	type of and actual organisation involved	x	x		
Data sets	availability	x	x	x	
	content	x			
	organisations usage		x	x	
Command systems	organisation	x	x		
	country/region	x	x		
Information manageme	organisation				
	country/region			x	

¹ use the inventory content to get overview about specific topics



nt processes					
Information systems	functionalities, characteristics	x	x	x	
	organisations usage	x	x	x	
Business models	PPP		x		
	regulations/legislation				x
	responsibilities				x
	recommend practices				x
ELSI	implications with regard to all categories of artefacts		x		

Table 6: Initial use case “Searching” for example other users

		Users		
Search inventory content for information		Politics, standardisation bodies	Information system producer	Research
Past disasters	location			x
	incident			x
	organisations involved			x
Data sets	organisations usage		x	
	availability		x	x
	demands		x	
	content			x
Command systems	organisation			x
	country/region			x
Information management processes	organisation		x	
	country/region		x	
Information systems	functionalities/characteristics		x	x
	organisations usage		x	x
Business	regulations/legislations	x	x	x



models	responsibilities	x	x	
	recommend practices	x	x	
	country/region			x
ELSI	actual ELSI		x	
	guidelines	x	x	x
	data from ELSI related research			x
	ELSI initiatives			x

3.2.4 Identify gaps in the provisioning of data and information systems

Besides retrieving or searching information, there are further initial use cases driven by politics and standardisation bodies. One is the identification of gaps in the provisioning of data and information systems in current processes of crisis management. Politics and standardisation bodies have access to provided datasets and information systems currently in use in crisis management. Relying on this information they can identify gaps and optimization potential. These gaps are the foundation for further project and service requests to other organizations.

In general in this use case, data sets, like publicly funded databases (Examples of database providing geo referenced data are: <http://www.eionet.europa.eu/gis/>, <http://edit.csic.es/GISdownloads.html>, <http://www.gis4eu.eu>, <https://lib.stanford.edu/gis-branner-library/data-websites-europe>), information systems and ELSI are in focus.

For the latter, ethical and legal constraints and guidelines will help to identify gaps in data provisioning. For information systems, further questions must be addressed, such as which of these systems are provided by higher level bodies, which are generally available (like Google Crisis Response), and which interfaces and especially data exchange formats are available. The last question allows the definition of additional systems that can interact and interlink with these existing information systems.

3.2.5 Harmonise European disaster response

A further initial use case is the harmonisation of European disaster response, also mainly driven by politics and standardisation bodies. Here the focus is on data sets, command systems and information systems.

The provisioning of data sets from a European perspective and a comparison of the use of this data in different countries and command systems needs to be conducted. Further research and information gathering is needed if a harmonised European disaster response solution is to be successfully developed.

Having a close look at existing and maintained command systems in practice, helps to identify gaps of these systems. Further, a comparison of European processes is enabled: what are differences between the defined processes and how they are maintained in practice (i.e., theory vs. practice)?



The analysis of information systems will lead to pan-European provisioning of information systems for disaster response and will enable a more efficient definition of interfaces between IT systems.



4 Requirement Life Cycle

A requirement life cycle describes the usage and the benefit of each requirement in the project and ensures the consideration of identified requirements during the iterative validation process. This validation process is proposed to be highly end user related, caused by the high numbers of requirements derived from this group. Together with the knowledge of the consortium it is possible to set up this document including a variety of requirements covering disaster response, recovery and prevention.

The requirement life cycle is divided in seven main steps or states:

1. Requirement definition
2. Transfer to technical requirement
3. Communication and traceability of requirement
4. Mapping of end users expectations and technical requirements
5. Input to development
6. Input to validation and evaluation
7. Verified and validated requirement

Step 4 and 5 are repeated in an iterative manner based on the end user feedback and results out of the validation process. Validation and evaluation activities are dependent from development activities that are mainly executed in WP5. The objective of the overall validation process with regards to the defined requirements is to emphasize the usefulness of SecInCoRe features and to measure the impact on the day-to-day working routine of end users.

Figure 4-1 depicts the validation process in consideration of the requirements and shows its relationship with stakeholders. The final box emphasizes the outcome of the process, mainly highlighting the value for each user.

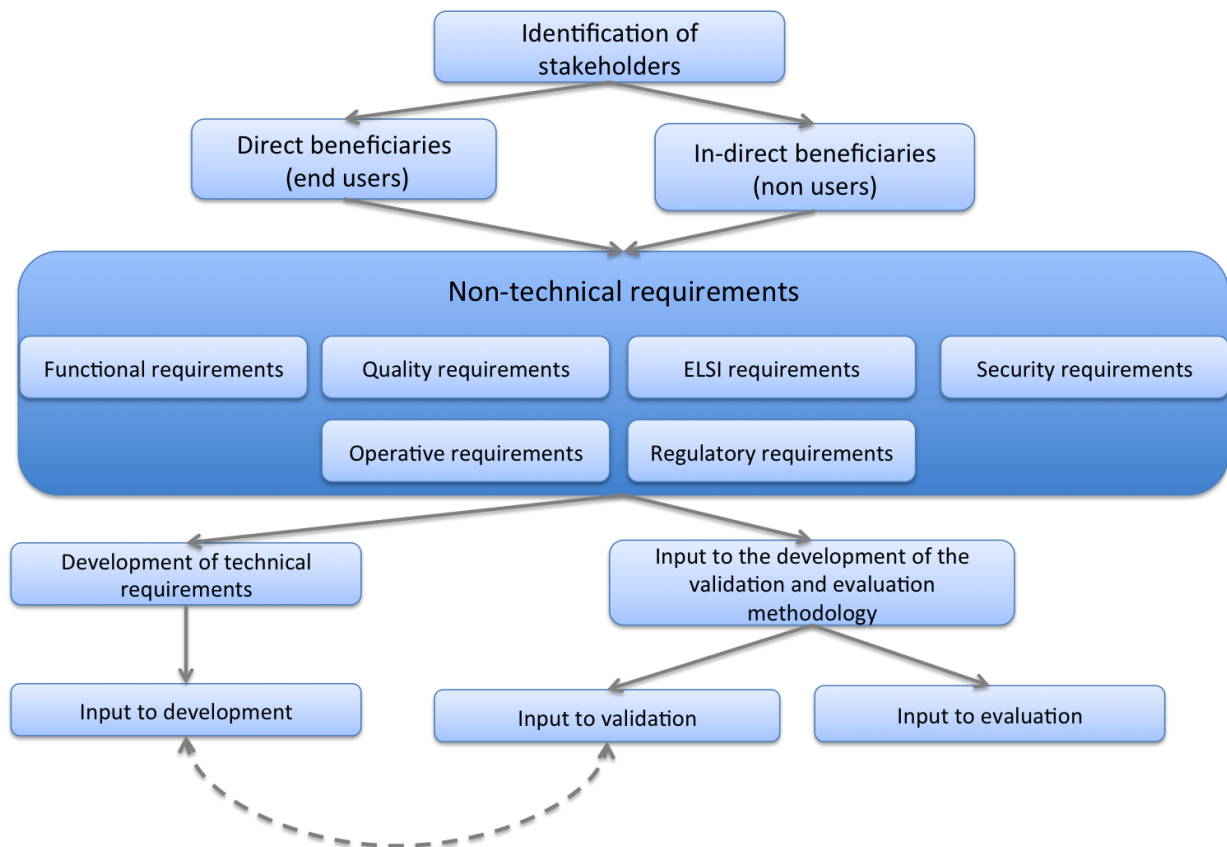


Figure 4-1 Requirements circle and validation activities

The next step in the requirement life cycle is the definition of an initial scenario of SecInCoRe services based on results in WP2, 3 and 4. D4.2 [10] will describe this scenario and in addition dealing with Concept of Operations, Systems Views, High Level Requirements based on the first workshop with end users related to crisis management organizations held in December 2014 (see D2.2 [5]). Following this process, the transfer to technical requirements according to the technical development is planned (T4.2 and related in WP4, T5.1) and the mapping of end users expectations as well as technical requirements (T4.3). The further validation process is link to activities in WP5 (see D5.1 [8] and D5.2 [9]).

5 Quality Requirements

This chapter copes with the definition of quality requirements. Quality requirements are related to user satisfaction and system dimensioning. The terms Quality of Service (QoS) and Quality of Experience (QoE) are adapted from the field of communication network to SecInCoRe, because their original meaning describes the service and user satisfaction in communication networks. Whereby QoS is more a quality parameter of any specific service and can therefore be seen as a service contract. QoE however evaluate the holistic process and can therefore directly mapped to user satisfaction. Furthermore, quality requirements from the system point of view are defined. This is mainly related to interfaces and data processing. In general, qualitative requirements are measurable, for example scalability and availability of the system.

This chapter is divided into two parts: firstly the requirements derived in interaction with users are given. These are followed by requirements from system point of view, derived from the knowledge within the SecInCoRe team. This lists are not final, yet. The ongoing evolution of processes and technology can lead to new requirements that will be added in the following deliverables of WP4.

5.1 *Requirements derived in interaction with users*

5.1.1 Police authorities, crisis organisations and first responders

- Resource efficient
- Size: sufficient, but not hindering the process
- Weight: low, but without loss of functionality
- Clear usability: The usage should be as simple as possible and possible without being an expert in technology.
- Integration with current systems and cross-platform suitable
- Based on already existing technologies and processes
- Real-time use
- Reliability
- Low-cost solution
- Supporting the current process in an intelligent manner
- No additional expenses
- Robustness: protected against physical influences
- Energy-efficient
- Time to access information

5.1.2 Politics, industry, research and volunteers

- Transnational coordination
- Accurate data for research purposes
- Support cross-cutting activities



- Uninterrupted services (back up infrastructure to ensure continuity), fast browsing and search.
- Long stand-alone operation for any portable device
- Kind of information provided
- Time to access to information

5.2 Requirements from system point of view

5.2.1 Communication and cooperation between organisations

There are not so many new requirements to communication networks, since these networks are already deployed and must be leveraged as much as possible as they are. SecInCoRe aims to optimize the combined usage of these existing technologies.

- On-demand access to the information: on-demand network access should be established in a transparent manner to users.
- Bear in mind the (throughput) capacity of communication network technology (e.g., TETRA and TETRAPOL, LTE)
- IP networks offering interoperability with TETRA/TETRAPOL

5.2.2 Inventory base

- Ensure correctness of data
- Ensure completeness of data
- Clarity of data
- Search Categories Options
- Advance search capabilities, able to combine key words, Type of disaster, location, etc. to minimize the results and research time.
- User profile targeted (i.e. if a user's profile does not match with global access levels, there should be a filter on the data available to the user)
- Status of engaged agencies, i.e. in use, available, reserved, damaged etc.
- Status of involved assets, i.e. in use, available, reserved, damaged etc.
- Each "item" (or an event) or asset should have a history or log. Whenever something changes, one can write a log entry just to tell what or how has been changed.

5.2.3 Cloud Platform and Cloud Services

- Indicator of available resources (e.g., free hospital beds, specialisation of hospitals)
- Service for on-the-fly transmission of number of injured people, damage to the related hospital/organisation.
- Service for the identification of related auxiliary facilities in range, depending on the scenario



5.2.4 Data protection

- Anonymized data: The challenge of how it is ensured that the data is properly anonymized is a field of study in SecInCoRe. In D2.1 [4] an anonymisation guide is proposed. The key is to acknowledge that complete anonymisation is not possible.
- Secure access to the CEIS
- Secure communication within the CIS: that means a) secure local communication, and b) secure communication to access the CIS.
- Secure interfaces within the CIS: Transmit information via secure interfaces and use secure interfaces for gathering external data.

6 Functional Requirements

In addition to quality requirements, this chapter defines functional requirements from a user and system point of view. Functional means required functionality for supporting existing process that are related to services. These services are manifold and are dependent on the user and the system components. Typical functional requirements are for example search capabilities with several keywords. Furthermore, having ELSI in mind, services for requesting ELSI guidelines are important for nearly every SecInCoRe user.

This chapter is also divided into two parts: firstly the requirements derived during interaction with users are given. These are followed by requirements from the system point of view, derived from the knowledge within the SecInCoRe team. These lists could also be extended when new requirements arises during the project or for example during validation activities.

6.1 *Requirements derived from interaction with users*

- Guidelines regarding ELSI
- Guidelines for accessing the information
- Integration in existing devices (e.g., smartphone, tablet, laptop, etc.)
- Integration in OS (e.g., Android, iOS, Windows phone, etc.)

6.1.1 Police authorities, crisis organisations and first responders

- Guarantee readability and usability under worst external conditions, like sunlight, rain, etc.
- Ensure the quality and correctness of entries
- Lock and unlock to avoid unwanted entries
- Focus on relevant information
- Automated warning function (e.g., toxins in the air, fire)

6.1.2 Politics, industry, research and volunteers

- How-to and guides for behaviour in certain situations based on past-disaster data (like an emergency plan for a building, if possible make them available for users on their smartphone)
- ELSI safe transmission of pictures and videos of the accident and the disaster
- Offering expertise, for example a doctor on holiday
- Visible and audible messages
- Interface to automated warning systems (e.g., toxins in the air, fire)
- Level playing field for industrial player
- Heterogeneous interoperable portable communication system to make communication efficient even for cross-border operation or joint operations in one country of multi-agency participants.



- Assistance to reduce the time for the decision making process by comparing relevant past disasters
- Based on the current state of a disaster, the system should estimate the evolution of the disaster (by weather forecasts for example) and propose solutions
- Availability of analytics: we need a way of automatic tracking the interactions between the “system” and the users (during workshops or in real-case scenarios)

6.2 Requirements from system point of view

6.2.1 Inventory base

- Search capabilities based on specific date(s) (e.g. DD/MM/YY to DD/MM/YY)
- Search based on location, type of disaster (e.g. fires, floods etc.)
- Advanced search capabilities, able to combine key words, type of disaster, location, etc. to minimize the results and research time.
- User profile targeted (i.e. if a user's profile does not match with global access levels, there should be a filter on the data available to the user)
- Status of engaged agencies, i.e. in use, available, reserved, damaged etc.
- Status of involved assets, i.e. in use, available, reserved, damaged etc.
- Each "item" (or an event) or asset should have a history or log. Whenever something changes, one can write a log entry just to tell what or how has been changed

6.2.2 Cloud Platform and Cloud Services

- Services for forecasts of datasets (e.g., resource availability)
- Services for past events
- Services for current data
- Enable different level of detail of information

6.2.3 Communication and cooperation between organisations

- Awareness of communication link quality
- Leverage the best communication network for a given service

6.2.4 Data protection

- Detection of non-anonymised data
- Terms and conditions for usage that has to be accepted before access

7 Transfer to technical requirements

For development purposes, quality and functional requirements have to be transferred to technical requirements (e.g., what means simple technology?). Those are more the requirements driven by the used system(s). Only in this way, they could be considered during the technological development process. The current phase of the project foresees the definition of common terms, the definition of requirements based on existing knowledge, the first end user workshop and the definition of initial use cases. This chapter describes how to transfer the above derived requirements into technical requirements and their respective handling in the requirement life cycle process of the project.

For the handling of technical requirements, a scheme is defined (see Table 7) that contains all relevant information as to the meaning of the requirement, the relation to validation activities and its consideration in demonstration. The elements are described as follows:

- Identifier: A clear identification using a short format of the name of the requirement and the category.
- Priority: There are mandatory or recommended requirements depending on the use case and the users.
- Short description: Provides a short description of the requirement that is indispensable for the understanding and correct assignment to evaluation and development processes.
- Precondition: There could be some input or preconditions to fulfil this requirement. This includes solutions to address ELSI by design (details will be specified throughout the project, utilizing methods of PIA and EIA).
- ELSI: Special issues that are applicable to the requirement will be described in the ELSI field. If nothing is mentioned the overall ELSI guideline is valid and will be regarded within the development and validation process.
- Relation to demonstrator and validation activities: This field describes if the requirement will be considered in the overall validation, the early demonstrator and if already known, which validation activities are in focus. Further requirements towards test cases are mentioned.
- Additional information: In addition to the short description, further information is given here. This can be additional explanations or specific background needed for the accurate use of the requirement.
- Initiator/author: The responsible and initiating partner or person abbreviation shall be included. This can be different from the partner(s) who has to regard this scheme during the implementation process.
- Source/WP: An external source and or the related WP should be mentioned in this field. This enables to assign responsibilities.



R-Sec001	Network security	Priority	mandatory
Short description	WPA2 encryption has to be used for secure WiFi access		
Precondition	Address ELSI issues, especially relating to the requirement to ensure that data is transferred and stored securely in accordance with data protection principles.		
ELSI	Add ELSI in this field if applicable		
Relation to validation activities	Considered for the demonstrator	Validation activity	
	Early Demonstrator	WPA2 is used within the demonstrator	Validated in workshops with end users? Yes, it will be part of the demonstrator that is used for end user validation.
	Requirements towards test case: n.a.		
Additional information	n.a.		
Initiator/ Author	TUDO	Source/WP	WP4

Table 7: Requirement scheme for technical requirement

Related to further tasks in the project in WP4 and WP5, technical requirements will be derived in the following fields, mainly relying on the requirements already derived from end users and existing knowledge in the project:

- Technical requirements of the cloud platform (→ Task 4.6 and Task 5.1)



- Technical requirements of cloud services (→ Task 4.6)
- Technical requirements of end user Interface for accessing the CEIS (Task 5.1)
- Technical requirements of communication (→ Task 4.5)
- Technical requirements of cooperation between organisations (→ Task 4.4)
- Technical requirements of data protection (→ Task 4.5 and Task 4.6)

During the development of the early demonstrator, the first technical requirements regarding service availability and security have been already identified and described in D5.1:

- Requirement R-Sec001: WPA2 for WiFi Access
- Requirement R-Sec002: SSL for CEIS connection
- Requirement R-Sec003: Secure cloud access using Radius and LDAP
- Requirement R-Sec004: Secure cloud access using one time passwords
- Requirement R-Sec005: MAC address filtering
- Requirement R-Sec006: Storage encryption
- Requirement R-Sec007: Security policies

8 Collaborative Requirement Management

Collaborative requirement management can be supported by the use of software. The consortium agreed on the use of JIRA for this purpose. In general JIRA is a project management tool, which provides a compilation of various tools to track issues, bugs and other processes of several kinds. The center of Jira is built on Workflows. These workflows are fully customizable to the needs which occur in the process. Furthermore, issues can be defined, organized and prioritized. These issues can be connected to their own workflows in order to customize the process. Actions taken by one person in the process can be seen by other project members, allowing everyone to keep track of requirements and get notifications instantly as changes happen.

Integration of requirement life cycle

In SecInCore it is important to have a lifecycle for requirements that appeared in the early demonstrator (see D5.1), the Co-design workshop and in the inventory set up (compare WP2). With the help of JIRA, these lifecycles can be tracked by creating fitting workflows. Requirements can then run through the different steps of creation and validation.

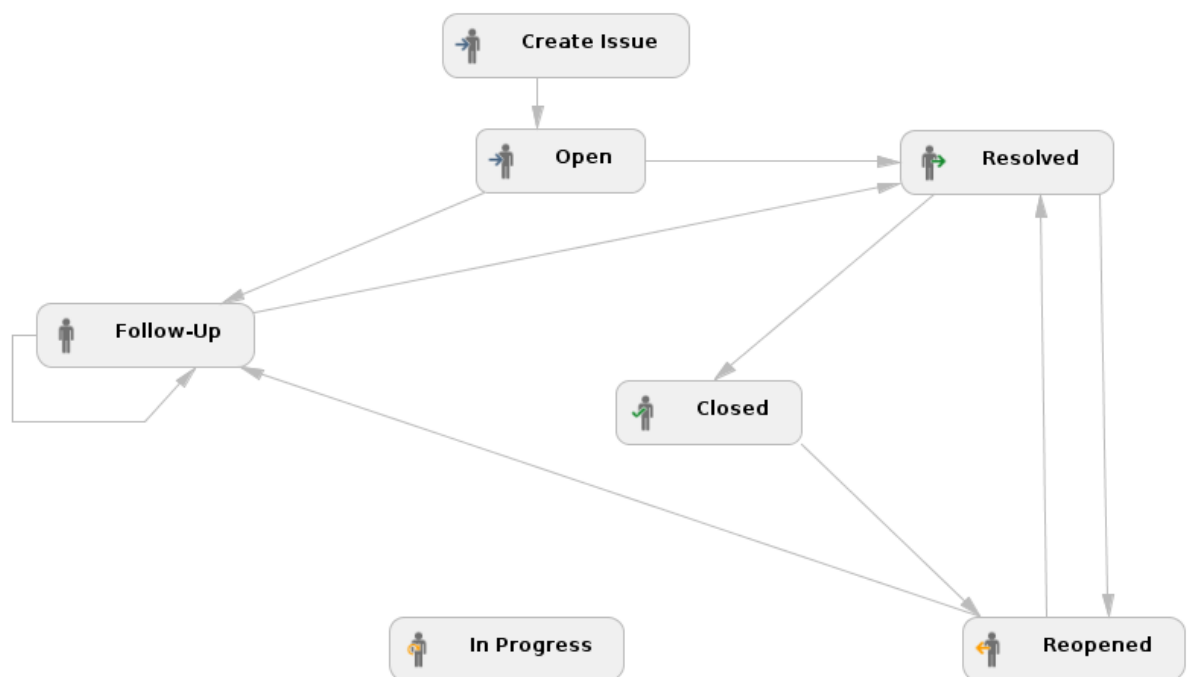


Figure 8-1 Example workflow in JIRA

To help with planning and reviewing, it is necessary to have different user groups each with different rights to the various lifecycle steps. This is important in order to ensure that requirements cannot be deleted or edited by every user. While users with approval rights take the role of supervisors which can request approval on reported issues, users with editing rights can review, make changes to the individual requirements or create new ones. JIRA offers the ability to integrate different access levels and update the status of the requirement in the lifecycle at the moment it happens.

The requirements in JIRA are divided into two different categories: Unplanned and planned requirements. Modifications to unplanned requirements can only be done by users with editing rights. They can either be validated, invalidated or given to users with approval rights. When the unplanned requirement is given to a user with approval rights, it is changed to a planned requirement, which can run through the process of approval or can be reviewed and changed by editing users.

In further detail, what this means is that users with approval rights can give suggestions to the requirements. Issue review and the actions which can be taken are done by the user with editing rights, who give the now developed and reviewed requirement back to the users to request approval. The requirement can then be approved or run through the loop of development and review again, until it is finally approved.

This lifecycle can be integrated into a Jira workflow so that every requirement can go through the different stages of the lifecycle without requiring much effort of the two different kinds of users in regards to planning and organising the required work.

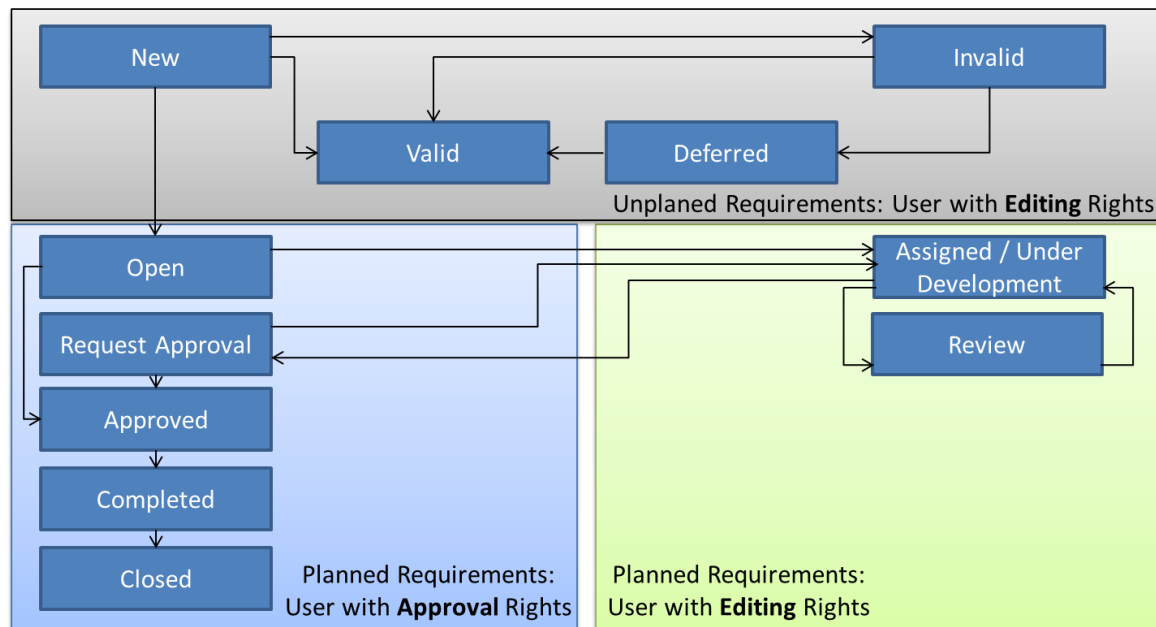


Figure 8-2 Planned and unplanned requirements in JIRA

9 First Requirement Analysis

This chapter describes the first requirement analysis related to the development process of the early demonstrator, related to D5.1 [8]:

9.1 CIK-Framework

As proposed in D5.1 [8] SecInCoRe targets to improve resource identification and allocation procedures in preparative and responding phases of crisis management. The presented CIK Framework enables the graphical presentation and mapping of these information. Besides the kind of information, the CIK Framework is usable on various devices, using various OS, because it is running in an internet browser that is nearly available on all mobile platforms. This has been considered as an indispensable user need: enabling integration in several platforms and technologies.

9.2 Inventory

The early demonstrator provides access to a first set of datasets based on past disaster events [4]. Retrieve information from past-disaster or searching for information are initial use cases of SecInCoRe. Further past disaster information provide a excellent foundation for training purposes or research activities in the field of process optimization. Moreover, it can identified what gaps occur during the disaster, what kind of information has been missing. The validity of past disaster reports can be proven by interlinking the reports and other available information (e.g., from media). The requirement of anonymized data has to be guaranteed by the provider of the information. In addition a second test if all personal data has been anonymized have to be added. We are even aware of the risk of data aggregation to re-identify people are derive sensitive information. SecInCoRe will carry further research on this topic and will develop measures to mitigate this.

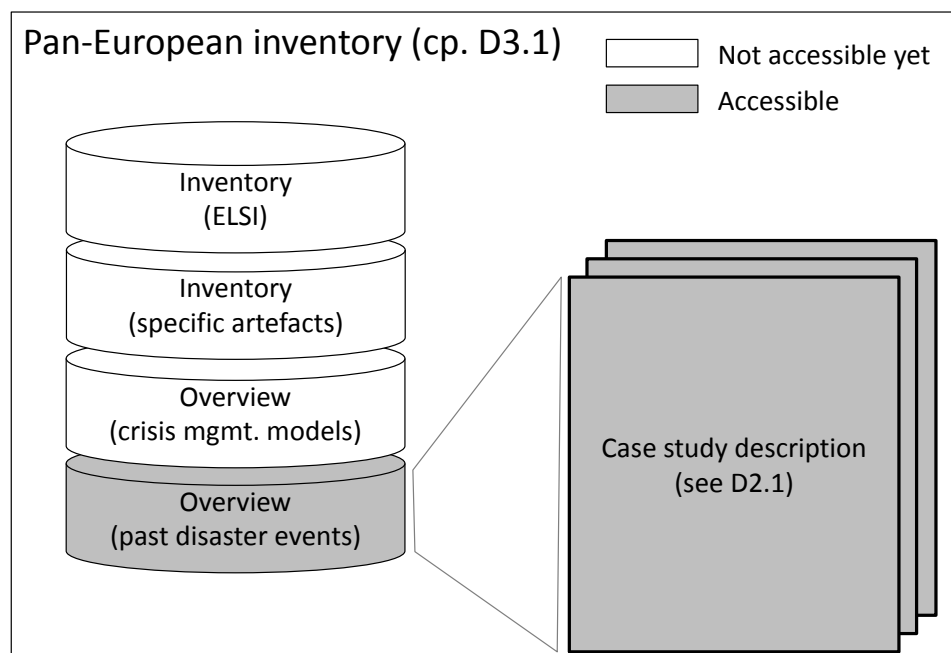


Figure 9-1 Inventory content of the early demonstrator [10]

9.3 *Process-oriented network deployment*

One of the main challenges in designing future communication technologies for crisis management is the lightweight integration of these technologies in the existing processes of rescue organisations, as these processes are well-established in practice, and they should not be hindered by the technology. Another important requirement is that future communication technologies should be as simple and as transparent as possible for end-users and it should take the specifics of the target scenario into considerations (indoor/outdoor, static/mobile, type of traffic flows, etc.).

Taking the aforementioned goals as well as further requirements elicited from the SecInCoRe project into consideration, we re-designed the intelligent hose coupling, which was initially proposed in [WSW2012]. By integrating a WLAN mesh module into the intelligent hose coupling, a fire brigade process-oriented setup of a communication network is enabled using this new solution. The communication network gets established while the fire brigades are deploying their water supplies.

The bottom of Figure 2-5 illustrates the new version of the intelligent hose coupling. In contrast to the first version (see Figure 2-5 - top), the new design incorporates an external antenna allowing for better network coverage. This also makes it more extensible, especially with respect to an energy harvesting module, which we seek to realize within SecInCore, in order to produce energy from the water flows. According to the feedback of different fire brigades after several demonstrations, the new design of the intelligent hose coupling is very simple to mount and it does not require additional resources (in the fire brigades regulations, it is stated that two personnel should be always involved to connect two fire hoses, thereby, mounting the intelligent hose coupling is straightforward). In other words, our solution is fire brigade friendly. Nevertheless, one open issue that still needs to be addressed is ruggedizing this solution.

From the software point of view, the main challenge when using the intelligent hose coupling is to have a secure and efficient auto-configuring, self-organizing, and self-healing network, as rescue personnel are not specialized in communication networks.

From the software point of view, the main challenge when using the intelligent hose coupling is to have a secure and efficient auto-configuring, self-organizing, and self-healing network, as rescue personnel are not specialized in communication networks.

Here, WLAN Mesh Networks (WMNs) are an appropriate technology. WMNs are mainly composed of legacy mobile clients (WLAN or Long Term Evolution (LTE) clients or others) and the mesh backbone. The latter is dedicated to network configuration and routing. It offers on demand network coverage to the clients, and deals with the transparent delivery of their data. The mesh backbone comprises mesh routers, mesh access points, and mesh gateways. Mesh routers are wireless relays, which run a routing protocol to dynamically set up and maintain routes in the network. Mesh access points are mesh routers that also provide network access to clients. Mesh gateways are mesh routers that connect the network to the Internet. While WMNs are a very suitable solution at the incident scene, they still suffer from security issues. We have recently shown in [SW14] that the existing mesh standard IEEE 802.11s is vulnerable against several attacks, which lead, with low effort, to a sabotage of the network. Besides, we have pointed out that the existing WMNs security proposals in the literature suffer from deployment impediments. They are



either not efficient, or they rely on non-realistic assumptions. Therefore, we have deployed on the intelligent hose coupling a novel secure and efficient routing protocol termed PASER. The protocol was initially proposed in [SPW12]. We have revised the protocol within SecInCoRe to meet the project requirements (with respect to security and performance). A comprehensive security and performance analysis of PASER has been submitted to the world class journal IEEE transactions on wireless communications. The intelligent hose coupling solution and the PASER protocol were successfully demonstrated at the SecInCoRe early-demonstrator meeting in France on 24-26 Nov. 2014.



10 Literature index

- [AAT07] Armstrong, H., Ashton, C., & Thomas, R. (2007). Data Protection and Sharing – Guidance for Emergency Planners and Responders. Office. London. Retrieved from www.cabinetoffice.gov.uk/media/132709/dataprotection.pdf
- [BB97] Bannon, L. and Bødker, S. (1997). Constructing Common Information Spaces. In ECSCW. Retrieved from <http://www.ul.ie/~idc/library/papersreports/LiamBannon/ECSCW.htm>
- [BB01] Bertelsen, O. W., & Bødker, S. (2001). Cooperation in massively distributed information spaces. In ECSCW01 Proceedings of the seventh conference on European Conference on Computer Supported Cooperative Work (pp. 1–17). Kluwer Academic Publishers. Retrieved from <http://portal.acm.org/citation.cfm?id=1241868>
- [BKA+14] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, “Survey of Wireless Communication Technologies for Public Safety,” IEEE Communications Surveys & Tutorials, vol. 16, no. 2, 2014.
- [B-W13] Barnard-Wills, D. (2013). Security, privacy and surveillance in European policy documents. International Data Privacy Law, 3(3), 170–180. doi:10.1093/idpl/ipt014
- [C01] Cavoukian, A. (2001). Taking Care of Business: Privacy by Design. Toronto. Retrieved from <http://www.ontla.on.ca/library/repository/mon/2000/10296375.pdf>
- [C12] Cavoukian, A. (2012). Privacy and Drones: Unmanned Aerial Vehicles. Retrieved from <http://www.ipc.on.ca/images/Resources/pbd-drones.pdf>
- [CH02] Cavoukian, A., & Hamilton, T. J. (2002). The Privacy Payoff: How Successful Businesses Build Customer Trust (p. 332). McGraw-Hill Ryerson. Retrieved from http://books.google.com/books?hl=en&lr=&id=cd_Bajx7xyQC&pgis=1
- [HSH+02] Heath, C., Svensson, M. S., Hindmarsh, J., Luff, P., & vom Lehn, D. (2002). Configuring Awareness. Computer Supported Cooperative Work (CSCW), 11(3), 317–347. doi:10.1023/A:1021247413718
- [G13] Grace, J. (2013). Too Well-Travelled, Not Well-Formed? The Reform of Criminality Information Sharing In the UK. The Police Journal, 86(1), 29–52. Retrieved from <http://www.vathek.org/doi/abs/10.1350/pojo.2013.86.1.607>
- [J94] Jasanoff, S. (1994). Learning from Disaster: Risk Management After Bhopal. University of Pennsylvania Press.
- [J07] Jul, S. (2007). Who’s Really on First? A Domain-Level User, Task and Context Analysis for Response Technology. Proceedings ISCRAM2007 B Van de Walle P Burghardt and C Nieuwenhuis Eds, 139–148.
- [L01] Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In Proceeding UbiComp ’01 Proceedings of the 3rd international conference on Ubiquitous Computing (pp. 273–291). Retrieved from <http://dl.acm.org/citation.cfm?id=647987.741336>
- [LMH+12] H. Lin, J. Ma, J. Hu, and K. Yang, “PA-SHWMP: A Privacy-Aware Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s Wireless Mesh Networks,” Springer



EURASIP Journal on Wireless Communications and Networking, vol. 2012, no. 1, 2012.

[NKJ08] A. Naveed, S. Kanhere, and S. Jha, "Attacks and Security Mechanisms," in Security in Wireless Mesh Networks, Y. Zhang, J. Zheng, and H. Hu, Eds. Auerbach Publications, 2008.

[RYL10] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: a Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 2, 2010.

[S13] J. Sen, "Security and Privacy Issues in Wireless Mesh Networks: A Survey," CoRR, vol. abs/1302.0939, 2013.

[SB92] Schmidt, K., & Bannon, L. (1992). Taking CSCW seriously. Computer Supported Cooperative Work, 1(1), 7–40. doi:10.1007/BF00752449

[SGB+14] M. Sbeiti, N. Goddemeier, D. Behnke and C. Wietfeld, PASER: Position-Aware, Secure, and Efficient Routing Approach for Airborne Mesh Networks, IEEE Transactions on Wireless Communications - submitted in July 2014.

[SPW12] Sbeiti, M., Pojda, J., Wietfeld, C., "Performance Evaluation of PASER - an Efficient Secure Route Discovery Approach for Wireless Mesh Networks", accepted, *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - PIMRC*, Sydney, Australia, Sep 2012.

[SVC13] A. Sgora, D. Vergados, and P. Chatzimisios, "A Survey on Security and Privacy Issues in Wireless Mesh Networks," Wiley Online Library Security and Communication Networks, 2013.

[SW14] Sbeiti, M., Wietfeld, C., "One Stone Two Birds: On the Security and Routing in Wireless Mesh Networks", accepted, *IEEE Wireless Communications and Networking Conference - WCNC*, Istanbul, Turkey, Apr 2014.

[WL06] X. Wu and N. Li, "Achieving Privacy in Mesh Networks," in ACM SASN, 2006.

[WSW12] Wolff, A., Sbeiti, M. and Wietfeld, C. (2012) Performance Evaluation of Process-Oriented Wireless Relay Deployment in Emergency Scenarios. IEEE Symposium on Computers and Communications - ISCC, Cappadocia, Turkey, July 2012.

[WXC08] T. Wu, Y. Xue, and Y. Cui, "Privacy Preservation in Wireless Mesh Networks," in Security in Wireless Mesh Networks, Y. Zhang, J. Zheng, and H. Hu, Eds. Auerbach Publications, 2008.

[ZF06] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 10, 2006.