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

Deliverable 4.2 **System Views and Concept of Operations**

Final Version

Maike Kuhnert[1], Daniel Behnke[1], Mohamad Sbeiti[1], Simona De Rosa[2], Antonella Passani[2], Steffen Schneider[3], Christoph Amelunxen[3], Jens Pottebaum[3], Christina Schäfer[3], Katrina Petersen[4], Monika Büscher[4]

[1]TU Dortmund/CNI, [2]T6 Ecosystems, [3]University of Paderborn, [4]Lancaster University

December 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	**Restricted**
Due date	30/11/2014 (due month 19)
Sent to coordinator	23/12/2015
No. of document	D4.2
Name	*System Views and Concept of Operations (CONOPS)*
Type	*Report*
Status & Version	*1.8*
No. of pages	*354*
Work package	*4*
Responsible	*TU Dortmund (CNI)*
Further contributors	*T6 Ecosystems, University of Paderborn (C.I.K.), Lancaster University (ULANC)*
Authors	*Maike Kuhnert, TUDO* *Daniel Behnke, TUDO* *Mohamad Sbeiti, TUDO* *Simona De Rosa, T6 ECO* *Antonella Passani, T6 ECO* *Steffen Schneider, UPB* *Christoph Amelunxen, UPB* *Christina Schäfer, UPB* *Jens Pottebaum, UPB* *Katrina Petersen, ULANC* *Monika Büscher, ULANC*
Keywords	*System Views, Concept of Operations (CONOPS), High Level Requirements*

History	Version	Date	Author	Comment
	V 0.1	01/04/2015	TUDO, MK	Initial version
	V 0.2	20/05/2015	TUDO, MK	Input from UPB, T6, TUDO
	V 0.3	23/05/2015	ULANC	Monitoring review
	V 0.4	24/05/2015	UPB	UPB review
	V0.5	19/10/2015	TUDO	Update incl Athens, Rome outcomes and review comments
	V0.6	29/10/2015	TUDO	Update on chapter 2 and 3
	V0.7	03/11/2015	TUDO	Update on chapter 4: HLRD, chapter 5: ConOps, include Annex A
	V1.0	09/11/2015	TUDO	General summary, Chapter one, Comments by UPB
	V1.1	25/11/2015	TUDO	Update based on QA Review, Monitoring Review, Added Requirement Process
	V1.2	4/12/2015	TUDO	Update based on Plenary Meeting Outcomes, Clarification of WP4/WP5 link/focus
	V1.3	07/12/2015	TUDO	Update chapter 2 structure
	V1.4	09/12/2015	TUDO	Update ConOps, HLR
	V1.5	16/12/2015	TUDO, UPB	Update CIS
	V1.6	17/12/2015	TUDO, UPB	Update CIS, HLRD
	V1.7	23/12/2015	TUDO, UPB, T6	Final changes
	V1.8	24/12/2015	UPB	Finalisation for submission

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

Authors

TU Dortmund

CNI

Maike Kuhnert

Email: maike.kuhnert@tu-dortmund.de

Daniel Behnke

Email: Daniel.behnke@tu-dortmund.de

Mohamad Sbeiti

Email: Mohamad.sbeiti@tu-dortmund.de

T6 Ecosystems

Simona De Rosa

Email: s.derosa@t-6.it

Antonella Passani

Email: a.passani@t-6.it

University of Paderborn

C.I.K.

Jens Pottebaum

Email: pottebaum@cik.upb.de

Steffen Schneider

Email: st.schneider@cik.upb.de

Christoph Amelunxen

Email: amelunxen@cik.upb.de

Christina Schäfer

Email: c.schaefer@cik.upb.de

Mobilities.Lab

Centre for Mobilities Research

Department of Sociology

Lancaster University

LA1 4YD, UK

Katrina Petersen

Email:

k.petersen@lancaster.ac.uk

Monika Büscher

Email:

mbuscher@lancaster.ac.uk

Reviewers

Mobilities.Lab

Centre for Mobilities Research

Department of Sociology

Lancaster University

LA1 4YD, UK

Monika Büscher
Email:
mbuscher@lancaster.ac.uk

Center for Security Studies

(KEMEA)

P.Kanellopoulou 4

1101 77 Athens

Greece

Giorgos Leventakis
Email: gleventakis@kemea.gr

Executive summary

The deliverable scopes out system views, high level requirements and concept of operations of SecInCoRe. The objective of this deliverable is to present a clear definition of different perspectives of usage (system views), how SecInCoRe can be used (ConOps) and what requirements have to be considered during the concept design process (high level requirements). All parts are relying on existing background knowledge and experiences in the consortium and are supplemented with results from a broad-based co-design process with stakeholders, including the SecInCoRe advisory board. The initiative SecInCoRe common information space overview is linked to WP2, WP3 and WP5. Further, the deliverable emphasizes the interdisciplinary nature of SecInCoRe research and the relationship between visionary concept and demonstrator implementation. The collaborative work on requirement management leads to flexible high level requirements relying on the evolution and new findings in this application domain. In the end, the document describes how the common information space is used in different scenarios.

All in all this report is divided into 5 chapters and an annex:

- 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.
- The common information space enabled by SecInCoRe is presented briefly in chapter **two**. Understanding the common information space is indispensable for the further understanding of the document. Enabling a common information space based on the pan European disaster inventory running in the cloud based emergency information system (CEIS) is one of the core objectives of SecInCoRe. Technology here comes together not as a complete, stand-alone technical system, it is a system in the sense of a dynamic socio-technical collection of tools and practices that each support collaboration and interoperability in a specific way. When, in the following, we refer to ‘the system’ or the ‘SecInCoRe system’, we refer to this dynamic assemblage of technologies, information sources and social practices. In contrast to other deliverables the main focus lies on the description of benefits, system boundaries and interfaces. At the end, the reader should have a clear understanding of what SecInCoRe will offer and what not. The outcomes in this chapter are derived from collaborative work in T4.2 and T4.3 and based on work package overlapping privacy and ethical impact assessments and co-design workshops.

- SecInCoRe systems views are described in chapter **three**. This chapter presents first operative, technological and regulatory views on SecInCoRe. Besides, using SecInCoRe in the response phase, the concept is adapted to be valuable in all phases of crisis management (e.g., pre-, post-, past-disaster). This differentiation enables various perspectives and it is summarized in a generic use case model. SecInCoRe validation is focussing on the planning phase in crisis management, where the information need and the need of collaboration and interoperability is enhanced when having pan-European crisis management in mind.
- Chapter **four** addresses the high level requirements. In SecInCoRe the requirement management is handled with the support of JIRA, every partner has access to. Based on D4.1 the requirements have been updated, especially with regard to ethical legal and social issues, empirical research and the outcomes of co-design workshops. This chapter presents the lists that are available in JIRA. In the corresponding chapter in the appendix the requirements are listed with more detail. In contrast to traditional system development processes the requirements should be dynamic to enable adaptation when new issues arises. Further, we use the term high level requirements to emphasize that the collection is not designed for software development only. There are related terms, like architectural qualities but these are more commonly used in the field of information technology.

  In addition to high-level requirements, the chapter is complemented by a description of the process SecInCoRe uses to define technical requirements in relation to high-level requirements. This includes also the definition of performance criteria for each requirement.
- Concept of Operations (ConOps) and a methodical approach of developing ConOps are presented in chapter **five**. The development of ConOps is needed to deepen end user interaction and concept specification. Using ConOps enables a “hands-on” presentation and discussion of SecInCoRe. Further ConOps are valuable for concrete specification of the demonstrator and, later on, validation of SecInCoRe concepts. In addition, the above presented system views are directly related to the ConOps development. This chapter ends with two concrete examples using the common information space in crisis management.

This document builds on D4.1 and presents adapted requirements and gives a clear definition of the common information space in crisis management SecInCoRe is aiming to. In the further work in WP4 specific technical solutions for supporting this concept are investigated (T4.5, T4.6) and a more technical system architecture is derived in T4.4.