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

Deliverable 6.3 **Report and Evaluation on new business models**

Final version

Andrea Nicolai[1], Simona De Rosa[1]

[1]T6 Ecosystems

April, 2017

Work Package 6

Project Coordinator

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

7th Framework Programme

for Research and Technological Development

COOPERATION

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

Distribution level	**Public**
Due date	30 April 2017
Sent to coordinator	27 April 2017
No. of document	D6.3
Name	*Report and Evaluation on new business models*
Type	*Report*
Status & Version	*Final Version*
No. of pages	*56*
Work package	*6*
Responsible	*T6 ECO*
Further contributors	*UPB* *TUDO* *ULANC* *CS* *ADS* *BAPCO* *KEMEA*
Keywords	*Business Models, Sustainability, Exploitation*

History	Version	Date	Author	Comment
	V0.1	23.01.2017	Simona De Rosa	ToC sent to the partners
	V0.2	14.03.2017	Peter Gray	Received contribution from CS
	V1	04.04.2017	Simona De Rosa	Sent to internal review
	V2	21.04.2017	Simona De Rosa	Sent to the coordinator for the final 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

T6 Ecosystems

Andrea Nicolai
Email : a.nicolai@t-6.it
Simona De Rosa
Email: s.derosa@t-6.it

Reviewers

CloudSigma

Peter Gray
Email: peter.gray@cloudsigma.com

TU Dortmund
CNI

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

ELSI Monitor

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

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

Executive summary

SecInCoRe is a cross-cutting activity in the 'Security' theme of the 7th research framework programme of the European Commission. Therefore, it envisages to close gaps identified by earlier or parallel projects and to address issues across all 'missions' of the security research programme. The project dedicates specific attention to research regarding the knowledge creation and dissemination, exploitation and standardisation of the SecInCoRe outcomes. These are important aspects for ensuring the project's progress beyond the state-of-the art and for sustainability after the completion of the project.

In order to support these objectives, this document describes the work performed on Business Model analysis deriving main conclusions for the project's sustainability and exploitation.

Deliverable 6.3 - Report and Evaluation on new Business Models - presents an analysis of traditional and innovative business models in order to shape a sustainability strategy after the end of the project.

Following the work of analysis and investigation of multiple sources, three strategies have been identified to sustain SecInCoRe after the end of the project. They are reported in this deliverable.

In addition to the approaches identified to support a project's sustainability, the last section of the deliverable is dedicated to individual exploitation plans for the SecInCoRe partners. Indeed, partners have different interests in SecInCoRe results and due to their organizational nature their business goals are completely different as well as the benefits they expect from the project. We have classified the exploitation plans according to different organisational structure, results are now publically available and reported in this deliverable to complete the broad overview of the SecInCoRe sustainability and exploitation.

Table of contents

1 Introduction 5

Purpose of this document 5

1.1 Validity of this document 5

1.2 Relation to other documents 6

1.3 Contribution of this document 6

1.4 Target audience 6

1.5 Glossary 6

1.6 List of figures 8

1.7 List of tables 9

2 SecInCoRe's business models strategy at a glance 10

2.1 Potential outcomes for future sustainability 10

2.2 Results from the Business models analysis performed with the project 11

2.3 Gathering inputs and insights from similar experiences 13

2.3.1 Resilience Direct 13

2.3.2 Open Geospatial Consortium 15

2.3.3 Everbridge 16

3 Prospective business and future market report 17

3.1 A comprehensive strategy for the CIS's sustainability 18

3.2 A modular strategy for the SecInCoRe components 20

3.2.1 ELSI Guidance for the design and use of a CIS for crisis management and response 21

3.2.2 Pan-European Inventory 22

3.2.3 Cloud based services 23

3.3 Commercial impact in the domain of PPDR 27

3.4 Interoperability and cross border communications 28

3.4.1 Markets and Services 28

3.4.2 SecInCoRe and 3GPP Context 28

3.4.3 Airbus position as part of SecInCore 28

3.5 RescueRoam from the idea to the commercial impact 29

3.5.1 RescueRoam: commercial aspects and new services 30

4 New business models for SecInCoRe 32

4.1 Innovation procurement through an overview of policy implementation 32

4.1.1 Pre-commercial procurement (PCP) 33

4.1.2 Pre commercial procurement procedures for SecInCoRe 33
4.2 Final reflection on new business models 35
5 Final exploitation Strategy for SecInCoRe Partners 36
5.1 Research partners 37
5.1.1 University of Paderborn (UPB) 37
5.1.2 Technical University Dortmund (TUDO) 38
5.1.3 Lancaster University (ULANC) 39
5.2 Industrial partners 41
5.2.1 CloudSigma (CS) 41
5.2.2 Airbus Defence and Space (ADS) 45
5.2.3 T6 Ecosystems (T6ECO) 46
5.3 Stakeholder organisations 47
5.3.1 British Apco (BAPCO) 47
5.3.2 Center for Security Studies (KEMEA) 48
5.4 Final remarks from the exploitation plans 50
6 Conclusions 51
Literature index 52

1 Introduction

Analysis and exploration of new business models is one of the aims of SecInCoRe. The aim has been pursued through several activities that have been implemented since the first stage of the project until its conclusion. The goal within this task has been twofold: first to find a suitable sustainability strategy for SecInCoRe and its components; second, to define a way to exploit results after the end of the project lifetime.

Sustainability and exploitation, indeed, have been at the core of the reflections of WP6 in order to provide a medium and long-term strategy together with an overview of the main challenges and opportunities.

In line with this, a framework to derive potential business models and to define a sustainability plan for SecInCoRe's outcomes has been developed in the previous deliverables dedicated to the topic (D6.1 and D6.2). This deliverable describes the final results achieved within WP6 for the aspects related to business models and sustainability.

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

- Chapter 1 presents a short summary of the strategy used for the analysis of business models and results. Starting from the plan produced at the beginning of the project, the main outcomes from investigating existing business models adopted by similar information systems are described in order to shape the model adopted by SecInCoRe.
- Based on what was discussed and analysed in the first chapter, Chapter 2 provides two different approaches for building a sustainability strategy for SecInCoRe. The first approach is based on a comprehensive strategy to sustain SecInCoRe's Common Information Space (CIS) as a unique outcome. The second strategy is based on a modular approach in which different components developed during the project can be sustained individually. Both approaches have been discussed during the project development with the stakeholders in order to evaluate them.
- Chapter 3 provides the investigation of an innovative business model, which is the procurement of innovation, and its relation with SecInCoRe.
- Chapter 4 reports the exploitation plans provided by each partner according to their interests and business. The aim of the chapter is to show that all project results will be exploited by the partners individually, increasing, or even improving, their current business.
- Chapter 5 closes the work of WP6 summarizing what has been presented before and producing final statements about the SecInCoRe sustainability and exploitation strategy.

Purpose of this document

The main purpose of this document is to describe the SecInCoRe activities on the analysis of business models making clear how the investigation performed during the project life time has produced input on the strategies for SecInCoRe's sustainability and exploitation.

1.1 Validity of this document

This document depicts the status of the work done by the SecInCoRe team related to business models for the different concepts of the project.

1.2 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)
[4] D6.1 Standardisation strategy including identification of relevant standardisation bodies
[5] D6.2 Status Report on Standardisation

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

[6] D6.4 Standardisation, Exploitation and Dissemination Report

1.3 Contribution of this document

SecInCoRe is a cross-cutting activity in the 'Security' theme of the 7th research framework programme of the European Commission. Therefore, it envisages to close gaps identified by earlier or in parallel projects and to address issues across all 'missions' of the security research programme. The project dedicates specific attention to research regarding the knowledge creation and dissemination, exploitation and standardisation of the SecInCoRe outcomes. These are important aspects for ensuring the project's progress beyond the state-of-the art and for sustainability after the completion of the project. In order to support these objectives, this document describes the status on standardisation activities.

1.4 Target audience

D6.3 is public and its main target audience are all stakeholders in the field that could be interested in understanding how project results will be sustained after the end of the project. One target audience in particular is the European Commission which may be interested in understanding how the SecInCoRe project intends to support a long term use of the project results.

1.5 Glossary

Abbreviation	Expression
AB	Advisory Board
API	Application Programming Interface
AWS	Amazon Machine Images
BB	Broadband
C.I.K	Central Index Key
CEIS	Cloud Emergency Information System

Abbreviation	Expression
CEN	European Committee for Standardization
CESG	Communications-Electronics Security Group
CIS	Common Information Space
CNI	Communication Networks Institute
CPU	Central Processing Unit
CS	Computer Science
DG ECHO	Directorate General Civil Protection & Humanitarian Aid Operations
DOW	Description of Work
EC	European Commission
ELSI	Ethical, Legal and Social Issues
ERAB	European Research Area Board
ERCC	Emergency Response Communications Centre
EU	European Union
FEU	Federation of European Fire-Fighters
FTE	Full Time Equivalent
GNU	General Public License
GW	Gateway
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IdP	Identity Provider
ISCRAM	International Crisis Response and Management
JRC	Joint Research Centre
KVM	Keyboard - Video - Mouse
MCS	Mission Critical Service
NB	Narrow Band

Abbreviation	Expression
NEC	Network Enabled Communication
NGO	Non-Governmental Organization
OA	Open Atrium
OGC	Open Geospatial Consortium
OSF	Operational Support Facility
PCP	Pre-Commercial-Procurement
PMR	Private Mobile Radio
PPDR	Public Protection and Disaster Relief
PPI	Procurement of Innovative Solutions
PSCE	Public Safety Communications Europe
RAM	Random-Access Memory
RFI	Request For Information
RFP	Request For Proposal
SaaS	Software as a Service
SME	Small Medium Entreprise
SP	Service Provider
TER-CDM	Terminologies in crisis and disaster management'
US	United States
VM	Virtual Machine
WLAN	Wireless Local Area Network
WS	Web Server
Y	Year

1.6 List of figures

Figure 1 Action plan for analysis of the business models conducted during the project life-time 10
Figure 2. Outcomes relevant for the sustainability of SecInCoRe..... 11

Figure 3. Categories for business models in crisis management 12
Figure 4. Business models potentially applicable to SecinCoRe 13
Figure 5. Business models categories and information systems investigated 13
Figure 6. The two strategies for project's sustainability 17
Figure 7. The SecInCoRe's components for a modular sustainability 21
Figure 8. Open Atrium drive image. 24
Figure 9. Mock-up for commercial exploitation 25
Figure 10. SecInCoRe CIS-as-a-Service value-chain 26
Figure 11 Authentication process in RescueRoam 30

1.7 List of tables

Table 1. Infrastructure costs provided by CS 20
Table 2. Infrastructure costs provided by CS 27
Table 3. List of exploitation plans produced by the SecInCoRe partners 36

2 SecInCoRe's business models strategy at a glance

SecInCoRe has performed a business model analysis since the beginning of the project in order to understand which model could be developed to support the sustainability of project results.

The analysis has been conducted according to a framework, which followed the stages of the project development. The aim of the designed framework was to cover a wide range of sources to investigate the most appropriate way to address business models for the project. The framework has been described in D6.1 and it was based on different levels of investigation, from desk analysis to interviews with stakeholders and the analysis of innovative business models in relation to the project's outcomes (Figure 1) and its discussion with stakeholders.

According to the plan provided in D6.1, the first actions performed at the beginning of the process were related to literature review and desk analysis of public procurement models, in house doctrine, public private procurement and new business models in Public Procurement. Indeed, in order to define the process in which information systems are generally acquired by National Authorities, public procurement models at national levels were identified as crucial issues.

Figure 1 Action plan for analysis of the business models conducted during the project life-time

Then, in addition to the literature review, several analyses have been performed, following the development of the project and studying existing solutions in more depth..

In order to specify suitable business models, it was essential to define, together with all partners, which components should be taken into account to build a business model strategy (results are reported in D6.2). In addition, discussions on business models have been conducted with stakeholders, namely experts of the SecInCoRe Advisory Board, to understand which business model they consider as the most adequate for the project's outcomes according to their experience and knowledge.

On this basis, the analysis of best practices and the analysis of systems that can be defined as similar to SecInCoRe (results are reported in D3.4) have been performed to understand the state of the art and the most common business models used and applied in the field of innovative solutions in crisis management.

Through literature review and the analysis of existing business models, also comparing the SecInCoRe system to existing concepts and technologies, it has been possible to derive some conclusions on the potential strategies for SecInCoRe. Results are reported in the following paragraphs.

2.1 Potential outcomes for future sustainability

During the project lifetime SecInCoRe has developed the conceptual design of a Common Information Space (CIS) in order to foster cooperation and collaboration among practitioners engaged in crisis management, in particular in the preparedness and training phase. The aim of the project has been the production of a new way to address emergencies and preparatory phases

in order to address several and crucial issues that practitioners face during their work routine. In this sense, from a comprehensive perspective, the main project outcome is:

- the conceptual design of the CIS

However, the consortium has designed the CIS based on several components (Figure 2). Looking at the single components it is possible to state that additional project outcomes are:

- the Semantic framework;
- the Taxonomy;
- the Pan European Inventory;
- the ELSI guidance;
- the Network Enabled Communication.

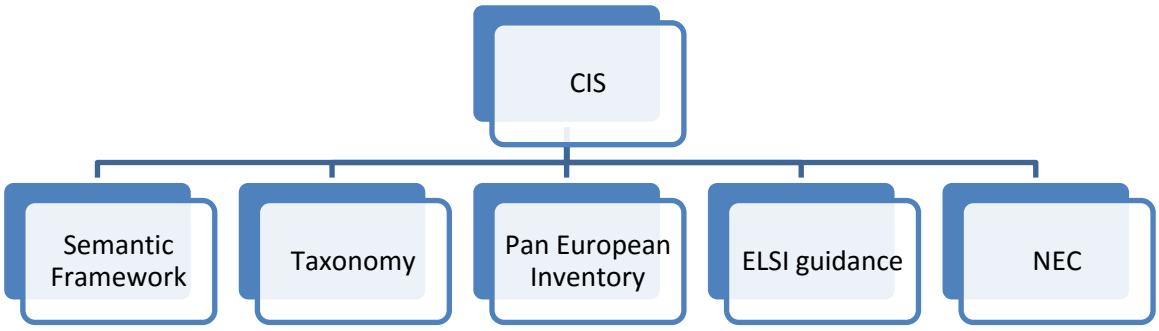

Figure 2. Outcomes relevant for the sustainability of SecInCoRe

Due to their conceptual nature not all the outcomes can be considered as possible results on which to build a potential business model. In line with this, the definition of components to sustain has been conducted in parallel to the analysis of existing business models. This analysis is reported in the following paragraph.

2.2 Results from the Business models analysis performed with the project

The investigation of business models has been performed taking into account the analysis developed within WP3. This analysis, aimed at building an Inventory on business models, has identified systems that are relevant for SecInCoRe in regard to the contents or functioning and stressing the kind of business model used. It has been possible to categorize the various business models according to four main categories. The four categories are (Figure 3):

- public funded Pan-EU model;
- vertical model, that can be public or private, focused on specific emergency or related topics;
- not-for profit model, building a volunteer community, that could be a new community or integrating outcomes into an existing one;
- commercial model mainly based on private companies.

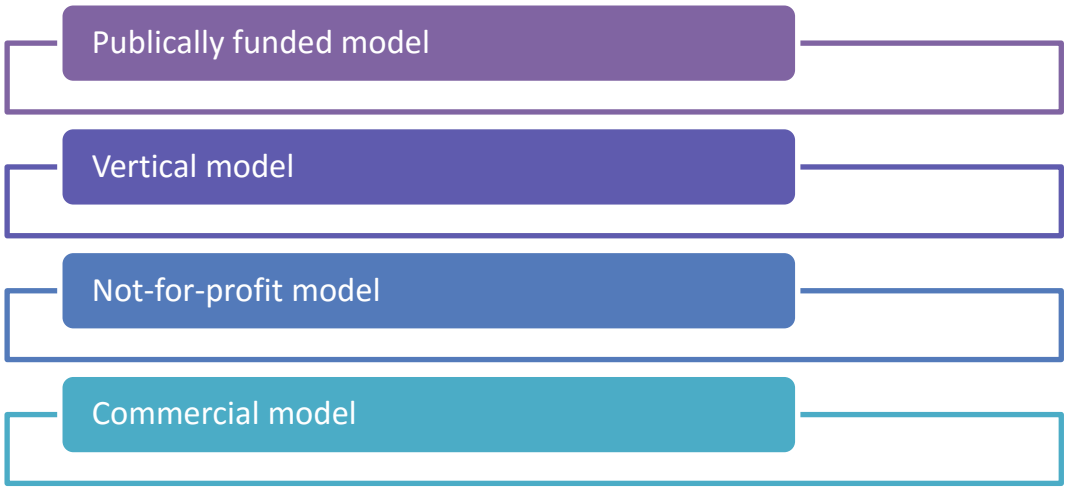

Figure 3. Categories for business models in crisis management

The four categories have been discussed and evaluated by the SecInCoRe Advisory Board members. The AB confirmed that talking about crisis management tools; these are the most relevant models to apply and to take into consideration.

Starting from the analysis conducted in WP3 and matching the results with the input from the Advisory Board, it has been possible to analyse which model(s) could best fit the purpose of SecInCore. In this process, it was possible to discard the option based on a not-for-profit model as well as the one related to the vertical model (Figure 4).

The not-for-profit model indeed is not applicable to SecInCoRe due to the fact that information that should be stored in the CIS and shared by users is in almost all cases information that cannot be accessible to anyone. In this sense, practitioners and first responders would not trust a system based on a not-for-profit organisation where any user could have free access to it and where there are no strict regulations implemented for the use of the CIS.
In addition, the option based on the vertical model has been discarded due to the fact that SecInCoRe expects to be a transversal source of information. SecInCoRe, indeed, even if it intends to cover the planning and preparation phase of the emergency, is not based on a selected topic. In this sense, it is not possible to build a vertical model based on selected sources because the aim is to let the users decide which is the scope of the CIS.

In this sense, the approach to follow in terms of business models was restricted to two models: the publically funded model and the commercial model. A thorough analysis of both models was performed with the aim to get a complete overview on how to build a sustainability strategy.

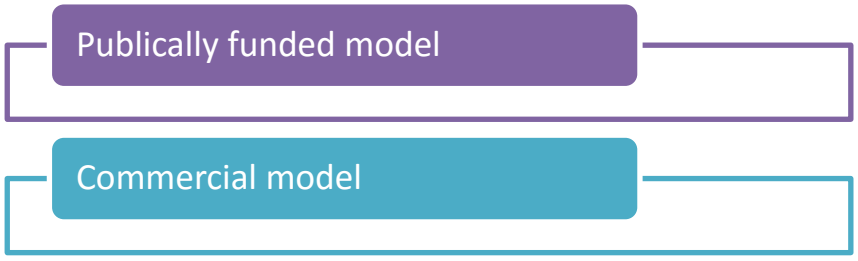

Figure 4. Business models potentially applicable to SecinCoRe

2.3 Gathering inputs and insights from similar experiences.

In order to create a sustainability strategy for SecInCoRe deeper discussions have been conducted with representatives of industry and organizations engaged in the sector. The aim was to gather data for the creation of the sustainability strategy starting from the experience of other actors on the feasibility of:

- a publically funded model;
- a commercial model.

In addition, it was also interesting for the project to understand in depth the functioning of a public-private consortium based on a strong stakeholder engagement, one of the issues also faced by SecInCoRe.

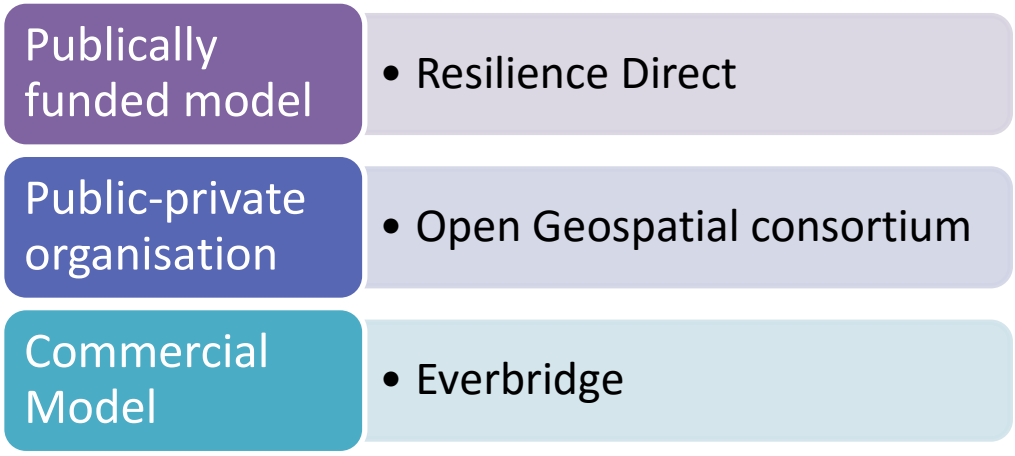

Figure 5. Business models categories and information systems investigated

In line with this, it has been possible to discuss SecInCoRe with representatives from the Resilience Direct and Open Geospatial Consortium, to collect their experience and their feedback. To complete the analysis with insights about a real commercial model solution a desk analysis has been performed. Results (Figure 5) are presented in the next paragraph.

2.3.1 Resilience Direct

Resilience Direct[1] has been one of the information systems that SecInCoRe had the chance to explore during the project life time, thanks to the direct involvement of users from Lancashire Resilience Forum in the project that were well aware of the platform. In line with this, Resilience Direct was approached by SecInCoRe as a potential source of inspiration for the future SecInCore development, as it is an example of a publically funded platform just for practitioners.

Resilience Direct, indeed, is a platform publically funded by the UK government through the Cabinet Office and supported by Ordnance Survey, a UK government agency responsible for the official, definitive topographic survey and mapping of Great Britain. As reported on the web site

[1] Available at https://www.gov.uk/guidance/resilient-communications#resiliencedirect

"ResilienceDirect is an online private 'network' which enables civil protection practitioners to work together – across geographical and organisational boundaries – during the preparation, response and recovery phases of an event or emergency. The UK Civil Contingencies Act 2004 requires that emergency responders co-operate and share information in order to efficiently and effectively prepare for, and respond to, emergencies and ensure that action is coordinated. ResilienceDirect helps organisations to fulfil these duties by supporting the adoption of common working practices, and ensuring that key information is readily and consistently available to users. ResilienceDirect helps to facilitate multi-agency collaboration in many ways"[2].

The platform can support several activities; among others, it can help practitioners in sharing plans among different agencies, maintaining awareness of forthcoming exercises and events, sharing situation reports and briefings between local responders and many other tasks. The platform is a web-based service. The platform is secure and it is accredited to hold electronic documents with a protective marking of restricted guaranteed by the Security Policy Framework.

Regarding the kind of user that can access the platform, Category 1 and 2 Responders (as defined by the Civil Contingencies Act 2004), government departments and agencies, and other key organisations in the UK resilience community can be accepted by the system, following a well-established procedure for registration. Indeed, "prospective users should contact the ResilienceDirect team. Before accessing ResilienceDirect, organisations are required to sign a Connection Agreement to ensure the continued integrity of the service[3]".

In line with all publically available information, it was possible to discuss the kind of approach pursued by Resilience Direct with a representative of the system during the ELSI workshop organised in Brussels by SecInCoRe on January 26, 2017. On that occasion, the functioning of the system was investigated in order to map positive and negative effects that could influence the sustainability strategy of SecInCoRe.

From the conversation with the person from Resilience Direct it was possible to deduce the positive effects produced by the system. First of all, a good clarification of management issues emerged. The system functioning, indeed, is based on a single authority, which is the Cabinet Office. This means that the Cabinet Office is the only institution that has the right of maintenance, right of development and the right of access to the platform. In line with this, the Cabinet Office is in charge of the acceptance of the organisation that can access the platform. Once an organisation is accepted, a local office provides the right of access to the people within the accepted organisation that can work with the system. This procedure helps a lot in defining the rules and terms of conditions to use the system, establishing from a top down perspective how it works. This approach also solves engagement issues. Indeed, because the platform is strongly supported by one of the most relevant national authorities, practitioners are pushed to apply for getting access and use the system as a tool for sharing information and communicating with other organisations. This allows solving an important issue related to the different layers of communication and several tools that used within organisations. Finally, the UK government's National Technical Authority for Information Assurance (CESG) has accredited

[2] Available at https://www.gov.uk/guidance/resilient-communications
[3] Available at https://www.gov.uk/guidance/resilient-communications

ResilienceDirect to Official Security. This also solves trust issues on the technology used by the practitioners.

On the other hand, the negative issue that was stressed by the person interviewed is related to the fact that the platform depends on public money. This means that the capability to sustain the platform is strongly related to the financial availability and political willingness at national level. Even if the community of users is solid and needs the platform for their daily work, users do not have the financial capability to sustain it. This issue opens to the possibility that the platform could be closed if financial availability or political will support it declines.

2.3.2 Open Geospatial Consortium

One of the crucial points that emerged in the analysis of information systems for crisis management was the need to have a strong community of stakeholders using a platform, allowing it to improve and grow in terms of contents, functionalities and in the capability to impact on existing processes. This aspect emerged clearly during a discussion opened with a representative of Open Geospatial Consortium at the ELSI workshop organised by SecInCoRe,

In line with this, the Open Geospatial Consortium (OGC) was chosen for a detailed analysis. OGC is "an international not-for-profit organization committed to making quality open standards for the global geospatial community. These standards are made through a consensus process and are freely available for anyone to use to improve sharing of the world's geospatial data. OGC standards are used in a wide variety of domains including Environment, Defence, Health, Agriculture, Meteorology, Sustainable Development and many more[4]".

The main potentiality of the platform is to have members from government, commercial organizations, NGOs, academic and research organizations. This allows a broad coverage of standard issues from different perspectives. Among the many principles listed by a representative of OGC, it is particularly important to mention:

- Abstract tools from data – use the same source of data for multiple purposes;
- Ensure authoritative data sources to maintain authority over their information;
- Facilitate an ecosystem of tools;
- Facilitate access to federated data sources;
- Record the provenance of data;
- Preserve an audit trail of information used for decision making in order to improve future incident handling and to respond to legal challenges;
- Capture scenarios that can be replayed for training purposes.

The example provided by OGC is interesting from a SecInCoRe perspective because it is based more on a service provision rather than being product based.

However, even if the OGC can show a great community of different stakeholders engaged at different levels in standardisation processes, some major issues in relation to funding the platform still remain and they are to be faced by the managing authority. More precisely, the chance to be funded by private capital does not solve the issue of sustainability, above all because the platform provides access to open data and the question is for how long people will pay to have access to it.

[4] Available at http://www.opengeospatial.org/

2.3.3 Everbridge

As already mentioned, one of the alternatives for SecInCoRe could be to follow a commercial model, making the different outcomes available as commercial products and setting the CIS according to the specific needs of the customer.

In order to gather some data on this kind of approach, it has been possible to investigate through a desk analysis the solutions provided by a commercial company, Everbridge, in order to collect some input and to understand challenges and opportunities.

Everbridge is a company that, since 2002, began to provide software applications to improve organizational response for critical events to keep people safe and businesses running. The company is based in the United States, Finland and UK. The technology used is based on a "Software as a Service critical communications platform built on a secure, scalable and reliable infrastructure with multiple layers of redundancy to enable the rapid delivery of critical communications, with near real-time verification, over numerous devices and contact paths[5]". Then the platform provides different features aimed at:

- Improving collaborations;
- Reporting and analytics;
- Fostering Communication;
- Providing a Secure infrastructure;
- Mapping data.

The business strategy is to customise the SaaS according to the need of the customers. This means that products can be purchased in a modular way and adapted according to the needs of the customers.
As it is possible to see from the company's website, among the customers there are a wide range of stakeholders, from private to public actors. Indeed, among the over 3,200 Global Customers, there are:

- Nine of the ten largest U.S. investment banks;
- Eight of the ten largest U.S. cities;
- Four of the 10 largest U.S.-based healthcare providers.

The company's strategy is purely commercial and it is based on the fact that even public institutions (above all in the United States) can easily purchase solutions and products for crisis management. This strategy however needs to be carefully analysed when facing European rules due to the fact that national authorities need to apply public procurement procedures in order to buy commercial systems (as mentioned in D6.1).
Finally, such a commercial strategy foresees a high level of product and technology development which are out of the scope of the SecInCoRe project. In this sense some element can be retrieved but the commercial model cannot be entirely applied to the sustainability strategy.

[5] Available at https://www.everbridge.com/

3 Prospective business and future market report

It is fair to say that the main result of SecInCoRe is represented by the design of a Common Information Space (CIS) for crisis management. However, it has to be taken into account that the CIS concept is itself based on several conceptual components as shown in Figure 2 in Chapter 2.

Building on the results of the previous analyses as well as from the feedback of the stakeholders, a sustainability strategy for SecInCoRe could be established from a double perspective. From one side, discussing business opportunities for the CIS as a unique and comprehensive outcome; from the other side, considering each single outcome and build a sustainability strategy for each of them (Figure 6).

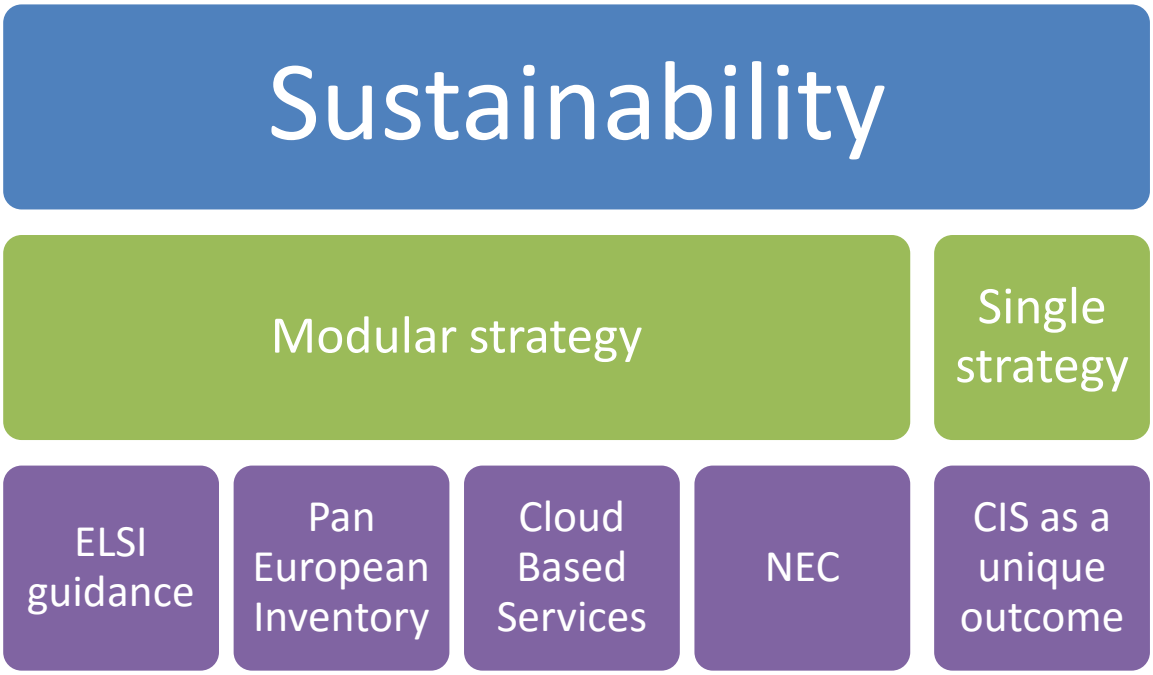

Figure 6. The two strategies for project's sustainability

Both strategies have been investigated and results are described in the following and referring them to the main comments received by the stakeholders engaged in the project in order to provide also a reflective approach.

However, it has to be pointed out that it was extremely difficult to envisage a business model for SecInCoRe adopting traditional tools, such as the application of the business model canvas[6]. The challenge to create a real business model is twofold. From one side, the research project was aimed at creating a concept, and not a fully functioning system. On the other side, following the way in which it has been designed, the CIS is intended to be a tool for emergency services. This means in most of the cases that a commercial strategy is not the best model to apply because procurement procedures are the ones to follow to implement a system in the current routines of emergency services in Europe (as reported in D6.1).

In line with this, rather than stressing the value of a business model from an economic and commercial perspective, the next paragraphs will be more related to the exploitation and future

[6] Osterwalder, A., & Pigneur, Y. (2010). Business Model Generation: A Handbook For Visionaries, Game Changers, And Challengers . Wiley.

sustainability of the projects' outcomes, taking into account similar experiences, suggestions from stakeholders and reflections on SecInCoRes' components and functionalities.

3.1 A comprehensive strategy for the CIS's sustainability

According to the feedback gathered from the stakeholder experts in the sector in different meetings organised by SecInCoRe (AB meetings, ELSI workshop, Joint Event and all other validation activities) it emerged that a good option for the project sustainability could be to set up a platform based on the SecInCoRe outcomes where practitioners could learn how to create a CIS, create it and use it for preparedness and training phases of an emergency.

It clearly emerged from the investigation that practitioners need to implement more homogeneous tools in current practices in order to harmonise procedures among European countries and to use them in strong collaboration with other organisations going beyond personal contacts and small national networks.
In this sense, the SecInCoRe platform could address the collaboration among different organisations through the adoption of similar tools and sources of information and supporting collaborative practices and information exchange above all during the preparedness and training phase of the emergency.

A way in which the platform could be envisaged is the following:

- The platform could contain all design information to set up a CIS and also a living demonstrator, as the one implemented during the project life time, in order to show all components and functionalities that could be used to set up a CIS properly;
- The information accessible through the search function could be the one inserted in the knowledge base during the project life time and then incremented by the future manager of the platform and by whom uses it according to their scopes and purposes. In this way, the platform would be a living system, growing according to the usage. The network enabled communication could sustain the connection in a secure and trustable way;
- At the top of the structure, the link with the ELSI platform and the integration of support for ELSI reflexivity designed into the SecInCoRe CIS concept could be a way to address ethical, legal and social issues pro-actively when developing a CIS, and enhance the capability of leveraging technology and social practices for good disaster risk management.

In this sense, the platform could be a way to increase awareness about the most relevant topics related to crisis management but also a tool to increase collaboration practices in the emergency world for preparedness and training phases.

Certainly, this is just a proposal for a potential SecInCoRe platform implementation. The platform could also be developed in a different way. However, some major issues that should be taken into account in any case for the sustainability are described in the following.

The first issue that should be solved is the identification of the subject that would sustain the platform.
What emerged so far is that a European institution should publically sustain the development of the platform. What emerged, is that such a platform could be sustainable in a long-term perspective only with a strong public support at European level. In this sense, some institutions have been identified that could take care of the platform as the managing authority; these are

ERCC, the DRMKC, JRC and DG ECHO. These are strong and well established European institutions, which could ensure a proper use of the platform, setting the rules and rights of access and regulations. In addition, this could also be the best way to foster organisations at national levels to use it. The model that could be applied is the model of regulation adopted by Resilience Direct. A top managing authority, in this case at European level, that provides access to the organisations that makes a request.

In this way, the platform could also be certificated as a secure technology (as in the case of Resilience Direct), solving also trust issues that emerge when using a technology to exchange also potentially sensitive data.

Furthermore, the managing authority should also regulate the data sources contribution and regulate responsibility for data quality and data protection within the system.

A second issue that should be taken into account is related to the fact that the majority of current models of exploitation are related to customised solutions. In this sense, the platform should also be realised with the possibility that the single components can be implemented in a modular way, according to the kind of CIS that the users want to set up. In this way, following the customised approach proposed by commercial companies (e.g. Everbridge), it would be possible to customise the CIS according to the users' purposes.

Finally, it also has to be taken into account that a critical mass of information should be based on a solid community of users to sustain and contribute to the inventory. In order to encourage the building of a community of practitioners, examples such as the OGC could be a source of inspiration. Practitioners from different organisations at national and regional level should be first users of the system under the umbrella of the European institution.

To conclude, the way in which the CIS can be sustained and taking into consideration all components does not seem adequate to define real business models. If a platform had to be sustained financially through the direct payment of the users it would be difficult to promote it among a wide range of national and European organisations engaged in emergency services. For this reason, the suitable way to sustain the platform would be if it could be sustained by a European institution.

On the other hand the motivation for a public EU body and for national governments to fund a system like SecInCoRe as a public service is related to the need improve systems adopted for crisis management.

Since the 1992 Earth Summit, 4.4 billion people or 64% of the world's population have been affected by disasters, and the number of 'loss events' has more than doubled (UNISDR 2012, Munich RE 2015). The year 2016 has seen the costliest twelve months for natural catastrophe losses in the last four years. Losses totalled US$ 175bn, a good two-thirds more than in the previous year, and very nearly as high as the figure for 2012 (US$ 180bn). In Europe a series of storms, and torrential rain triggered numerous flash floods, particularly in Germany, and there was major flooding on the River Seine in and around Paris. Overall losses totalled some US$ 6bn (approximately €5.4bn), around half of which was insured (Munich RE 2017).

In a world where disasters strike more frequently and with more intensity, governments have a strong incentive to increase resilience and CIS concepts like SecInCoRe are an ultimately highly cost-effective way of addressing this responsibility for risk management.

According to the feedback gathered from the stakeholders engaged throughout the project, this strategy seems to be the preferred one. The SecInCoRe Advisory Board suggested several times

that the most applicable way to sustain SecInCoRe is to be sustained and maintained by a European institution. This would increase the level of trust in the platform as well as push organisations to adopt it.

This approach was also identified as a possible implementation during the Joint Event conducted in Brussels on 28th February 2017[7]. Indeed, at the event, several high level stakeholders discussed the opportunity to identify an organisation that could take care of the system.

To conclude, in order to give an overview of costs of implementation and maintenance of a CIS for a Pan European body, a tentative estimation has been provided following.

According to the data provided by CS (reported in Table 1) costs for the infrastructure can be summarized as following:

		Subscriptions		
Resource	Purchase	Free Tier	Paid	Cost per month
CPU	2.2 Ghz	0.0 Ghz	2.2 Ghz	10.77 EUR
RAM	2GB	1GB	1GB	4.90 EUR
SSD	100GB	50GB	50GB	6.00 EUR
Data transfer	5TB	5TB	0TB	Free
IP	1 static IP			2.00 EUR
			Total	23.67 EUR

Table 1. Infrastructure costs provided by CS

In addition to infrastructure costs, our estimation foresees the need to add some other expense.
In particular, we foresee that should be considered to be added the cost of a technical manager Full Time Equivalent (FTE) in order to guarantee a proper technological development. It is fair to say that at the current stage it is not possible to estimate the cost of the technical manager because this is related to the place where he/she is employed.
Then, a researcher FTE should be employed as well to manage and update the CIS contents and the knowledge base material.
Finally, also a 10% of the development cost should be taken into account for CIS update and further technical upgrade.

3.2 A modular strategy for the SecInCoRe components

As written before, the second option is a sustainability strategy that allows us to analyse the exploitation potential of the different parts of the SecInCoRe system individually.

The main elements on which it could be possible to build individual sustainability strategies are (Figure 7):

- ELSI guidance;
- Pan European Inventory;

[7] The Joint Event has been organised by all the projects financed by the call SEC-2013.5.1-1 in order to show to relevant stakeholders and to representatives to the EC main projects' results.

- Cloud based services;
- Network Enabled Communication.

The CIS as a cloud based service is the only component where it is possible to foresee a commercial interest.

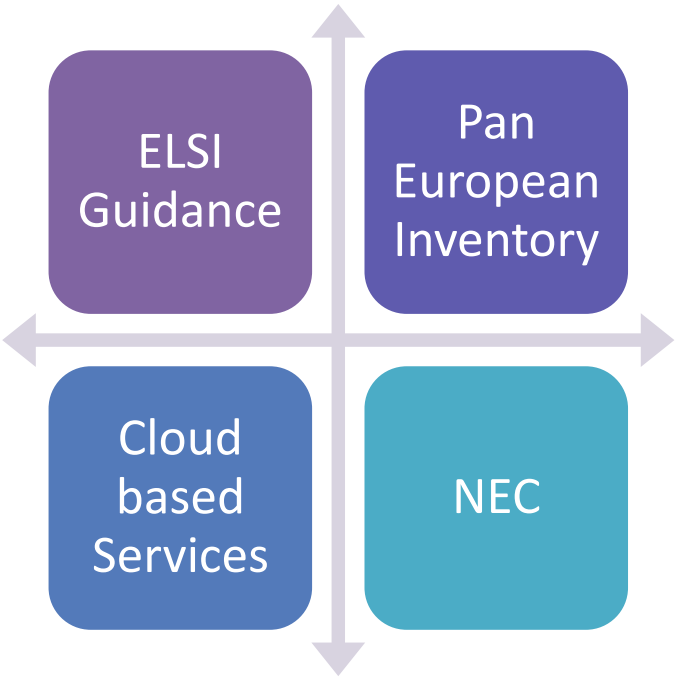

Figure 7. The SecInCoRe's components for a modular sustainability

3.2.1 ELSI Guidance for the design and use of a CIS for crisis management and response

As reported in D6.2 "ELSI Guidelines are mainly related to the standardisation strategy in order to change existing practices that link information spaces during and before/after the crisis and ethical, legal and social issues".

In this sense the work performed by SecInCoRe, in addition to the exploitation of the research within scholarly publications, has led to the opportunity to apply the research results in practice. These efforts have been pursued through conversations, iterative co-design, and evaluation of prototypes with a wide range of practitioners and stakeholders. It has produced two exploitation activities:

1) The development of ELSI Guidance to enhance the capacity for proactive approaches to ELSI in design and use. This is a collaboration between the ELSI Task Force (SecInCoRe, SECTOR, EPISECC, REDIRNET) and a range of other projects, including COnCORDE, IMPRESS, BROADMAP, BRIDGE. The result is the ELSI Guidance Community Platform www.isITethical.eu hosted by the Public Safety Communications Europe (PSCE http://www.psc-europe.eu). PSCE is a major European network for practitioners, industry developers, policy-makers and researchers, and they have agreed to host the ELSI Guidance, to promote it and make it widely available to practitioners and policy communities. The prototype ELSI Guidance platform www.isITethical.eu is available for interested parties to be explored and commented. By the end of April 2017, the transfer to PSCE will be completed.
2) The development of ELSI Key Terms as a component in the ELSI Guidance builds on a broader overview of the ELSI terminology in the BRIDGE project. Combining research

results from our ELSI Task Force collaborations, we are in the position to draw together a broad ranging set of ELSI terms related to Crisis and Disaster Management. At a meeting on the 1st of March 2017[8], it has been decided that this is a useful contribution to the CEN Workshop Agreement on Terminologies in Crisis and Disasters. Development of an ELSI terminology can help build a baseline for ELSI sensitive networked disaster risk management, with a particular focus on multi-agency collaboration and with a view to cross-border collaborations.

Thanks to the strong collaboration between PSCE, SecInCoRe, EPISECC and SECTOR, it has been possible to concretely produce the ELSI platform, which will be launched at the PSCE Conference 3-5 May 2017. The ELSI Guidance motivates networked disaster risk management models and grounds them with support for ethically circumspect, lawful and socially responsible socio-technical innovation. It thereby promotes and supports the further development and appropriation of CIS concepts like those developed by SecInCoRe, EPISECC, SECTOR and REDIRNET. The fact that the platform will be sustained beyond the project life-time will provide the opportunity for practitioners and designers to build on the work in SecInCoRe, EPISECC, SECTOR and REDIRNET. In this sense SecInCoRe's results will be sustained and exploited beyond the end of the project, influencing the way in which CIS are built for crisis management, addressing urgent issues that should be taken into account.

Considerations to expand the concept of ELSI Guidance from Disaster Risk Management to related wider practices of networked interoperability in public services, energy, smart city, and Internet of Things domains exist, building on engagement with the European Data Protection Supervisor's Office (EDPS) and their efforts in developing a Digital Ethics framework.

3.2.2 Pan-European Inventory

During the project lifetime a Pan European Inventory of past critical events and disasters has been developed. The main focus is on collaborative emergency operations and especially planning and preparing to emergency operations. The final aim of the Inventory has been to produce a critical mass of content and the infrastructure for a self-sustaining dynamic inventory that grows with the evolving landscape of practitioners, mainly first responders' and police authorities' practice. The Inventory does not intend to be a complete and comprehensive of all possible information, but it intends to create a structure and a way for information collection. Indeed, even a template for past disaster collection have been created to allow user to easily store an information that could be easy accessible by the users

[8] The meeting was initiated by the Taxonomy Task Force with support from the ELSI Tax Force and held at the CEN-CENELEC Management Centre in Brussels. The aim is to draw up a Workshop Agreement, which is a mechanism of the European Committee for Standardization (CEN), designed to create a document that specifies 'Terminologies in crisis and disaster management' (WS Acronym TER-CDM) which will be officially distributed by CEN/CENELEC. Participants included: Mr. Georg Neubauer (AIT Austrian Institute of Technology GmbH, EPISECC), Mr. Tom Flynn (TFC Research and Innovation Limited, Ireland), Mr. Uberto Delprato (Intelligence for Environment & Security – IES Solutions, EPISECC), Mr. Rainer Koch (Paderborn University, SecInCoRe), Mr. Jens Pottebaum (Paderborn University, , SecInCoRe), Ms. Christina Schäfer ((Paderborn University, , SecInCoRe) – online via web conference, Ms. Toni Staykova (Cambridge University Hospitals, ConCORDe) – online via web conference, Ms. Martina Baucic (University of Split, EPISECC) – online via web conference, Ms. Snjezana Knezic (University of Split, EPISECC) – online via web conference, Ms. Monika Buscher (Lancaster University, SecInCoRe), Mr. Jean-Louis Olie (French Ministry of Environment, Transport and Energy), Ms. Cinzia Missiroli (CEN-CENELEC), Mr. René Lindner (DIN).

As described in D3.4 the Knowledge Base as the technical representation of parts of the Inventory includes beside the past critical events the following categories:

- Data sets;
- Information management processes;
- Information systems;
- Business models.

At the current state of writing, the Pan European Inventory contains 1000 files, all publically available. The sources inserted on the knowledge base are 240 for datasets; 70 on business models and 150 for Information Systems.

As said, the multiple sources of information that make up the Inventory are applicable and dedicated to the training and preparedness phase of the emergency.

In line with this, an additional way to sustain one of the project's outcomes would be the exploitation of the Pan European Inventory as a single outcome. Nevertheless UPB will provide publically available a link to the SecInCoRe Knowledge Base and also to the semantic search as parts of the overall CIK framework and keep care of this outcome.

Further, the Inventory could be exploited by following two strategies. The first one could be to build a private Inventory based on a pay-per-use business model. The second option could be to release the current stage of the Inventory to a European Institution that will host it for free, providing access to the stakeholders.

The first strategy is already implemented by several databases and inventories containing a high level of specific information. For example, as reported in D3.4, in the case of the Interpol crimes database, the business model is based on a pay-per-use solution so that each country pays according to the number of searches done by its agents. Other examples are the database for chemical emergencies managed by a private company, Herwell UK, that introduced a fee for all stakeholders that wanted to access the database.

In this sense, the SecInCoRe Inventory could be transformed into a privately managed tool, accessible only as a subscription service in order to cover costs of infrastructure, maintenance and further development.

In order to promote this approach a declaration of interest from one or more partners in the consortium needs to be expressed which currently is not the case.

The second option is to set up a collaboration with a European institution so that they host the Inventory. In this way, due to the ownership by a European body, the inventory would be financially supported in order to maintain the system and make stored data and information publically accessible for stakeholders. This could guarantee a high level of visibility, willingness to contribute and the impact of the stored knowledge will be higher. However, this means that political willingness and a strong interest from the institution should be present in creating a collaboration with the SecInCoRe project.

3.2.3 Cloud based services

An additional way to sustain SecInCoRe's output is related to the fact that SecInCoRe has been designed as a cloud based service. One of the partners, CS, currently hosts the CIS on its cloud. In the following section, a business model based on the vision of CS and their expertise on cloud services has been provided according to SecInCoRe potentialities.

During the project, CloudSigma has hosted servers for each component of the CIS including the OpenAtrium and Pan-European Inventory and provided direct access via the OA to the isITethical website. The CIS benefits from the usual real-world advantages of the cloud including, increased accessibility, instant scalability, commercial grade service provision, and increased reliability due to strict Service Level Agreements. Organisations can also take advantage of the infrastructure-level security offered by a commercial cloud provider, as well as the data protection laws relating to the location where the data is being stored.

CloudSigma has identified three main ways in which the SecInCoRe CIS can be exposed via the cloud to potential customers. We outline each one below.

CIS Drive Images

The simplest way to expose the SecInCoRe CIS in the Cloud is to allow users to create a Virtual Machine (VM) and attach a ready drive image. The OA drive image is shown below (Figure 8) in the Drive Library of the CloudSigma WebApp as proof-of-concept. This could be extended to include other components of the CIS such as the Semantic Framework.

Figure 8. Open Atrium drive image.

The same steps would apply in a real-world setting beyond the project:

1. Create CloudSigma account;
2. Clone CIS drive image to ‘My Drives’;
3. Create custom server/VM and attach CIS drive image.

Hosted / Managed Services

Due to the functional and economic advantages, the cloud provides a rich environment where services can be packaged and hosted.

It must be noted, that as managed services are currently outside CloudSigma’s core business as a pure Infrastructure-as-a-Service cloud provider, there is no immediate plan to implement such services. Instead, CloudSigma remains open to partnerships with service providers wanting to run web services on scalable and cost effective cloud infrastructure. Such services would typically have their own user interface or web application, shielding the end-user from the complexity of maintaining the underlying infrastructure. However, some end-users may prefer to have direct control over the underlying cloud resources for the purpose of performance optimisation or tracking resource consumption. In this case, another approach would be a partnership whereby CloudSigma promotes the service via their marketing site and makes the service configurable from within the CloudSigma WebApp.

The Figure 9 presents a mock-up of how this might look according to a common model applied by many WordPress hosting providers. Please note, that the pricing is indicative.

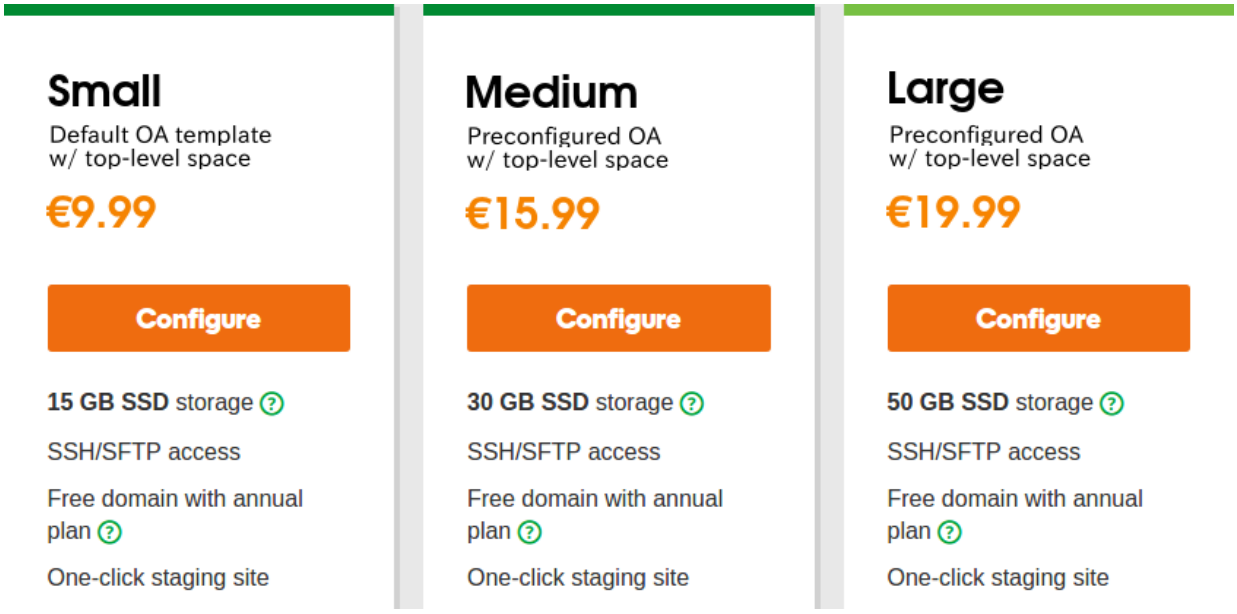

Figure 9. Mock-up for commercial exploitation

As shown, different cost brackets are typically applied depending on the level of service. For example, a low-cost tier could be offered which would include only the essential elements required to create a top-level space, subspaces and section, combined with minimum cloud resources. Paid tiers could also be offered, providing users with pre-configured spaces, subspaces and sections, with more cloud resources. Users would still be able to customize appearance and create the necessary permissions. A pre-configured space would resemble the current Demonstration Space created as proof-of-concept for the project including the current section structure; Discuss (discussion board), Contribute (document share), Inquire (semantic search), Reflect (ELSI Guidance), Admin Support (how-to-guides), and the live chat facility available across all pages. Customers would have the option to increase storage capacity at any time. One advantage of making the CIS cloud-based is that users are able to connect to and manage other components of the modular system, such as a data repository, which could even be hosted in the same cloud using the same account to avoid extra networking costs.

The following sub-section describes how this model could potentially be commercialised further using the CIS-as-a-Service approach.

CIS-as-a-Service

The cloud offers a unique opportunity for third-party software developers to build upon the default OpenAtrium platform, create new CIS templates, and as Service Owners either provide them for free or on-sell them as-a-Service. The definition of Service Owner in this context could be an Emergency Service with an IT department dedicated to integrating and maintaining the CIS, to an independent software vendor or value-added reseller who wishes to offer the CIS as a commercial service. Theoretically, developers could take only the CIS concepts developed during the SecInCoRe project and develop their own CIS using whatever platform or programming language they prefer. Service Owners can choose from a number of different billing models. However, the two most common billing models applied by Cloud Service Providers and most Online Services are subscription based (recurring periodic billing) and/or a one-time payment system. Subscription is usually preferred as discounts are often applied.

As a commercial cloud provider, CloudSigma encourages this approach as it creates new sales channels, more potential sign-ups and ultimately the consumption of cloud resources. It should also be noted, that due to the project's commitment to ensure interoperability, Service Owners are not limited to using CloudSigma as their cloud infrastructure provider. This model is replicable on any Cloud, or even on an organisations on-premise infrastructure.

Below (Figure 10) is an example showing how this approach could be commercialised in this way.

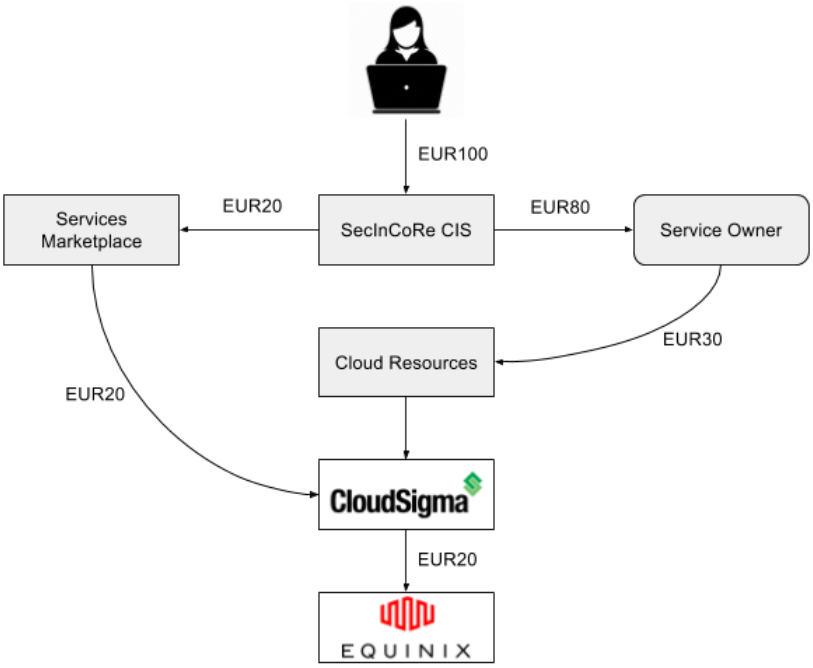

Figure 10. SecInCoRe CIS-as-a-Service value-chain

An indicative amount of EUR100 (Figure 10) is used for simplicity to demonstrate how revenue could be split between stakeholders. Again, the service could potentially be hosted anywhere, but CloudSigma is used as an example.

1. The customer deposits EUR100 into his/her account using CloudSigma's existing merchant services;
2. The marketplace takes a 20% commission from the service leaving EUR80;
3. Of the remaining EUR80, the Service Owner receives EUR50;
4. CloudSigma receives the additional EUR30 for the infrastructure hosting and operational management of the services marketplace;
5. CloudSigma retains EUR10 for providing the cloud stack and operational management, and passes on EUR20 to the data centre for providing the data center environment, power, space and the physical equipment.

In real commercial terms we are able to calculate the cost of running and maintaining the SecInCoRe CIS components based on the current system hosted on CloudSigma's infrastructure. CloudSigma offers a very simple and transparent approach to pricing. Resource consumption is billed in aggregate allowing customers to build their infrastructure exactly how they like with totally unbundled resources and server sizing. The billing looks at CPU, RAM, storage and data traffic usage every 5 minutes. Resources can be purchased on demand, via subscription, or a combination of the two. All accounts created at CloudSigma qualify for a free resource tier comprised of 1GB RAM, 50GB SSD, and 5TB of outgoing data transfer, applicable on a monthly

basis, forever.

We can assume the following resources (Table 2) will be adequate based on current resource consumption in the project.

		Subscriptions		
Resource	Purchase	Free Tier	Paid	Cost per month
CPU	2.2 Ghz	0.0 Ghz	2.2 Ghz	10.77 EUR
RAM	2GB	1GB	1GB	4.90 EUR
SSD	100GB	50GB	50GB	6.00 EUR
Data transfer	5TB	5TB	0TB	Free
IP	1 static IP			2.00 EUR
			Total	23.67 EUR

Table 2. Infrastructure costs provided by CS

It should be noted, that a service owner could benefit from further volume discounts and by hosting multiple CISs on a shared environment. This would significantly decrease the operational costs allowing for a greater profit margin. Further volume discounts are available by negotiation for baseline services (compute and storage).

CloudSigma's standard SLA is applicable for all accounts and includes the following guarantees: 100% Virtual server availability, 100% Network uptime, 1MS or less network latency.
CloudSigma's comprehensive tiered support service and escalation policy is available for all accounts. Live support is provided 24/7 via Telephone, Live Chat, Email and the Zendesk online ticketing system. The free tier is usually enough for most customers. However, two paid tiers are also available and include extra services such as quicker guaranteed response times, unlimited named contacts and dedicated resolution engineers.

3.3 Commercial impact in the domain of PPDR

In addition to all the components identified for potential sustainability, another important effect of SecInCoRe is related to the commercial impact of the project in the field of PPDR in order to create new business services for training and preparedness.

In line with this, two particular concepts that could be affected are related to NEC (Network Enabler Communications) which targets to:

- Provide interoperability and cross border communications for PPDR organisations in the European countries during mission on the field;
- Guarantee mobile and seamless access to SecInCoRe-supported CISs. Using RescueRoam and SecInCoRe's seamless access technologies, the NEC provides CIS access regardless of existing infrastructure.

Indeed, it is in line with these two targets that SecInCoRe plans to create new business opportunities related to new services provision. The following paragraphs address the way in which SecInCoRe can create new services in the PPDR domain in ways that link the potential of

SecInCoRe to the commercial expertise and interest of the two major commercial partners of the consortium: ADS and CS. The aim is, from one side, to explain the potential exploitation of interoperability systems and ADS interests in this regard. From the other side, reports the potentiality of RescueRoam for preparedness and training and its potential commercial exploitation from CS's perspective.

3.4 Interoperability and cross border communications

Interoperability and therefore cross-border communications between Public Safety organizations in the European countries have so far been very limited mainly due to incompatible communication systems in the countries. This has been one of the topics of interest within SecInCoRe. However, ADS clearly also had a relevant interest on the issue and its relation with the market. The following paragraph described the ADS market position stressing the potentialities of new services that could be provided in relation to SecInCoRe outcomes.

3.4.1 Markets and Services

Airbus's interests on the topic are evident from its own business, ADS, indeed, has deployed more than 280 PPDR networks in 74 countries worldwide based on Tetra, TetraPol and P25 technologies. In this sense, more and more, customers intend to use and maintain their networks up to 2030 or even 2035, while they also intend to deploy, in parallel, new services over Broadband private or commercial networks. Therefore, users on the field will benefit not only of new Mission Critical Services (e.g. MCPTT, MCData, MCVideo) but also of applications (including data base information), intranet and internet information during their mission. In order to achieve this, the gateway between the services offered by the legacy networks and the services offered by the Broadband network is a key enabler to ensure service continuity and smooth evolution. Moreover, some PPDR organisations envisaged this service continuity not only for fixed networks but also for tactical networks solution or a combination of both, including during mission abroad or during cooperation.

3.4.2 SecInCoRe and 3GPP Context

As part of the SecInCoRe project, the work performed in WP4 and described in D4.3 report details on the analysis, on the options and on the rational to select the Mission Critical Services specificied by the 3GPP since 2015; then, D6.2 describes the status of the work done by the 3GPP on the Mission Critical Services.

3GPP has planned to address the interoperability and cross border communications with the Feasibility Study called "Mission Critical Communication Interworking between LTE and non-LTE LMR systems" started in 2016. Airbus is an active contributor at 3GPP working groups on this item. The feasibility study is planned to be completed by June 2017, and then the first set of technical specifications will be initiated and are planned to be available by end 2018.

3.4.3 Airbus position as part of SecInCore

Without waiting for the availability of the full set of 3GPP specifications on this item, ADS has started to design a few months ago, in line with the current specifications, a prototype of a gateway to bridge MCS services with PMR legacy services.

The prototype of this gateway has been installed in the show room on Airbus premises and a demo can be held during customers visit. Moreover, some weeks ago, an Airbus users group session gathering all customers was organized, and the prototype of this gateway was part of the overall demos.

This demo was very well received by PPDR organisations and has generated interesting discussions related to the services which could be leveraged thanks to this gateway. It is also seen as a key enabler for some customers to start to deploy new services on BB networks (private or commercial) while ensuring service continuity and allowing interoperability with other PPDR organisations.

In line with this feedback, RFIs (Request For Information) and RFPs (Request For Proposal) issued by PPDR organisations request this capability to bridge the services offered by their existing legacy networks with BB networks and services (e.g. MCS services). In their view, this gateway is a key enabler for these PDDR organisations, not only to ensure service continuity while leveraging new services, but also in order to help them to unify their existing PPDR communications solutions, including at borders or abroad during their missions. Therefore, this interoperability really opens perspectives which may have a commercial impact in the domain of PDDR.

3.5 RescueRoam from the idea to the commercial impact

One important aspect in order to establish a strong collaboration between different rescue organisations above all in preparedness and training in Europe is the network access to the Cloud Emergency Information System (CEIS).

The network access has to be reliable and secure as well as easy-to-use for potential users. To underline the collaboration aspect, SecInCoRe provides concepts for a common network system.

The idea behind RescueRoam is depicted in Figure 11, each participating organisation sets up its own individual communication network. A local RADIUS server checks the user credentials for the rights to access the network. At the same time the user credentials are forwarded to the CEIS, if access is granted the user gets access to the inventory and to the semantic services, the CEIS is offering.

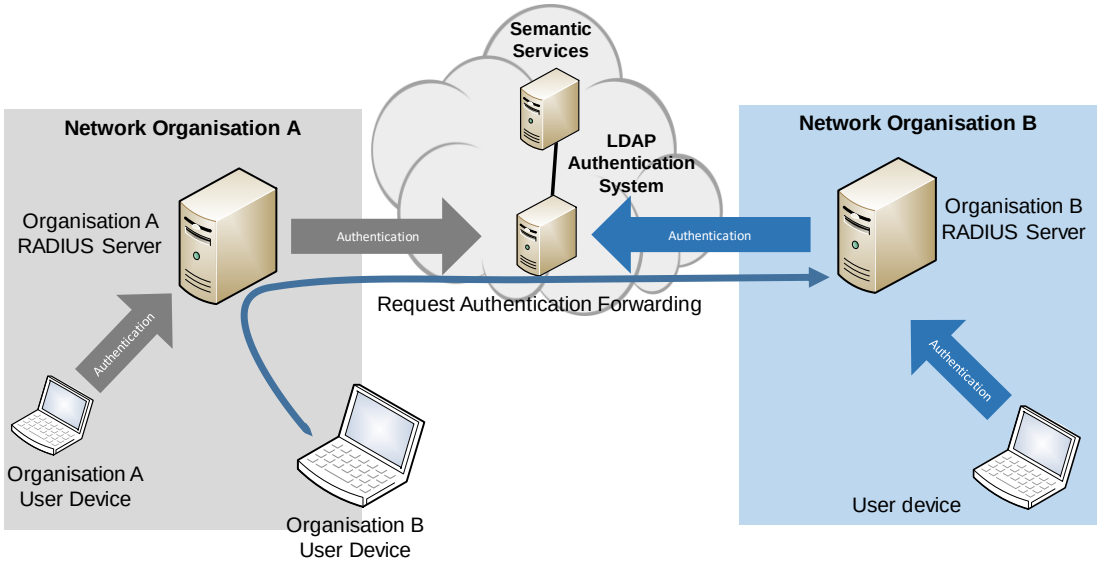

Figure 11 Authentication process in RescueRoam

A main benefit of RescueRoam becomes obvious when a user from Organisation B is visiting Organisation A, e.g. to work collaboratively on contingency plans. At the moment, the visitor has to ask for access rights to a local WiFi network, which at most provides access to the Internet. Using RescueRoam, the visitor will be able to use the same credentials as always. The request for network access will be forwarded by the RADIUS server of Organisation A to the CEIS and then to the RADIUS server of Organisation B. Hence, the visitor gets access to Organisation A's network.

Furthermore, the connection between pure network access and the access to the CEIS enables the visitor to obtain the same files and services he would obtain in the network of Organisation B.

The proposed seamless connectivity concept enables the usage of RescueRoam in each phase of emergency management. In the mitigation and preparedness phases, the setup would work as described before. In the response and recovery phases the necessity to setup ad-hoc network capabilities might rise. Seamless connectivity provides access to the Internet using all available communication technologies, e.g. WiFi or LTE Femtocells. The user credentials will be checked by the CEIS LDAP system and afterwards the user will be able to work the same way in the field as in the office.

3.5.1 RescueRoam: commercial aspects and new services

To understand the commercial potential of the RescueRoam, a number of other authentication and authorisation solutions such as EduRoam and GovRoam which serve public sector institutions in academia and government respectively have been examined. In this section it has been mentioned mainly, EduRoam, as GovRoam is based on EduRoam technology.

EduRoam provides free and secure WiFi access to millions of students, researchers and academic staff, serving multiple participating institutions in 85 countries globally. In some countries, EduRoam is also available at other locations such as libraries, public buildings, railway stations and airports. Authenticated users from participating academic institutions are provided secure internet access at any other EduRoam participating location.

User authentication is performed by the user's Identity Provider (IdP), using the authentication method specific to the IdP. The authorisation decision allowing access to the network resources

upon authentication is done by the Service Provider (SP), typically a WiFi hotspot on location. EduRoam essentially separates the concepts of authentication (handled by identity providers) and hotspots (handled by service providers) allowing both public and commercial WiFi initiatives to offer EduRoam. However, commercial entities cannot become identity providers and cannot charge for access to the network. Commercial terms can only be negotiated between a commercial entity and the identity provider.

The separation of authentication and access point could be applied in a similar way to combine both RescueRoam as the primary authentication mechanism and the NEC based on technologies such as 3GPP, both described in the previous sections.

This presents the possibility for organisations specialising in emergency response and crisis management in different countries to employ a commercial model of joint ownership, where operational costs are shared among members. This could be achieved by means of confederation, whereby RescueRoam serves as the foundation for secure access to a unified resource system. Each organisation would essentially act as Identity Provider (IdP) and operate a RADIUS/LDAP server (or any equivalent technologies) responsible for authentication of its users. It would be the responsibility of each organisation to manage user accounts and enable, restrict or terminate users based on internal policies. In the example of EduRoam, the term Home Service refers to the service provided by each organisation (e.g. University, library, etc.). In the case of SecInCoRe, the CIS could serve as a portal or user interface similar to the Home Services of the institutions connected to EduRoam. However, where RescueRoam and EduRoam differ is with the distribution of access points. In the case of EduRoam, the network is handled by the local NREN (National Research and Education Network) and WiFi provided to users in range of static locations. This is not necessarily possible in all emergency scenarios, in particular with events resulting from natural disasters.

Any form of alliance between organisations will need to address the issue of governance. There is no one-size-fits-all approach to this as the appropriate governance model must be negotiated and agreed between all the involved organisations while maintaining a simple and open process for onboarding new members. EduRoam once again offers some example of the scope and complexity of such an alliance. If we look at how the initiative began in 2003 with 5 members and how it has developed over the past decade, we can see that EduRoam was far from an overnight success, but rather took a number of years to gather momentum and become what it is today. The success of EduRoam can be measured by the growth rate of the service across the research and education networks over recent years. In 2016 EduRoam experienced a 23% increase in international authentications and a 26% increase in national authentications. According to statistics quoted by EduRoam, the EduRoam AuthN system recorded over 2.6 billion national authentications (where users from another institution in the same country authenticate their WiFi access via EduRoam) and more than 592 million international authentications. The initiative has been steered by the Global EduRoam Governance Committee (GeGC) since 2010, currently comprising of eleven global representatives. Secretariat support is provided by GÉANT, which finalised the charter for governance after consultation with EduRoam representatives from each operational region. The GeGC has the central role in the global EduRoam governance structure. Its members are nominated by the European EduRoam confederation, respectively by the National Roaming Operators in each region.

Governance between an alliance of collaborating emergency services would expect a similar level of complexity and will also need to address the various data protection laws between the EU and non-EU countries. The responsibility for creating a charter would be decided by the founding members of the confederation.

4 New business models for SecInCoRe

Investigating traditional business models for SecInCoRe has created some challenges during the project lifetime. This was essentially due to two main factors. From one side, public authorities should adopt the innovation produced by SecInCoRe but this exposes the system to public procurement procedures rather than commercial approaches. From the other side, the aim of SecInCoRe was to produce a conceptual design of a CIS. This means that even at the end of the project no fully functional system was produced on which to build a business model. In both cases the obstacle of producing several outcomes that are neither tangible and not ready for the market, opened to the reflection on alternative solutions for the SecInCoRe sustainability.

4.1 Innovation procurement through an overview of policy implementation

Bearing this in mind, another opportunity for SecInCoRe has been explored, which is Innovation procurement. Innovation procurement is a process strongly sustained by European institutions since 2009 in order to solve some of the challenges often faced in putting ICTs solutions on the market that can be considered of public interest.

In particular, due to their low application in Europe, the European Commission (EC) has started to foster the implementation of innovation procurement procedures within the Digital Agenda.

To increase the application of innovation procurement procedures by 2020, the EC started several policy initiatives. Among the many policy actions[9] that have been pushed by the EC it is possible to summarise that the EC has:

- Launched a consultation on the interest of public procurers for innovation procurements of ICT based solutions for Horizon 2020 work programme 2018-2020;
- Created a benchmarking and measurement framework for innovation procurement in Europe;
- Reinforced EU co-financing for Public Procurement of Innovative Solutions (PPI) and the Pre-Commercial-Procurement (PCP) in Horizon 2020;
- Set-up a measurement framework for ICT and R&D procurement.

In addition, the European Council, the European Parliament and other eminent institutions such as the European Research Area Board (ERAB) hold discussions on innovation procurement as a driver for research and innovation.

The EC has also been proactive in promoting this approach at national level, providing the assistance of expert to public procurers on the adoption of two main instruments which are part of innovation procurement: the Public Procurement of Innovative Solutions (PPI) and the Pre-Commercial-Procurement (PCP).

Public procurement of innovative solutions “is used when challenges can be addressed by innovative solutions that are nearly or already in small quantity in the market and don't need new Research & Development”. In line with this approach, the aim is to allow innovative goods or services which are not yet available on the market at large scale to start testing phases, creating a demand even before a commercial market has been established.

The contracting authority leads the process, boosting market opportunities within the public sector.

[9] Available at https://ec.europa.eu/digital-single-market/en/news/eu-policy-initiatives-pcp-and-ppi

However, being such process dedicated to solutions that are close to market exploitation, this solution is not appropriate for the exploitation of SecInCoRe.

This is different for the Pre-Commercial Procurement, namely the procurement of research and development of new innovative solutions before they are commercially available.

4.1.1 Pre-commercial procurement (PCP)

Pre-commercial procurement (PCP) "can be used when there are no near-to-the-market solutions yet and new R&D is needed. PCP can then compare the pros and cons of alternative competing solutions approaches. This will in turn enable to de-risk the most promising innovations step-by-step via solution design, prototyping, development and first product testing[10]".

The approach is based on creating concrete opportunities to share risks and benefits between procurers and suppliers for the entire development phase of a product, or a technology, which needs high investments in research and development, before it is ready to be commercialised. Sharing risks during the R&D phase means that more companies are able to face the developments phases. With this, markets are opened to new business actors that otherwise would be cut off; on the other side procurers get the opportunity to acquire an innovation before others.

The entire process is steered by the competition between providers of innovation. Indeed several suppliers compete with each other during the different phases of the research and development process. The phases established by the process are:

- Solution design;
- Prototyping;
- Original development;
- Validation/testing of the first products.

At the end of the process, public procurers can choose the best proposal according to the final product/service developed and according to the money proposition.

In line with this, PCP provides several positive effects for both sides: for public procurers it means to drive innovation from the demand side, acquiring innovative solutions for public services in a faster and convenient way. For the suppliers it means to have more chances to enter the market, having the opportunity to participate in a process where risks and benefits of designing, prototyping, and testing new products and services are shared.

Broadly speaking, the general advantage is that better conditions are established to commercialise results from R&D, fostering the development of innovative solutions that could address crucial future societal challenges.

4.1.2 Pre commercial procurement procedures for SecInCoRe

According to what has been explored so far, PCP is a method that could allow new actors to understand, co-create and appropriate technological potential more effectively, finding a space on the market by matching socio-technical innovation opportunities with potential investors. This is strongly related to opportunities for European companies to gain positions in the market by understanding the needs of public actors.

[10] Available at: https://ec.europa.eu/digital-single-market/en/innovation-procurement

However, such a process can also be seen in relation to organisations purely engaged in research, such as research centres and universities. In this sense the EC, under Horizon 2020, is also providing financial support for the exploitation of outcomes coming from the domain of research and innovation defined under each programme.

Recently, the EC has financed 26 projects from the ICT domain in order to provide ICT solutions to public actors through innovation procurement.

The sectors that have been financed so far are:

- Health;
- Transport;
- Energy;
- Education;
- Public administration;
- Safety.

The safety domain is clearly the one of particular interest for the SecInCoRe project. At the moment the Smart@Fire is the project that has been financed for PCP. The challenge that the project aims to resolve is that "Every year, more than 100 firefighters lose their lives whilst saving others. The SMART@FIRE project aims to tackle this by undertaking a PCP that reduces the risks inherent to fire fighting. The research and development focus for the PCP is on localisation systems, data transfer, visualization and sensors. SMART@FIRE is a cooperation between procurers of equipment for fire fighters and first responders".
Against the backdrop of the SecInCoRe project, it is clear that research and innovation in the safety domain through networked common information spaces could drive highly productive socio-technical innovation. The exploitation and sustainability of SecInCoRe could follow the procedure of PCP. However, as a matter of fact, SecInCoRe also provides insight into how PCP methodologies need to develop to enable interdisciplinary co-creation of technologies beyond simply aspiring to 'meet' pre-existing needs and demands or 'solve' pre-existing problems[11].

Due to the high-level topic of the project and due to the need of providing a new system that improves crisis management, public interest is at the core of the SecInCoRe mission, implying that public authorities are key actors of reference. Accordingly, SecInCoRe could try to constitute a group of public procurers from different European countries in order to further develop the implementation of the CIS design that has been achieved during the first financing received by FP7.

Thanks to the relation with the stakeholders created during the project lifetime, the set-up of a consortium could be started from this collaboration to develop socio-technical innovation to

[11] Technologies are transformative, enabling new ways of working. Neither technology developers, nor practitioners or policy-makers can know what these new ways of working might be. To enable agile development of technologies that anticipate and 'fit' such emergent future ways of working, interdisciplinary, experimental and iterative approaches are needed. These need to combine technological innovation with organisational innovation and analysis of often tacit social and material work practices. It is necessary to drive and synchronise innovation in technology and practice with innovation in wider policy and practice frameworks. Moreover, to proactively and creatively address ethical, legal and social issues arising in the process of socio-technical innovation, creative approaches to ethical impact assessment are needed. SecInCoRe has developed such methods and highlighted the emergence of new 'networked' concepts for crisis management, above all during the preparedness and training, but also more generally across the whole crisis management cycle.

deliver more efficient and qualitatively stronger emergency services. In this way it would be possible to translate the conceptual design of the system – arrived at through extensive and intensive practitioner engagement and co-design – into prototypes that could really be tested and adopted by public actors. Such level of public procurement could also foster the adoption of the system from public authorities from different countries, going beyond the national limitations that depend on each country when discussing national procurement procedures.

4.2 Final reflection on new business models

It is possible to conclude that the European Union is strongly working on the support of technology creation improving and fostering integrative research and development based on strong practitioner engagement.
In this sense, the EU provides new instruments in order to help technology providers in gaining positions arriving to present their ideas with the support of EU; pre commercial procurement is one of those instruments. Such opportunities are very well fitting with the needs of European projects that often struggle with obstacles and barriers of different natures that hinder translation of technology into products and services.

This situation seems also very applicable to SecInCoRe. During the three years of project, a CIS concept has been developed, in addition a demonstrator has been created to allow users and stakeholders to better understand the project's results. However, the final project's achievements cannot be defined as directly ready for a real exploitation. While it was not intended to produce ready-ness levels that are open for direct exploitation, the results are clearly exploitable and could, with some focused effort be brought into a state ready for exploitation. This would, require further interdisciplinary collaboration and collaborative design through practitioner engagement. Pre commercial procurement could be seen as a way for the project to continue the work of CIS design and its implementation addressing directly one of the major issues, namely the definition of procurers and managing authorities.

To conclude, the major suggestion for consortium partners that will keep going on the SecInCoRe exploitation is to discuss the opportunity to participate to future call for innovation procurement in order to proceed on improving current results with the aim of a real adoption from public procurers and potential managing authorities. .In addition, due to the good level of collaboration established among all the partners financed by the call SEC-2013.5.1-1, an opportunity could be to participate to a call for innovation procurement unifying the best solutions created by each project financed by the call in order to see the creation of a final product which is the result of the 4 projects financed by the EU on the topic.

5 Final exploitation Strategy for SecInCoRe Partners

A collaborative approach to ensure the sustainability of the project's outcomes has been described in the previous chapters. It is based on a project perspective without specifying the single interest of the consortium partners on future sustainability and exploitation of SecInCoRe results (or parts of it).

Therefore, this chapter will describe the exploitation plans of each partner of the consortium, taking into account their interests behind their participation in the project.

The reason why partners decided to take part to the project and what they will be interested to exploit after the end of it varies from one partner to another, mainly due to the fact that they come with different expertise from different sectors and backgrounds.

In line with this, the exploitation plans produced by the single partners are presented in the next paragraphs, following the three typologies of organisations engaged in the consortium: research partners, industrial partners and stakeholder organisations (Table 3).

Research partners
UPB
TUDO
ULANC
Industrial partner
CS
ADS
T6 ECO
Stakeholder organisations
BAPCO
KEMEA

Table 3. List of exploitation plans produced by the SecInCoRe partners

According to this difference, it is possible to anticipate that research partners are mainly producing exploitation based on research co-creation and knowledge exchange, disseminating projects results to scientific communities and impact through engagement with practitioners and stakeholders, while industrial partners are the ones that can use the projects' outcomes for a more commercial aim. Finally, the two stakeholder organisation partners can exploit mostly the knowledge acquired, the experience achieved and the contacts made for future projects and business activities.

In order to produce an exploitation plan partners have been asked to provide information about the following items:

- Partner profile;
- Identification of outcomes to exploit;
- Identification of stakeholder to collaborate with for future exploitation opportunities;
- Exploitation steps.

However, questions were slightly adjusted in regard to the different types of organisations. Indeed, industrial partners were asked to produce a plan taking into account a market strategy and commercial exploitation and giving input on:

- Market opportunities;
- Business partners;
- Competitive position.

5.1 Research partners

5.1.1 University of Paderborn (UPB)

The research group "Computer Application and Integration in Design and Planning" as a part of the University of Paderborn (UPB), is one of the leading German Institutes for research on civil safety and security. UPB participates or coordinates several research projects in relation to the PPDR domain, and is the coordinator of the SecInCoRe project. In particular, UPB is in charge of several tasks i.e. the design of the taxonomy, the CIS concept and the Inventory of data sets, information systems, processes and command and control structures used by first responder and police authorities.

In line with that, the main outcomes of SecInCoRe from UPB's perspective are the following:

- Inventory of used, available or needed data sets, information systems, business models and processes as well as command and control structures – the inventory is co-owned with other partners involved in the production of the inventory and also the technical representation of the inventory the knowledge base (partners are: ULANC, KEMEA, BAPCO, T6);
- Sematic Framework including sematic search is one service to access the knowledge base and its content and is mostly owned by UPB;
- Taxonomy based on the different inventory artefacts and especially the part describing ELSI is co-owned with ULANC;
- Concept of common information space was mainly introduced by UPB, but is a general outcome of the project, supporting future projects and organisations in the PPDR domain (owned by UPB, all).

Overall, the outcomes have been developed together with other project partners and in close cooperation with end-user.

However, the exploitation strategy foreseen by UPB is related to the fact that being an university it is not possible to sell any products, so exploitable market options from a business point of view are limited from a traditional perspective.
Nevertheless, to ensure the sustainability of the above mentioned research results, UPB will mainly reuse knowledge or IT components developed in scientific national and international

dissemination (ISCRAM, SYSCONF, INFORMATIK) and standardisation activities. Dedicated standardisation activities are already planned and they are described in more depth in D6.4.

The way in which knowledge gathered within SecInCoRe will be exploited is summarised here:

- CEN workshop agreement TER-CDM, bringing in the knowledge gathered in the research of SecInCoRe taxonomy, especially the work conducted in relation to the ELSI taxonomy;
- Reuse of the concept and ideas of a common information space in the ANYWHERE project and a further EU networking project in the proposal phase (use of the concept to share information and lessons learned with other project partners and user / end-user);
- Reuse of inventory content to bring in other research projects and in particular in the ANYWHERE project e.g.:
    - Already described case studies targeting incidents with high weather impact,
    - ELSI in the emergency domain,
    - Success factors for the uptake of information systems,
    - Analysed information management processes
- Reuse of the concepts and lessons learned of the semantic framework including the semantic search in another EU project (in the proposal phase);

In addition to the knowledge gathered, it has been possible for UPB also to maximise the collaboration with other research partners for future research activities. For example, thanks to SecInCoRe, UPB will keep going in collaborating with research partners in further projects to build on existing knowledge and common dissemination activities. For example, UPB foresees to collaborate:

- With partners of the CWA TER CDM and the taxonomy task force between the projects EPISECC and SECTOR;
- In the H2020 project ANYWHERE to bring developed systems in the market.

Furthermore, also collaboration with end-user and end-user organisations (e.g. FEU) started within the project will be foster and implemented even after the end of SecInCoRe. Then, UPB will strongly exploit the project's results participating at scientific conferences, such as ISCRAM and SYSCONF.

To summarise, UPB's exploitation strategy will be mainly based on the following activities:

- Ensure the sustainability of research results of UPB disseminating project's results;
- Reuse of knowledge or developed IT components in scientific national and international projects;
- Keep on working on standardisation activities.

5.1.2 Technical University Dortmund (TUDO)

The Communication Networks Institute [CNI], TUDO focuses on the development and quantitative performance analysis of cutting-edge communication networks and services for Cyber-Physical-Systems.

Within SecInCoRe, TUDO has been in charge of the design of the "Common Information Space" framework with a focus on the communication network developing concepts for a reliable and seamless connection to the cloud and the underlying services.

In line with the activities performed, the outcome of major interest for TUDO is the Network Enabled Communication.

However, the exploitation strategy foresees by TUDO is related to the fact that being an university it is not possible to sell any product, so exploitable market options from a business point of view are limited from a traditional perspective.

As a general approach for sustainability, TUDO is not planning a commercial exploitation of the project results and the reason is twofold. From one side because the developed concepts are based on open source projects and products, which are free-to-use for research institutes, and this would limit the possibility to commercialise the product. From the other side, TUDO is mainly interested in exploiting SecinCoRe's results, giving visibility to the project, through scientific dissemination.

TUDO has already published results and aims to publish results of the project on scientific journals and conferences, e.g:

- IEEE Transactions on Wireless Communications;
- IEEE International Symposium for Technologies on Homeland Security;
- IEEE International Systems Conference;
- International Conference on Information Systems for Crisis Response and Management;
- International Symposium on Wireless Communication Systems.

However, further dissemination at scientific conferences and on scientific papers will be pursued focusing on exploitation of the results for the scientific community to assure the sustainability of SecInCoRe research outcomes.

In addition, the work done in SecInCoRe will be resumed in other research projects:

- In the H2020 project AUTOMAT, concepts and demonstrators for seamless link aggregation will be used for further developments in the segment of car-to-car and car-to-infrastructure communication;
- The National-funded research project LARUS will provide concepts for a robust communication system for long-range maritime rescue operations.

Indeed, TUDO has significantly enhanced its knowledge in the area of seamless communication and reliable, secure cloud service provisioning. In line with these results and knowledge gathered it will facilitate the initiation of further research projects in that domain with National and European funding.

In addition to the knowledge gathered, TUDO will benefit from the strong collaboration in SecInCoRe between the partners and members of the Advisory Board. TUDO foresees to collaborate with the Fire Department of Dortmund to integrate robust and performant communication systems in emergency operations.

In summarization, TUDO's exploitation strategy will focus on following activities:

- Ensure the sustainability by scientific publications;
- Evolve the concepts in current and future research projects;
- Start further project activities based on the collaboration in SecInCoRe.

5.1.3 Lancaster University (ULANC)

The Centre for Mobilities Research (CeMoRe) at Lancaster is an interdisciplinary research centre, specialising in social science and design research based research co-creation around all

things mobile – from transport to informational mobilities. Within SecInCoRe, ULANC has led the production of domain analysis, ELSI guidance, Ethical Impact Assessment and co-design methodologies, PIAs and Ethical Monitoring.

In terms of exploitable products and services, ULANC has produced the following outcomes:

- Research on the practices of communication and collaboration in EU disaster risk management, ethical impact assessment methodologies, ethical, legal, social and societal opportunities and challenges and more. Ownership is captured in authorship of publications and reports. This includes the Case Studies incorporated into the SecInCoRe Pan-European Inventory;
- ELSI Guidance (isitethical.eu). This is jointly produced by the ELSI Task Force (led by ULANC) and governed by ULANC and PSCE (www.psc-europe.eu) under a Creative Commons License. Some content (in the legal section and the organisational interoperability section) was provided by partners in EPISECC, SECTOR, and REDIRNET, as well as examples and individual guidelines by project stakeholders. Further content will be contributed by future users;
- ELSI Terminology and Taxonomy. This has been produced in collaboration with the SecInCoRe team, particularly UPB, and in collaboration with EPISECC. This is being incorporated in the CEN Workshop 'Terminologies in crisis and disaster management' (WS Acronym TER-CDM);
- A socio-technical CIS concept that builds upon existing research in computer supported cooperative work to address contemporary and future technologies, with a specific focus on their role and potential in disaster risk management.

The outcomes described above are an integral part of the innovation produced by the SecInCoRe project. Together, the components described above support the conceptual development of support for:

- Awareness of what knowledge (e.g. of past disaster events) is out there;
- Greater efficiency in finding such knowledge and increase understanding of how it is relevant and relates to local risk assessment practices;
- Secure (both technical and social) information sharing and communication practices through systems that have technical and human practice-based security techniques built in (less hackable or breakable system);
- Ethically, legally, and socially circumspect and proactive disaster information technology use;
- CIS design that supports real world work practices more carefully, ensuring technical and human practice-based system security (less hackable or breakable system);
- Social suitability of the systems (e.g. support building trust, enable configuring awareness);
- Societal security (better and more ethical information sharing to support the ability to more critical engage with necessary actions to better address individual, community, national, and international security).

Through the collaboration in the SecInCoRe project, researchers at Lancaster University have acquired new knowledge about networked and mission critical communications infrastructures, cloud computing and services, taxonomy and semantic frameworks, common information space concepts. We have extended our network of stakeholders and practitioners in disaster risk

management and developed new capacities in methodologies for responsible research and innovation and ethical impact assessment. These results and new capacities are exploitable. Two different but interrelated aims shape our efforts here:

A first goal is continued advanced responsible research and innovation through co-creation and knowledge exchange with researchers and research organisations (e.g. the BRIDGE and SecInCoRe consortium, ELSI and Taxonomy Task Forces, ISCRAM, and other EU projects, such as IMPRESS, ConCORDe, EMERGENT, iTrack, SATORI), emergency services practitioners and stakeholders within disaster risk management, the general public, policy-makers, commercial developers of services and technologies, including also policy-makers, and public bodies such as Emergency Response Coordination Centres at national and EU levels. We are part of efforts to pursue, and individually pursue, opportunities with national, EU and international funding bodies. Further publications, including interdisciplinary publications with SecInCoRe and the ELSI and Taxonomy Task Force members are in development, as are invited presentations and keynotes.

A second, closely related goal is to co-create impact through translating research results into real world contexts in dialog and collaboration with practitioners and stakeholders, for example, by actually hosting the ELSI Guidance as a community platform at www.isITethical.eu in collaboration with PSCE, and orienting this towards PCP within ICT, security and safety domains as well as independent organisational and commercial innovation. Through engagement with a broad network of practitioners, commercial and industrial technology and service developers, academics, policy-makers and public service organisations (e.g. FEU, DG ECHO, JRC, DRMKC, the Lancashire Resilience Forum, and UK Cabinet Office Resilience Direct network). Engagement with standardisation initiatives forms another avenue in this process, for example through the ELSI terminology and taxonomy work incorporated in the CEN Workshop 'Terminologies in crisis and disaster management' (WS Acronym TER-CDM).

To summarise, the exploitation plan for the end of SecInCoRe is based on three major steps:

- Develop a sustainable ELSI Guidance Community Platform together with PSCE, develop proposals for research collaborations that can drive development of ELSI Guidance and Ethical Impact Assessment innovation forward;
- Develop ELSI terminology and taxonomy incorporated in the CEN Workshop 'Terminologies in crisis and disaster management' (WS Acronym TER-CDM);
- Share knowledge through publications and presentations in interdisciplinary scholarly and public forums (e.g. ISCRAM, sociology journals, emergency journals, etc.), develop further responsible research and innovation collaborations on related topics;
- Develop research proposals with national, EU and international funding bodies and consortia.

5.2 Industrial partners

5.2.1 CloudSigma (CS)

CloudSigma is a pure-cloud Infrastructure-as-a-Service (IaaS) provider that offers highly available, flexible, enterprise-class cloud servers and cloud hosting solutions. CloudSigma is one of the most customizable cloud providers on the market. Customers are able to provision processing, storage, networks and other fundamental computing resources at their discretion, meaning CPU, RAM, Storage and bandwidth can be purchased independently to allow the best

combination of cloud resources without the limitation of fixed sizes. This enables customers to "right-size" their workloads and take advantage of cost control methods for best possible VM and Storage consumption. CloudSigma uses a proprietary cloud stack on top of KVM. This enables CloudSigma's development team to incorporate new features at a much faster rate based on customer demand. CloudSigma is available via a number of multi-cloud drivers such as libcloud, fog.io, jclouds, Ansible, that enable customers to drive multiple cloud stacks including CloudSigma and Openstack side-by-side. CloudSigma's WebApp offers full management capabilities at the infrastructure layer as well as VNC access to cloud servers. Additionally CloudSigma has 100% coverage of all features via our API allowing full automation of any functionality as required by customers. There are absolutely no restrictions on the type of operating system that can deployed. Any x86/x64 operating system will run on the CloudSigma platform, as long as it is compatible with standard Intel/AMD architecture. Customers can use their own images, import AWS and VMware images, or use images from our Marketplace.

CloudSigma's primary role in the SecInCoRe project was to facilitate the hosting and maintenance of cloud infrastructure and implement the cloud-based communication system, Common Information Space concept. CloudSigma provided insight into the available cloud services, and in particular the security and privacy mechanisms employed to maintain integrity at the infrastructure level, as well as mechanisms required to facilitate the authentication of emergency personnel from different EU member states. This led to the implementation of the RescueRoam, which provides a common network space that can be shared by all parties involved in an emergency event. It includes mobile access points situated on the sights of emergency, secure WLAN connectivity that provides access to the full SecinCoRe functionality, personal single-sign-on credentials that can be used to access other SecInCoRe components. In summary, CloudSigma makes available to the project a cloud offering comprising of a production cloud environment in Zurich, Switzerland and provides real-world commercial expertise to help determine the design of the secure cloud emergency information services.

Regarding the outcomes that are potentially exploited by CS, those are:

- CIS;
- Semantic Framework;
- NEC.

SecInCoRe CIS - Various free open source frameworks for building the CIS were explored at the beginning of the project. At the time, Open Atrium (OA) was deemed the best choice due to its large open source community, comprehensive list of apps and modules, compatibility with prominent authentication mechanisms, and highly customizable security functionality. OA, maintained by Phase2 Technology, is a Drupal distribution used predominantly as a tool for building intranets and other collaboration platforms. Drupal is a free and open source content management framework written in PHP and distributed under the GNU General Public License. The current SecInCoRe CIS can exposed to end-users with CloudSigma infrastructure accounts as a drive image via the Image Library. This image would comprise of a CIS with three spaces, (1) the SecInCoRe CIS Concept documentation space, which administrators can use to explore the underlying concepts of the CIS and (2) a Validation Space, providing information regarding the validation process and outcomes achieved within the SecInCoRe project, and (3), the SecInCoRe Demonstration Space, allowing administrators to experiment and build upon a preconfigured space. They will be able to clone spaces and utilise the pre-installed apps, modules (plugins) and widgets. Administrators can also refer to the Admin Support page of the Demonstration Space for step-by-step how-to guides explaining such tasks as, controlling access

to content, managing space membership, and creating teams and groups.

Semantic Framework - It has been suggested before in previous deliverables that the components required to deliver the semantic search (OSF, ManifoldCF, Contribution, Knowledge base) could potentially be delivered as a suite of independently deployable, modular services, benefiting from the usual advantages attributed to the deployment of microservices in the cloud, such as independent testing, scalability and fault tolerance. The semantic framework would essentially be separated into a presentation layer (User Interface), an application layer which performs the domain logic, an integration layer to connect the different components of the application layer, and the database layer which stores the knowledge base. The presentation layer could also provide a single user interface which not only presents the separate components of the Semantic Framework, but the OA CIS as well. While the microservices concept was not in scope of the project, it is considered a logical strategy to explore for any post project exploitation activities. This could include exploring synergies with other H2020 projects we are involved in and assessing the technical and commercial feasibility of including this into our current development roadmap.

SecInCoRe NEC (Network Enabled Communication) system - No direct exploitation of the NEC is envisaged by CloudSigma. However, the NEC system is seen as an essential network technology, compatible with and complementary to the cloud-based service provisioning infrastructure.

Regarding the market opportunity envisaged for the above mentioned outcomes, it is possible to state that OA started strong and the opensource community increased rapidly. However, since CS decided to adapt OA for the CIS, support for the platform has noticeably declined, certainly in comparison to its competitors. This lead to some problems when trying to upgrade and improve the OA due to incomplete or unstable modules, a lack of supporting documentation and a shrinking developer community with forum results from several years ago showing unresolved bugs. OA remains a viable and competitive option for building secure collaborative platforms where user-generated content is required, but if popularity wanes in favour of new open source players such as Redmine, Moovia, Podio and VisionProject, OAs future is uncertain. Even the recent upgrade to OA 2.0 did not manage to provide a much needed boost. There has also been a boom in recent years of multi-tiered commercial solutions such as Pydio, IBM Connections, Jive and Sharepoint, which now dominate the market. Slack is a newcomer making huge waves by combining advanced functionality with extreme customization and a streamlined, user-defined user experience. Since 2014, Slack has grown rapidly to serve 2.7 million daily active users, 800,000 paid users and employs 430 staff. According to 451 Research, the social business application revenue is expected to reach EUR34 Billion by 2019, rising 22% from 2014 to 201912. While OA has served a purpose at least in terms of providing a tool for demonstrating the CIS concept, CS sees somewhat limited opportunity for commercial exploitation of the current OA CIS implementation as it stands, without considerable future investment.

The stakeholders identified as relevant for the business depend on the current implementation which offers software developers with Drupal experience a solid platform upon which to extend and enhance functionality and offer as a commercial product. In this sense, independent software vendors and value-added resellers have been identified as key stakeholders and therefore intend to include both OA (without modification) and the SecInCoRe CIS (retaining the free open source license model) in the Drives Library, accessible from the CloudSigma Web App. In

[12] Available at: https://451research.com/images/Marketing/press_releases/05.07.15_SocBus_Press_Release.pdf

theory, the SecInCoRe CIS can be included as an application template making it instantly deployable into a CloudSigma Infrastructure account, offering auto-scaling and load balancing as the demand on computing resources varies through their use.

Regarding its own business in the sector, the company states that CloudSigma's services marketplace offers developers a simple and powerful platform for exposing applications to potential customers, directly on top of a highly flexible and customizable underlying cloud infrastructure with a simple and transparent billing model. This offers independent software vendors and value-added resellers a highly efficient and cost effective environment to build their offering and to implement whatever business model they wish. The options are endless, but one model which has gained a lot of traction in recent years in line with Cloud Computing, is the as-a-Service approach.

In this sense adopting for SecInCoRe CIS-as-a-Service allows software vendors the opportunity to make use of a multi-tier service delivery model. To illustrate how the service might look we provide the following three service levels as an example:

- Free tier - default OA template comprised of top-level space only, accompanied by intuitive instructions on how to build a CIS from scratch;
- Paid tier (1) - pre-defined structure based on the SecInCoRe CIS demonstration space
- Paid tier (2) - pre-defined structure based on the SecInCoRe CIS demonstration space, with more templates, premium features and better technical support.

All application level support would be provided by the Service Owner, as well as most of the marketing aspects. It would be in CloudSigma's interest to support marketing efforts and promote the service in parallel, using such methods as, customer newsletters, social media, and blog posts.

Then, it was also asked to CS to explain its position on a future collaboration with SecinCoRe partners for a collaborative exploitation. In this sense CS made clear that at least some Drupal expertise is required to make the most of OAs functionality and to offer the CIS at a commercial level. Software developers unfamiliar with Drupal, may prefer to develop their own application using tools and programming languages they are proficient in. If this is the case, they will benefit greatly by the CIS concepts and lessons-learned documented by the consortium during the SecInCoRe project.

If the consortium expects to attract third party software vendors to the SecInCoRe CIS implementation, and convince them of its commercial potential, it will still need to be demonstrated at the very least to meet the requirements of the targeted user groups. CS sees this effort continuing past the end of the project, with consortium members continuing to provide support according to their contribution so far on the project.

As a potential stakeholder, CloudSigma would focus on its core business and expertise by providing the marketplace and underlying cloud infrastructure upon which further CISs can be deployed. This would be provided unconditionally, regardless of whether the CIS was developed by the consortium or by third-party software vendors.

Looking at possible competitors, at an infrastructural level, CS sees hybrid cloud solutions becoming more and more common, essentially changing the way customers manage security and privacy. According to research by information technology research and advisory firm Gartner, private cloud is slowly being overtaken by hybrid cloud topologies, with more than half of large enterprises predicted to have hybrid cloud deployments by the end of 2019. A Hybrid Cloud solution suits SecInCoRe proposition perfectly as it offers data owners the opportunity to store

broad data sets with different data protection requirements, all accessible from the same point. Organisations wishing to develop a SecInCoRe style CIS may want to use both public and private infrastructure for storing data depending on the sensitivity of the data. This would involve a data movement and data discovery strategy. While this was out of scope of this project it is something that is very achievable.

To conclude, in addition to the individual interest in project's results in the field of cloud services, CloudSigma stated that its participation in SecInCoRe increased its exposure to new user groups, allowing to explore research topics that are increasingly relevant to meeting the demands of the customers, but may not have the specific expertise or resources to explore and address them alone. They also see the collaborative component of the project as invaluable as it puts them shoulder to shoulder with leading commercial and academic partners. In line with this, the collaboration achieved so far will be extremely useful for future collaborative and further business opportunities.

5.2.2 Airbus Defence and Space (ADS)

As reported in D6.2 "Introduction of digital Private Mobile Radio communications (PMR) technologies during 1990's (TETRA, TETRAPOL) triggered significant improvements for mission critical users where it comes to security, operational efficiency, feature richness and service availability. Today these networks are used widely in more than 120 countries by mission critical and business critical user organizations".

In the previous deliverable a state of the art of the sector was provided by ADS in order to clarify the most important requirements of Public Safety user organizations when evolving towards future solutions for mission critical communication.

In addition to a market evolution outline in Europe, it was also stated that the Public Safety business environment is in turmoil, following such analysis, ADS identified its own role in the current changes facing some major topics that are effecting the field such as business models and partnering. In addition, ADS also stated that it is currently facing changes on transforming technology and application eco-system.

According to the massive transformation happening nowadays in the public safety domain, ADS, in quality of a major actor in the field, has redefined its exploitation's interest according to SecInCoRe's results.

Airbus Defence and Space is one of the 3 divisions of Airbus and is composed of four programme lines: Military Aircraft, Space Systems, Unmanned Aerial Systems and CIS (Communications, Intelligence and Security). Within the CIS line, one of the core businesses is the design and deployment of PPDR communications networks worldwide based on NarrowBand (NB) and Broadband (BB) technologies.

In this regard SecInCoRe is designed for PPDR organisations and this is where ADS's interest in exploitation is particularly high.

Regarding the exploitable product in the context of SecInCoRe project, ADS has addressed the interoperability issue between the BB networks and NB networks by developing a prototype of the Mission Critical Services (MCS)-TetraPol Gateway (GW). This prototype GW is based on the 3GPP- MCS specified by the 3GPP, and it anticipates the results of the study item work initiated by the 3GPP related to MCS interworking with legacy networks.

The developed prototype GW has been individually owned in order to sell the prototype as a product, when the development will be fully completed. This implementation will be part of the Airbus DS PMR products portfolio. In line with this, there is no applicable a common consortium exploitation.

The relevance of the prototype GW is due to the fact that this represents a key milestone in the development of this GW as a product. As a product, this GW will also take into account other NB technologies such as Tetra and P25 in addition to TetraPol. Moreover legacy technologies can interop via three main interfaces: analogue, console interface and inter-network interface. Therefore, many combinations may have to be supported according to the market and existing customer deployments.

PPDR networks are deployed worldwide in more than 120 countries. The market opportunities envisaged by ADS are first where the TetraPol networks are deployed by Airbus DS and then the Tetra and P25 markets.

It is key for these PPDR organisations to bring BB services, including at borders, while still ensuring continuity of the service with existing legacy networks, thanks to interoperable BB solutions based on 3GPP standards.

5.2.3 T6 Ecosystems (T6ECO)

As already reported in D6.2, T6 ECO is a consulting and research company with extensive experience in participating and co-ordinating national and international research and innovation projects. The T6 ECO mission is to study the development of the Information Society, promoting studies and innovative projects through the use of information and communication technologies for a sustainable and durable development of territories, companies, clusters and research actors.

T6 ECO is specialised in socio-economic research, planning, coordinating and deploying research activities using both qualitative methods (ethnography, in-depth interviews, focus groups, Delphi, etc.) and quantitative techniques (longitudinal survey, multivariate analysis, social network analysis, etc.) techniques.

In line with this, even if T6 ECO is identified as an SME, its main business is based on research activities at national and European level. For this reason, T6ECO has no commercial interest on the commercial exploitation of the outcome of SecInCoRe. On the other hand, T6 ECO is extremely interested in exploiting the knowledge acquired during the project and to take advantages from the networking opportunities explored so far in order to enlarge future research opportunities.

In particular, the knowledge acquired on CIS and ELSI guidance opens up new opportunities for T6 ECO to be engaged in new fields of research.

The first opportunity to exploit the knowledge acquired is in relation to the validation and evaluation methodology that has been developed specifically for the CIS of SecInCoRe. Implementing and revising the usual T6 ECO methodology for the purposes of SecInCoRe, T6 ECO has experienced a different way to approach impact assessment and thanks to this experience it will be able to propose the work on impact assessment for information systems and also for other IT solutions. This will improve the fields in which the impact assessment can be applied, opening new possibilities for T6 ECO to apply to calls funding European or national projects.

Second, another chance for exploiting the results of SecInCoRe is in relation to networking opportunities emerging from the project. Thanks to the work of validation and evaluation with

the stakeholders engaged in the project, T6 ECO had the chance improve its knowledge on the world of emergency services, also establishing personal contacts with some of the people engaged in the activities. The aim is to transfer some of the contacts in formal partnerships, applying for other project in which exploit some of the results achieved so far. For example, potential collaborations could start with the Italian Fire brigades and the Italian Civil Protection Agencies.

At the current stage of the writing a concrete example of what stated on networking opportunity for future partnerships can already be provided. Thanks to SecInCoRe, during the project development T6 ECO has established a contact with the Leitrim County Council. Such contact has been translated in a partnership opportunity. Indeed, together with the Leitrim County Council and other six fire services from European countries, T6 ECO has submitted, in March 2017, a project proposal within the ERASMUS +[13] funding, for the call Strategic Partner in the field of the education, training and youth, in order to run the impact assessment of a set of activities that will be developed to promote fire safety awareness in schools in Europe.

As preliminary reported in D6.2, also the chance to explore co-design methodologies to design ELSI is a knowledge that will be of use for being applied in other European projects. The experience gathered in SecInCoRe, indeed, will allow to apply for a call funded by H2020 under the topic Integrating Society in Science and Innovation – An approach to co-creation[14]- in order to exploit lessons learned from SecInCoRe and contribute to the definition of new methodologies and approaches. At the current stage of the writing T6 ECO is working on writing the proposal on the field.

5.3 Stakeholder organisations

5.3.1 British Apco (BAPCO)

British APCO is an independent user-led organisation active in the field of emergency service communications and information systems. Within the SecInCoRe project, BAPCO has been in charge of the stakeholder engagement to sustain the overall process.

Regarding the main project outcomes and according to its interests, BAPCO is interested in exploring further the following components:

- The Common Information Space;
- ELSI Guidance;
- The Inventory.

However, as a non-profit organisation, BAPCO has no direct commercial interest in the outcome of the project.

On the other hand, BAPCO is interested in using the research and experience gained through the management of the external users to promote the principles of the SecInCoRe project. In particular, BAPCO will use the experience gained from the management of the User Advisory Board (identification / targeting of appropriate members; presentation of appropriate elements of

[13] Available at https://ec.europa.eu/programmes/erasmus-plus/opportunities-for-organisations/innovation-good-practices/strategic-partnerships_en

[14] Available at http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/swafs-13-2017.html

the project; involvement of members at key points of the project, etc.) to further its own objectives of promoting knowledge sharing between the emergency services.

According to its business, BAPCO works with and represents end-users in the emergency services and first-responder field. As such it has contacts within their respective organisations and the local and national government departments responsible for their governance. To foster results from SecInCoRe, BAPCO will explore the possibilities of extending the use of the ELSI guidance through its contacts with local and national government organisations. It will further explore the possibilities around the Common Information Space and the Inventory with its extensive contacts and membership in police and other first-responder organisations. The aim would be to use the knowledge gained through the development of the project (user needs / concerns / organisational change) to influence future technological developments, standards and adoption of best practice wherever possible. In addition, knowledge gained through research into information sharing and management to influence institutional / governmental thinking could be applied to foster the adoption and promotion of new technologies and to improve the need to associated human behavioural factors to the crisis management in order to modify current procedures.

It has to be stressed that BAPCO is a growing community with extensive communications knowledge gained as a result of delivering real-life public safety. The Association fosters knowledge exchange in communications to support and improve the delivery of public safety and maintains powerful relationships within public sector agencies, commercial suppliers, technologists and governments, providing a unique centre of excellence, nationally and across Europe, that is dedicated to improvement in public safety communications. Of consequence, BAPCO plans to exploit the knowledge gained in the project through BAPCO's own organisational networks, conferences and workshops.

5.3.2 Center for Security Studies (KEMEA)

The Center for Security Studies (KEMEA) is a think tank on homeland security policies and an established research center since 2005 (L. 3387/2005) within the Hellenic Ministry of Interior (former Ministry of Public Order and Citizen Protection), aiming to support security policy implementations in Greece at a strategic level.

More specifically, the activity of KEMEA includes a). the certification of practitioners of private security professionals at the national level, b). research and development in context of National and European projects in close cooperation with Law Enforcement Agencies (LEAs), working under the auspices of the Ministry of Interior and c). training of practitioners in new systems and technologies. The Center also provides advisory and consulting services to the Ministry of Interior as well as to other Public and Private authorities on safety and security issues.

A main objective of KEMEA is to bring together all national Law Enforcement Agencies (Police, Fire Service, Coast Guard, Civil Protection agency, etc.) and to enable them to collaborate, interconnecting them with corresponding agencies, research institutions and the industry from around Europe. This dedicated approach to exploring synergies, establishing communication links and working together to produce end-user driven research on all fronts of the Security Sector during the last decade, has earned KEMEA its participation in numerous National and EC R&D projects.
Within SecInCoRe, due to the high level experience in this task, KEMEA has been, together with BAPCO, in charge of the stakeholder engagement and networking with the practitioners.

In the absence of a commercially developed or available product, KEMEA's orientation towards the exploitation of the results and experience gained during the SecInCoRe project, involves the methodologies towards the reporting and formatting of the case scenarios utilized for the inventory of the project, the extraction of the relevant data sets that form the foundation and stepping stone of Common Information Space (CIS). Other aspects that were investigated in the build-up of the CIS, such as the crisis management models, the business models, the database design have been of added-value to the activities and knowledge in the personnel of KEMEA.
The invaluable experience of interaction with the personnel of authorities of first responders involved in emergency events, through various channels of communication such as the preparation of questionnaires, the interviews and the broader conversations regarding the procedures but also reaction mechanisms, and planning at all levels from the strategic, to tactical and to operational phases, has induced a wealth of knowledge that can be translated to experience that can be utilized in future design of environments such as this developed in SecInCoRe, the CIS. This is crucial for an organization such as the KEMEA which serves as the link between the end-users and the R&D, many times transferring the requests of the end-users to the developing community.
KEMEA being involved in the policy making of all facets in the security sector at national level, has gained great insight through the development of the ELSI guidelines.
The organization of workshops with participants from a broad range of first responder authorities, academics, industries and NGOs from a pan-European pool, is a knowledge gained that will be exploited in future for other projects but also KEMEA's events.

Regarding exploitation, KEMEA will take care of disseminating project's result through the well-established network of practitioners and policy makers. Indeed, one of KEMEA's fundamental objectives, as already described, is the involvement with the first responder authorities due to its position at the Ministry of Interior; this has been demonstrated during this project too. Therefore, direct interaction and access to stakeholders such as the Police, Fire Corps, Civil Protection Agency, but also the Coast Guards, Medics provides the opportunity to involve personnel of the aforementioned agencies of all levels, and expose them to the environment developed by the SecInCoRe project.

KEMEA's government authority will explore the diffusion of the knowledge gained in the ELSI guidelines to other national public agencies and bodies that could benefit from the whole or components of a concept and an environment such as the CIS.

Furthermore, the role of KEMEA as a think tank for policy making in the ministry, gives ground for exploring the ELSI guidelines; the direct interaction of KEMEA with the private security industry (certification agency) influences the training and directive of operation of these bodies.

In line with this, KEMEA exploitation will be mainly addressed through the organization and participation to events, national and international where members from all communities of the aforementioned facets of security (end-users of all levels, academics, researchers from policy and law makers to pure technology, etc.) gather and interact exchange knowledge and experience. The knowledge and experience gained during the SecInCoRe project from the design to the materialization of a concept, the parameters that can be detrimental and/or highly efficient, will be exploited and diffused towards awareness to a broad network of collaborators and interacting bodies.

5.4 Final remarks from the exploitation plans

As already stated at the beginning of the chapter, SecInCoRe is based on a heterogeneous consortium. This heterogeneity has led to a very different approach for the exploitation showing all the different interests coming from the partners.

Indeed, even among the research partners it is possible to trace and to map the different interests of research that will be exploited at the end of the project. This is the same for the commercial partners that will follow the exploitation of the project's results according to their business and economic activities.

However, according to the fact that SecInCoRe aims to deliver a concept more than a tangible technology output, it is possible to observe that generally the exploitation strategy envisaged by project partners is not very much focused on the direct commercialisation of products or services. Rather, the thread of the exploitation for almost all the partners is more related to the dissemination of the knowledge acquired and developed through different channels.

In most of the cases, specific projects' outputs (e.g. ELSI guidance), and not SecInCoRe as a unique product, will be taken into consideration for future exploitation. In parallel, it is possible to state that all the partners will exploit the network created during the project lifetime to create new partnership or to continue the collaboration already started.

To conclude, due to the differences from partners it is not possible to derive a similar exploitation strategy for all. However, it is fair to say that the knowledge produced as well as the network created during the project lifetime will allow all the partner to foster their own business increasing their competences and skills in the sectors of reference.

6 Conclusions

The investigation and determination of business models has been a crucial and challenging task since the beginning of the project.

Due to the complexity of the topic the strategy that has been defined has been based on the need to look at SecInCoRe from several different perspectives in order to cover as much as possible and derive a suitable model for future sustainability.

As described in the deliverable, the process of business models has followed the project development starting from a broader perspective and then going in depth in analysing the more similar solutions to SecInCoRe to gather suggestions and lessons learned.

In this sense, public opportunities, such as public procurement, as well as commercial examples has been taken into account for the project sustainability. In addition, new business models promoted by the EC have been investigated to derive a complete picture of what could be the best solution for the future of SecInCoRe. In parallel, a work of definition of all project's components for exploitation has been investigated to make clear that SecInCoRe can be seen as a unique concept but also as a concept based on several components.

In addition, the exploitation strategy for each partner has been delivered to complete the picture and make clear that each partner will take care of the project's outcome and results and will foster the work achieved done during the project lifetime according to its own business and core activities.

In line with this, the aim of the deliverable is twofold. On the one hand, it aims to provide a final and comprehensive picture of the work performed within SecInCoRe on business models for its future steps. On the other hand, it aims to capture the richness and complexity of the collaboration to define business models for socio-technical systems in order to provide some reflection for future project partners that will be faced with this task.

Literature index

451 Research. Available at https://451research.com/images/Marketing/press_releases/05.07.15_SocBus_Press_Release.pdf

Erasmus +. Strategic partnership in the field of education, training, and youth. Available at https://ec.europa.eu/programmes/erasmus-plus/opportunities-for-organisations/innovation-good-practices/strategic-partnerships_en

European Commission. Innovation Procurement. Available at https://ec.europa.eu/digital-single-market/en/innovation-procurement

European Commission. Policy Initiatives. Available at https://ec.europa.eu/digital-single-market/en/news/eu-policy-initiatives-pcp-and-ppi

Everbridge. Available at https://www.everbridge.com/

Integrating Society in Science and Innovation. Available at http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/swafs-13-2017.html

Munich RE. (2015). *NatCatSERVICE Loss events worldwide 1980 – 2014*. Retrieved from http://www.munichre.com/site/touch-naturalhazards/get/documents_E2080665585/mr/assetpool.shared/Documents/5_Touch/_NatCatService/Focus_analyses/1980-2014-Loss-events-worldwide.pdf

Munich RE. (2017). Natural catastrophe losses at their highest for four years | Munich Re. Retrieved April 13, 2017, from https://www.munichre.com/en/media-relations/publications/press-releases/2017/2017-01-04-press-release/index.html

Osterwalder, A., & Pigneur, Y. (2010). Business Model Generation: A Handbook For Visionaries, Game Changers, And Challengers . Wiley.

Resilience Direct. Available at https://www.gov.uk/guidance/resilientcommunications#resiliencedirect

UNISDR. (2012). Impacts of Disasters since the 1992 Rio de Janeiro Earth Summit. Retrieved September 8, 2016, from http://www.preventionweb.net/files/27162_infographic.pdf