ARIES WP3 – Needs and Requirements Analyses

Jacob Löfvenberg and Jonas Hallberg
FOI

Christian Gehrmann
SICS

Mehran Ahsant
Saab Systems

Abbreviations

COTS	Commercial off the Shelf
HW	Hardware
IAN	Incident Area Network
IP	Internet Protocol
JAN	Jurisdiction Area Network
PSCD	Public Safety Communications Device
SDR	Software Defined Radio
SW	Software
VCT	Voice of the Customer Table

Contents

1 Introduction

As the importance of information for the business of organizations is increasing so is the need for adequate information security. The information security of organizations depends on the qualities of the systems processing, storing, and transferring the corresponding data. These information systems have human, organizational, and technical aspects. Even if the scope is limited to computer security, that is, leaving the issues of how humans and organizations handle business information, it remains vital to address the influence of humans and organizations on the IT part of the information systems.

The ultimate goal, for any organization in this context, is to be able to perform efficacious information security risk management. For this purpose, it is vital to establish the security levels of the information systems of the organization.

1.1 Motivation

The foundation for the ability to reach adequate security levels is laid during the system development. However, providing viable security architectures is not enough; there has to be sufficient mechanisms for the stakeholders to be able to establish enough trust in these systems for their intended use. This is a vital prerequisite for efficacious information security risk management.

Thus, when developing security mechanisms and architectures, in order to be able to provide appropriate solutions it is paramount to understand the needs of the stakeholders regarding the ability to trust these systems. Research on security architectures for trustworthy systems requires understanding of the corresponding needs in order to be able to focus on relevant issues.

1.2 Problem Formulation

The aim of the study is to capture the needs and requirements considering trust in information systems. To accomplish this, when trust, information systems, and stakeholders are considered in general, is not possible. Thus, approximations have to be accepted. The aim is to identify sets of relevant needs and requirements that will support the identification of relevant research issues. These sets should be validated in order to enhance and establish their suitability.

One approach to identify needs and requirements is to use scenarios. An issue with this approach is that the scope of the study and, consequently the applicability of the results, may become limited to situations with contexts similar to the scenarios. Still, the use of scenarios supports the identification of needs and requirements and the scope of the study has to be limited in order to make it feasible.

The following are the main issues to be addressed during the study:

- identifying suitable scenarios to be used as the basis for the needs and requirements analyses
- identifying needs for trust based on the scenarios
- transforming the identified needs into requirements.

1.3 Contributions

The results presented in this report include:

- Two sets of needs for trust resulting from the analyses of the scenarios included in the appendices. The two sets of needs are presented in Chapter 3 and 4 respectively.
- Two sets of requirements on mechanisms for trust in security architectures. These sets result from the analyses of the identified needs. The two sets of requirements are presented in Chapter 3 and 4 respectively.

1.4 Report Layout

In Chapter 2, the necessary background is presented in the form of a list of terms used in the report. In Chapter 3, the needs and requirements identified using the scenario "Trusted Communication using COTS" are described. In Chapter 4, the needs and requirements identified using the scenario "Trust Establishment for Cross-organizational Crises Management" are described. Finally, in Chapter 5, the results are discussed.

2 Background

In this chapter the terminology relevant for this report is introduced.

COTS

Commercial off-the-shelf, COTS, are commercial components and products that are widely available.

Information security

Information security relates to information assets and the ability to uphold security-related characteristics, such as confidentiality, integrity, and availability [1]. Consequently, information security is a vast area including administrative as well as technical security issues. Contrary to IT security, information security includes issues related to information processing not connected to information (IT) systems, such as transmission by speech or paper documents.

Information system

Information systems collect, process, store and distribute information. The term has a general meaning, but is most often used for computer-based information systems. The definition includes the technical equipment of a system as well as its human activities and routines [2].

Need

Needs describe activities or resources that are required to be able to perform tasks or reach goals. Needs are related to stakeholders. They can be conscious or unconscious, real or imagined, and satisfied or unsatisfied. Outspoken needs are often related to implicit requirements for action or change.

Requirement

In the context of information systems, requirements describe what should be implemented by specifying demands on system behavior, properties, or attributes [3].

Software-defined radio

Software-defined radio (SDR) refers to wireless communication in which the transmitter modulation is generated or defined by a computer, and the receiver uses a computer to recover the signal information. To select the desired modulation type, the proper programs must be run by microcomputers that control the transmitter and receiver.

System

A system consists of cooperating entities working together with a common purpose.

Trust

Trust should in this report be interpreted in terms of communication or computing system, i.e., to what extent the users are convinced that the system behaves as expected and that it does not perform any hostile operations.

3 Trusted Communication using COTS

This chapter describes the needs and requirements identified using the scenario "Trusted Communication using COTS". The scenario is further described in Appendix 1 and gives a background that is beneficial for understanding this chapter.

The scenario uses made up names for the entities, but in reality it is a secure communication system which is to be designed by FOI.

For the requirements process we have in principle followed the methodology described in [4]. The process consists of the following steps:

1. collect data
2. identify statements
3. determine needs
4. analyze needs
5. determine architecture-driving requirements
6. analyze architecture-driving requirements

The first step, data collection, is typically done through interviews, workshops, or document studies. In this study, the data collection is based on one interview conducted with an end user of the future system included in the scenario. It would have been valuable with input from more users, but this has not been possible within the scope of this study. Still, the data collection yielded sufficient material to perform an analysis, based on the methodology presented in [4]. Since the material is rather limited in size, we have merged steps 2 and 3, yielding the Voice of the Customer Table (VCT) in Section 3.1.1. Next, we have analyzed the identified needs; the results are summarized in the hierarchy diagram in Section 3.1.2. Finally, we have determined the requirements, the result of which is given in the table in Section 3.2.

3.1 Needs

3.1.1 Voice of the customer table

In Table 1 below, we have extracted statements based on the end user interview. In practice we first identified statements in the interview notes, which we have entered in the first column below. These have then been refined into needs, the last column.

Statement	Who	What	When	Where	Why	How	Need
1. The system shall replace open communication over telephone and Internet.	The users	Communi cation	When travelling	Abroad	To be able to exchan-ge infor-mation		1. A communi-cation solution

Statement	Who	What	When	Where	Why	How	Need
2. For simple documents secure communication using e-mail, protected by GnuPG cards, is ok. But when communication is more intensive, with people placed abroad, something more is needed.	The users	Communi cation	When travelling	Abroad	To be able to exchan-ge infor-mation	More efficient than e-mail	2. A simple and con-venient communic ation solution
3. In long, spoken communication, there is a greater probability of revealing sensitive information. With documents you are usually more careful with washing and checking. When in a hurry, you usually use the simple solution, i.e. the telephone.	The informatio n owner	Protect communic ation.	When travelling	Abroad	To avoid confiden-tiality breach		3. Confi-dentiality protection for the co-mmunica-tion
4. A person abroad may need to communicate with other experts at home. A solution is a server at home and mobile computers capable of communicating with the server. Exchange of documents, e-mail, chat and sometimes video conferencing is needed.	The users	Communi cation	When travelling	Abroad	To be able to exchan-ge infor-mation	Over public, easily accessed networks	4. A com-municatio n system for public, easily accessed networks
5. The rooms from which the communication is done can be considered secure. What is critical is the link between clients and server.	The informatio n owner	Protect communic ation	When travelling	Abroad	To avoid confiden-tiality breach	By protecting the links between clients and server	5. A se-cure con-nection between clients and server

Statement	Who	What	When	Where	Why	How	Need
6. It would be convenient to be able to use the same physical machine both for normal work and for secure communication, perhaps using two unremoveable hard drives.	The users	Communication and work	When travelling	Abroad	To be able to exchange information and work		6.A system that is easy to use with regard to the number and size of hardware devices
7. It should take 6-8 hours for an attacker to modify a captured computer in a way that affects security. You have to be able to bring your computer when travelling, without using special transports. The security of the computers must not prevent the user from bringing it, or even leaving it unsupervised for a few hours.	The users	Convenient access to the computer	When travelling	Abroad	To keep using the secure solution and not fall back to usage of simpler, insecure solutions		7. The client has to be tamper protected and penetration protected and have strong authentication as well as a high level of software integrity
8. Usage must be simple and convenient, or it will not be used. GnuPG is considered simple and convenient.	The users	Simple and convenient, secure communication system	When travelling	Abroad	For the communication system to really be used		8. A secure communication system that is so easy to use that users are not tempted to revert to simpler, insecure means for communication

Statement	Who	What	When	Where	Why	How	Need
9. Since not all people are equally security aware, there is a need for being able to verify the security compliance of others.	The users	A method for verifying the security level of the other part in a communication session	When travelling or at home	Abroad or at home	To be able to trust the confidentiality protection when exchanging information		9. A way of verifying the security of the other part in a communication session
10. The customers trust in the system designer is what is important. The customers want a solution like this.	System designer	Create customer trust in system designer	in international cooperation	when needed	to be able to attract customers	by offering a secure communication solution	10. To be able to offer a secure communication solution
11. How much security do we want? The problem is the balance. How secure should it be? 100% secure is not possible to achieve. It must not be to complicated to use. As secure as possible, but still usable.	The customer	A secure system that does not put the users off	In international cooperation	Abroad	To be able to establish cooperation between customers and FOI	By making the security solution easy to use	11. A communication solution that is secure enough and that is still accepted by the users
12. The system needs better security [than now] due to an aimed interest against the system.	The customer	A communication system allowing secure exchange of sensitive information	In international cooperation	Abroad	To be able to establish and maintain cooperation between customers and FOI		12. A communication solution that is secure enough considering the threat level

Statement	Who	What	When	Where	Why	How	Need
13. It is very important to keep the trust in the security level of the system designer	System designer	Documentation supporting the claim that FOI is a trustworthy partner	In international cooperation	Where needed	To be able to establish and maintain cooperation between customers and FOI	By offering a secure communication solution	13. A communication solution that is secure enough considering the threat level
14. We anticipate really potent adversaries, e.g. intelligence agencies.	The customer	A communication system allowing secure exchange of sensitive information	In international cooperation	Abroad	To be able to trust the confidentiality protection when exchanging information	By offering a security solution with a high level of security, both for the nodes and the communication stream	14. A communication solution with a high level of security, both for the nodes and the communication stream
15. There should be not great extra costs after the initial cost. There is an acceptance for system development costs, but the individual client computers must not be much more expensive than standard laptops (e.g. at most SEK 10000 extra) ant not very much more cumbersome to administrate.	The customer	A communication system that is relatively cheap	In international cooperation	Abroad	For the communication system to be used enough	By using standard components (COTS)	15. A communication solution with a price comparable to an expensive laptop

Table 1: VCT derived from end user interview

3.1.2 Hierarchy diagram

The needs in Table 1 above have been reworked and restructured. This has resulted in that needs have been joined, rephrased and some new, less specific needs have been added. The result of this work is shown in the hierarchy diagram in Figure 1 below.

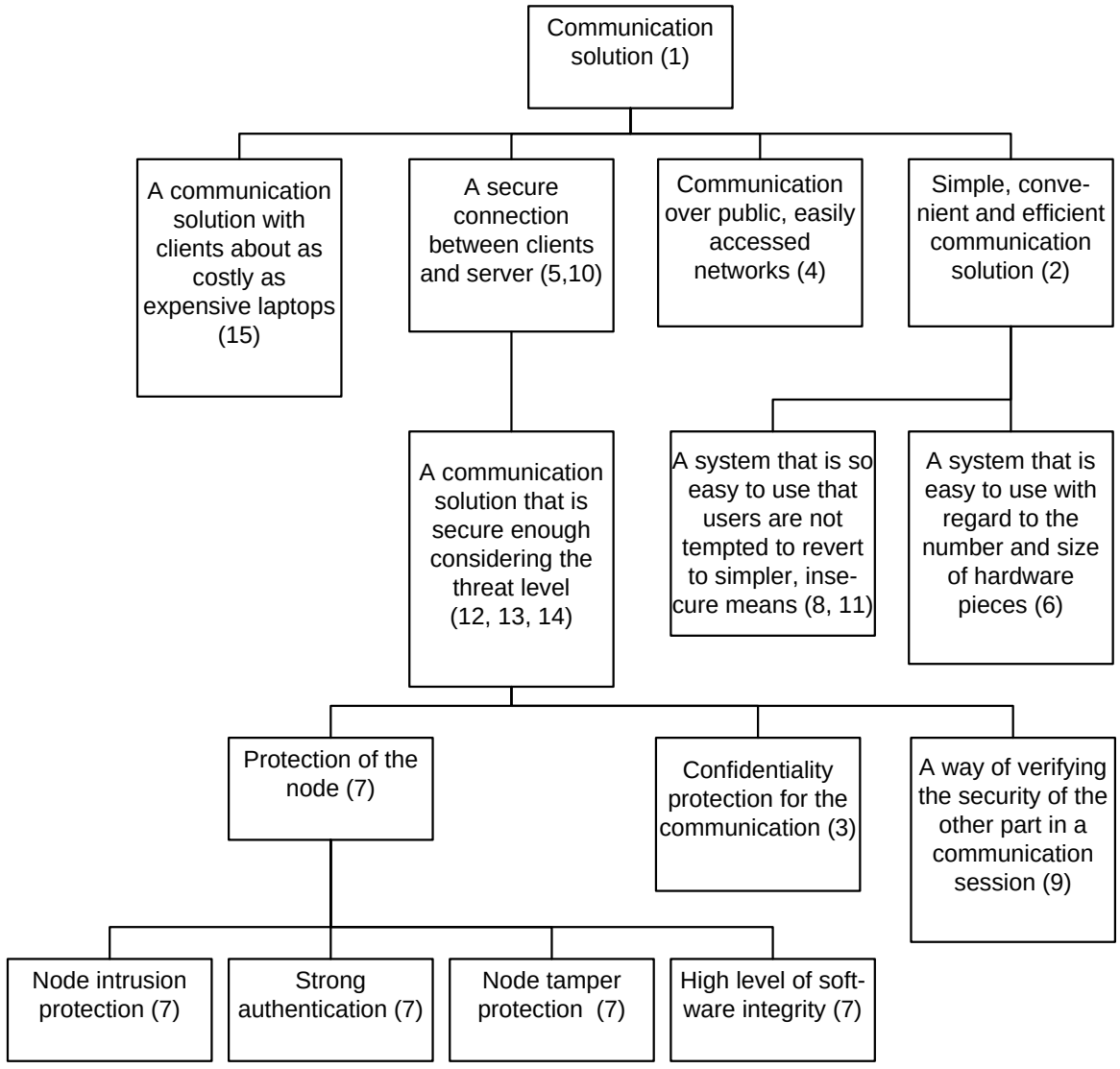

Figure 1: Hierarchy diagram.

3.2 Requirements

Finally, in Table 2 below we formulate requirements corresponding to the needs identified in the previous steps.

Need	Requirements
A communication solution with a price comparable to an expensive laptop (15)	The main part of the hardware in the system shall be COTS (15)
	The client hardware shall be COTS (15)
	The main part of the software in the system shall be COTS (15)
	To build a client must not be cost dominating (15)
	Client administration must not be cost dominating (15)

Need	Requirements
Communication is to be done over a publicly available, easily accessed network (4)	It shall be possible to use the Internet for the communication stream (4) Communication shall be possible over mobile broadband (4) Communication shall be possible over WiFi (4)
A system that is so easy to use that the users are not tempted to revert so simpler, insecure means of communication (8, 11)	A short training session shall be enough for a user to correctly handle the system (8, 11) It shall be possible to transfer documents to and from the user's communication software (8, 11) Starting the client and its communication software shall be quick enough not to discourage from using them (8, 11) The client communication software shall have a user interface that is orderly and logical (8, 11) The client communication software shall be designed by a person with knowledge of, and interest in, usability (8, 11) The client communication software shall require little interaction with the user (8, 11)
A system that is easy to use with regard to the size and number of hardware devices (6)	The communication client shall either be run in the user's work laptop, or in a physically small hardware device(6) Any hardware in excess of the client hardware, shall be very small (6)
Confidentiality protection for the communication stream (3)	The communication stream shall be encrypted with a strong cryptographic algorithm, except in parts of the client or server that are logically secure (3) The software treating the unprotected communication stream shall be carefully reviewed and be without known defects (3) The clients shall have some function for verifying and/or protect the integrity of the parts of the software treating the unprotected communication stream (3, 7) The communication protocol shall be designed to prevent man-in-the-middle attacks (3)
A way of verifying the security of the other part in a communication session (9)	When two nodes negotiate to establish a communication session there shall be a method for verifying integrity and version of the other part's soft- and hardware (9) When a node negotiates with another node, no communication session shall be established if the integrity of the other part cannot be verified, nor if the other part's soft- or hardware version cannot be considered secure (9)

Need	Requirements
Node intrusion prevention (7)	Software and data at the communication system clients shall be encrypted with a strong cryptographic algorithm when they are not used or under the supervision of a trusted person (7)
	The communication system nodes (both server and clients) shall use operation systems and programs especially designed and configured for security (7)
	The communication system nodes (both server and clients) shall have as few services, programs and functions as possible installed and active (7)
	The communication system nodes (both server and clients) shall have protection against malicious software (7)
Strong authentication (7)	To be able to use the clients in the communication system it shall be required both password/passphrase and a tamper protected physical object cryptographically authenticated by the client (7)
	Before a communication session is established, the identity of the node of the other part shall be verified using cryptographic mechanisms (3, 7, 9)
Node tamper protection (7)	The client hardware shall be designed so that it cannot be physically opened using standard tools without it being easily detectable afterwards (7)
	The client hardware shall be designed so that it cannot be physically modified using standard tools without it being easily detectable afterwards (7)
High level of node software integrity (7)	The clients shall have some function for verifying and/or protect the integrity of the parts of the software treating the unprotected communication stream (3, 7)

Table 2: Requirements list

4 Trust establishment for Cross-organizational Crises Management

This chapter describes the identified needs and requirements for the Aries WP3 "Trust Establishment for Cross-organizational Crises Management". The scenario is further described in Appendix 2 and gives a background that is beneficial for understanding this chapter.

For the requirements process we have in principle followed the methodology described in [4]. The process consists of the following steps:

1. collect data
2. identify statements
3. determine needs
4. analyze needs
5. determine architecture-driving requirements
6. analyze architecture-driving requirements

The first step, data collection, is typically done through interviews, workshops, or document studies. As we do not have direct connection to end-users for the chosen scenario, we have purely based this part on documents. This is not any major problem as there already are substantial relevant requirements work performed in the related Euler project [5]. We have used requirement [6] and design [7] documents from that project as primary data sources and we do not specifically document that process step in this report. Furthermore, we have merged steps 2 and 3, the result is summarized in Voice of the Customer Tables (VCT) in Section 4.1.1. Next, we have analyzed the identified needs, the results are summarized in the hierarchy diagram in Section 4.1.2. Finally, we have determined and sorted the architecture driving requirements based on the previously identified needs. The results are summarized in Section 4.2. This work has to a large extend been a rather straightforward process as we already had good requirements input from the Euler project documented in [6].

4.1 Needs

4.1.1 Voice of the customer table

In Table 2 below, we have extracted statements based on the security analysis performed in [7]. In particular the threat analyses, with respect to the following two threats, are relevant for the scenario we are considering:

- Threats on interacting heterogeneous wireless communication systems in a crises area,
- Threats on SDR as programmable and re-configurable radio system.

The results from the primary source document are *mainly* obtained through threat analysis and do not identify *need* per se. However, these threats can be formulated in terms on needs which we have done.

Statement	Who	What	When	Where	Why	How	Need
1.1 Security is critical to public safety radio because failures such as successful attacks on radio functionality or compromise of information could gravely impact the lives of public safety users and the people they serve	PSCD users	Incident system	When in use	In the field	Critical for rescuing human lives	Secure system design	Robust and secure system design that will provide trustworthy incident information to the end users
1.2 Fear of unauthorized use of application and network services	PSCD user, NIB manager as well as JAN manager	PSCD, NIB	When a PSCD device gets loss or system left unprotected	In the field	Insecure system design	System under attack	Secure access control and authentication mechanism on PSCD and NIB units
1.3 Fear of unauthorized modification of software	PSCD user, NIB manager as well as JAN manager	PSCD, NIB	When downloading software for reconfiguring PSCD or NIB	Anywhere	Insecure system design	System under attack	Secure software installation and upgrade routines on PSCD and NIB devices
1.4 Fear of malfunctioning radio equipment	PSCD user and NIB manager	NIB	When downloading software for reconfiguring NIB	Anywhere	Insecure system design	System under attack	Secure software installation and upgrade routines on NIB devices
1.5 Fear of SDR NIB compromise through scripted attacks	NIB manager	NIB	At any NIB software installation or change	Anywhere	Insecure system design	System under attack	Secure NIB software execution environment
1.6 Fear of SDR NIB compromise through usage of unlicensed/unsupporte	NIB manager	NIB	At any NIB software installation	Anywhere	Insecure system design	Bad software control	Strict control of NIB software installation and usage

Statement	Who	What	When	Where	Why	How	Need
d OS and software			or change			routines	
1.7 We need protection against attacks that replace legal NIB software payload at software upgrade	NIB manager	NIB	At NIB software upgrade	At software upgrade	Insecure system design	Software upgrade routines under attack	Secure NIB software upgrade routines
1.8 Fear of downloading invalid NIB software updates	NIB manager	NIB	At NIB software upgrade	At software upgrade	Bad software upgrade routines	Availability of bad software upgrade packages	Secure NIB software upgrade routines
1.9 Fear of bugs in NIB software	NIB manager	NIB	Any time	Anywhere	Insecure system design	Bad software development process	Strict verification of approved NIB software such as formal verification/evaluation of NIB software
1.10 Fear of NIB hardware tampering	NIB manager	NIB	When NIB is left unprotected	Anywhere	Insecure NIB hardware design	NIB hardware under attack	Tamper resistant NIB hardware design
1.11 The NIB node implementation must ensure that only necessary and authorized communications flow from one domain to the other.	NIB manager	NIB	When connecting two different IANs	Anywhere	In order to protect IAN internal information	Sound NIB authentication, authorization and access control mechanism in place	The NIB node implementation must ensure that only necessary and authorized communications flow from one domain to the other
1.12 All the communications strictly internal to the IAN, and all the databases stored in the NIB section of the node, must be kept away from prying eyes accessing the node via the Euler waveform, or from SW modules installed on the node, unless	NIB manager	NIB	When connecting two different IANs	Anywhere	In order to protect IAN internal information	Sound NIB authentication, authorization and access control mechanism in place	The NIB software integrity must always be kept both at configuration and run time. The NIB must implement and enforce IAN to external IAN security policies. The NIB must perform the necessary authentication and trust verification of

Statement	Who	What	When	Where	Why	How	Need
duly authorized							connecting NIBs from other IANs.
1.13 Develop a policy driven configuration framework for SDR that : - download policies on the fly - verifies their certification - parses, compiles and loads the policies - activates the desired radio device - provide attestation of its configuration to service providers	JAN manager	NIB	At NIB software update	Anywhere	Prevent compromised NIB SDR		NIB SDR policy framework: - download policies on the fly - verifies their certification - parses, compiles and loads the policies - activates the desired radio device - provide attestation of its configuration to service providers
1.14 Certify authenticity of configuration software and validity of the configuration to an external entity : - Prevent loading, installation, instantiation of unauthorized software - Verify downloaded software from trusted vendor - Ensure confidentiality and integrity of over-the-air software download and stored data - Ensure the terminal operates within allowed frequency bands	JAN manager	NIB	At NIB software update	Anywhere	Prevent compromised NIB SDR		Strict control over NIB SDR software installation, boot and upgrade procedure: - Prevent loading, installation, instantiation of unauthorized software - Verify downloaded software from trusted vendor - Ensure confidentiality and integrity of over-the-air software download and stored data - Ensure the terminal operates within allowed frequency bands

Statement	Who	What	When	Where	Why	How	Need
and power levels specified by local regulators							and power levels specified by local regulators
1.15 Identify and authorize SDR users, i.e., use a voice authentication application that identifies and authorizes SDR users, allowing specific radio capabilities to be unlocked depending on the user. For example, a software defined radio for emergency response with a voice authentication application and security profiles enabling an identifier response commander to use the radio to communicate on a number of private bands reserved for responding teams—police, fire, medical, etc.	NIB users	Voice based authentication of NIB user	When using NIB SDR modules	Anywhere	User authentication	Voice authentication mechanisms	NIB voice authentication mechanisms that control radio capabilities based on NIB SDR policy settings.
1.16 System security requirements on confidentiality protection on: - Owner /user /equipment information e.g., Identity and physical position. - Cryptographic data (Keys, passwords, PINs and access codes)	All users	Data are not exposed to unauthorized users during the transition or in a database	Always	Anywhere	Exposure of sensitive information and data can affect the emergency operations	Data shall be kept confidential	Confidentiality protection of: - Owner /user /equipment information e.g., Identity and physical position. - Cryptographic data (Keys, passwords, PINs and access codes)
1.17 Integrity protection of:	All users	Data are not modified	Always	Anywhere	Modified or corrupted	Data shall be protected	Integrity protection of:

Statement	Who	What	When	Where	Why	How	Need
- User traffic - Network Control and management data - Radio control data - Configuration data for SDR (platform and SDR Waveforms) - Cryptographic data (Keys, passwords, PINs and access codes) - Security policies for SDR platform - SDR waveforms and user roles login data - SDR platform SW including cryptographic algorithms and parameters - SDR platform hw including cryptographic modules		or corrupted during the transition or directly in the database			data can affect the emergency operations	against unauthorized modification	- User traffic - Network Control and management data - Radio control data - Configuration data for SDR (platform and SDR Waveforms) - Cryptographic data (Keys, passwords, PINs and access codes) - Security policies for SDR platform - SDR waveforms and user roles login data - SDR platform SW including cryptographic algorithms and parameters - SDR platform HW including cryptographic modules
1.18 It shall be possible for an authorized NIB manager to set SDR platform parameters. After loading the configuration parameter set(s) shall be checked by the radio for integrity and authenticity and for	NIB manager	Configuring the SDR devices and check the authenticity of configurations	Always	Before and during the emergency operation	Unauthorized user shall not be able to change the configurations.	By limiting configuration to authorized users, verifying the authenticity and integrity	It shall be possible for an authorized NIB manager to set SDR platform parameters. After loading the configuration parameter set(s) shall be checked by the radio for integrity and

Statement	Who	What	When	Where	Why	How	Need
compatibility. A failed integrity and authenticity check shall cause rejection of the configuration parameter set(s). The result of an integrity and authenticity check for received configuration parameter set(s) shall be an auditable event.						of changes and keeping trace of applied modifications.	authenticity and for compatibility. A failed integrity and authenticity check shall cause rejection of the configuration parameter set(s). The result of an integrity and authenticity check for received configuration parameter set(s) shall be an auditable event.

Table 2: VCT derived from [7].

Table 3 summarizes the needs identified from the requirements analysis done by the Euler project [6]. Similar to our activity, the Euler project has derived functional requirements for a *broader* scenario than the one we are analyzing. Furthermore, the focus has not been on security, which implies that a rather limited set of security requirements have been defined and those are on a very high level. Consequently, they provide a valuable input to our activity, but need to be complemented with more detailed requirements that is the result of our in depth analysis of the needs identified in Table 2 and Table 3.

Statement	Who	What	When	Where	Why	How	Need
2.1 The fear of inappropriate or insufficient level of protection on sensitive data, transmitted between all organizations involved in emergency communications	Originator of data	Sufficient level of protection	Specifying the level of protections for transit data	Anywhere	The same level of protection shall be provided	Ensuring the same level of protection when transmitting data	For all emergency communication, the organizations involved have to make sure that data is protected according to its sensitivity level during transmission, processing and storage and that access to communication channels and critical systems is only granted to authorized persons.

Statement	Who	What	When	Where	Why	How	Need
2.2 The concerns regarding degradation of performance caused by conflicts between each individual or national jurisdiction security requirements and other nation's requirements.	Network end-users	Incompatibility between security requirements	During communications	Anywhere	Same level of performance shall be ensured	Expandability of security requirements	The basic security platforms should be capable of being expanded and enhanced to meet each jurisdiction and nation's individual requirements without degradation to overall system performance.
2.3 The concerns regarding unavailability of network resources for special users who need more resources under specific circumstances and conditions.	Network prioritized users	Prioritization when using resources	Communication under specific conditions	Anywhere	Availability of resources in emergency situation	Possibility for prioritizing access to resources	Access to the network shall be controlled by using functionalities such as assigning priority to potential users, thereby restricting some parties from access to the network under certain circumstances.

Table 3: VCT derived from [6].

In addition to the requirements derived from the Euler documents, we have made an own analysis of the scenario described in Appendix 2. This analysis resulted in a set of additional statements and needs, which are summarized in the table below.

Statement	Who	What	When	Where	Why	How	Need
3.1 When two NIBs from different organizations are connected on the field, it must be possible for the NIB to securely authenticate connecting NIB.	NIB manager	NIB node	Two different IANs are connected	Anywhere	Prevent unauthorized IAN access	Secure authentication	When two NIBs from different organizations are connected on the field, it must be possible for the NIB to securely authenticate the connecting NIB.
3.2 When two NIBs from different organizations are	NIB manager	NIB node	Two different IANs are connected	Anywhere	Prevent malicious NIB to connect to	Check of connecting NIB software/	When two NIBs from different organizations are connected on the

Statement	Who	What	When	Where	Why	How	Need
connected on the field, it must be possible to verify that the connecting NIB is in a trustworthy state prior to giving it access to the IAN.					IAN	hardware states and configurations	field, it must be possible to verify that the connecting NIB is in a trustworthy state prior to giving it access to the IAN.
3.3 When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to securely authenticate connecting PSCD.	NIB manager	PSCD node	Roaming PSCD	Anywhere	Prevent unauthorized IAN access	Secure authentication	When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to securely authenticate connecting PSCD.
3.4 When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN, to verify that the connecting PSCD is in a trustworthy state prior to giving access to the IAN.	NIB manager	NIB node	Roaming PSCD	Anywhere	Prevent malicious PSCD to connect to IAN	Check of connecting NIB software/ hardware states and configurations	When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN, to verify that the connecting PSCD is in a trustworthy state prior to giving access to the IAN.
3.5 When two NIBs from different organizations are connected on the field, it must be possible for the NIB to securely verify the detailed security policies that apply for the connecting IAN and provide access based on the policies.	NIB manager	NIB node	Two different IANs are connected	Anywhere	Prevent unauthorized access to sensitive IAN information	Check of connecting NIB security policies	When two NIBs from different organizations are connected on the field, it must be possible for the NIB to securely verify the detailed security policies that apply for the connecting IAN and provide access based on the policies.
3.6 After two NIB are connected on the field, the security policies that apply for the connecting IAN	NIB Manager	NIB node	Two different IANs are connected	Anywhere	Prevent unauthorized load and modification of	Secure update of security policies	After two NIB are connected on the field, the security policies that apply for the connecting IAN can be

Statement	Who	What	When	Where	Why	How	Need
can be updated and changed securely.					policies.		updated and changed securely.
3.7 When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to securely verify the detailed security policies that apply for the connecting PSCD and provide access based on the policies.	NIB manager	NIB node	Roaming PSCD	Anywhere	Prevent unauthorized access to sensitive IAN information	Check of connecting PSCD security policies	When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to securely verify the detailed security policies that apply for the connecting PSCD and provide access based on the policies.

Table 4: Statements derived from the scenario described in Appendix 2.

4.1.2 Hierarchy diagram

Figure 1 shows the hierarchy diagram we have derived from the voice of the customer tables in Section 4.1.1.

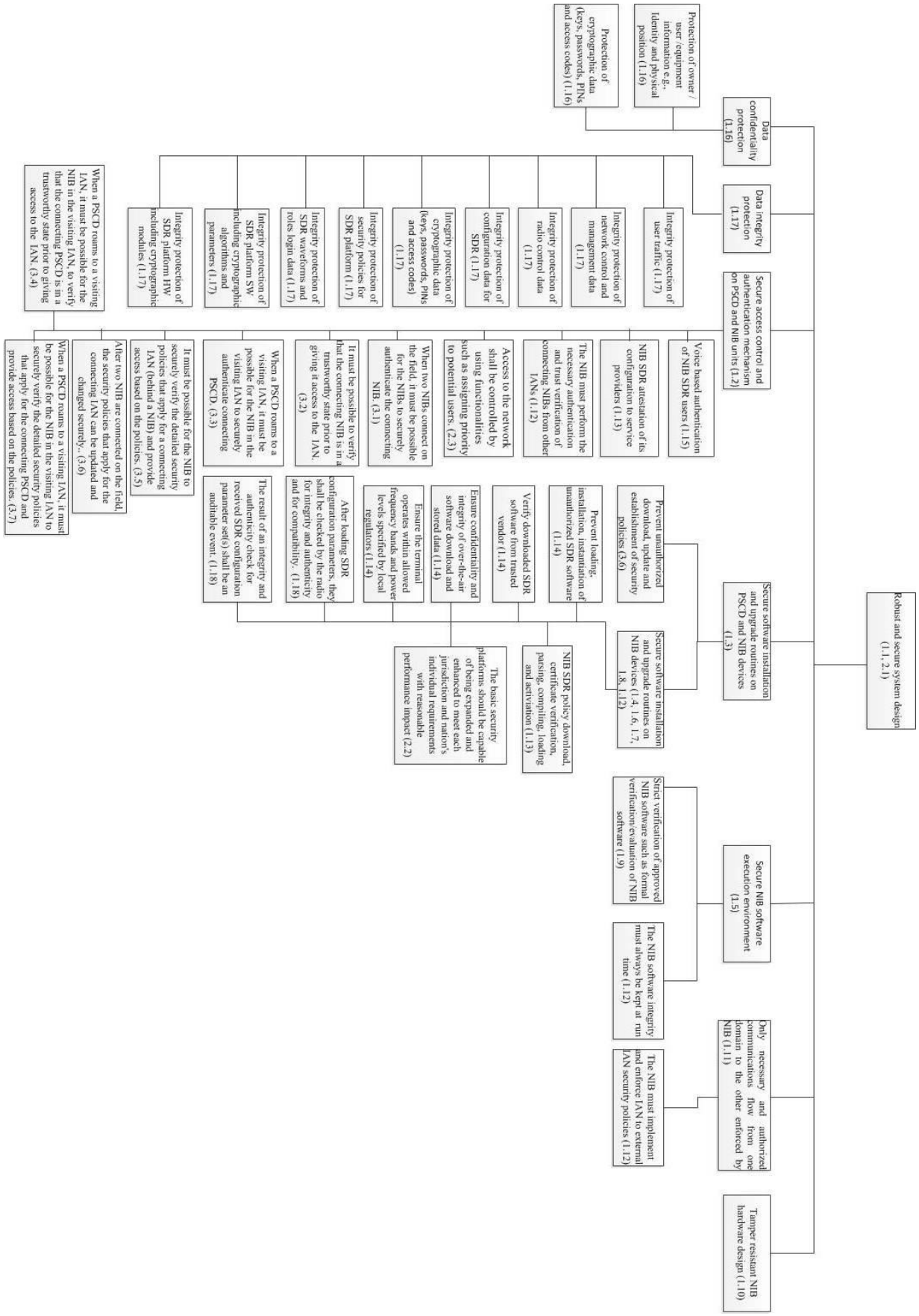

Figure 2: Hierarchy diagram.

4.2 Requirements

Finally, we map the needs *and* requirements identified in the previous steps into a table that summarize the architecture driving requirements. The document we started from already had a fairly detailed level with several requirements identified. Hence, we have been able to directly map most of the needs and requirements from the source documents into architecture driving requirements.

Needs	Requirements
Protection of owner /user /equipment information e.g., Identity and physical position (1.16)	A.1 The NIB and PSCD shall provide confidentiality protection of owner information at storage and at transfer. A.2 The NIB and PSCD shall provide confidentiality protection of user information at storage and at transfer. A.3 The NIB and PSCD shall provide confidentiality protection of equipment information at storage and at transfer.
Protection of cryptographic data (keys, passwords, PINs and access codes) (1.16)	A.4 The NIB and PSCD shall provide confidentiality protection of all kinds of cryptographic data at storage and at transfer.
Integrity protection of user traffic (1.17)	B.1 The NIB and PSCD shall provide Integrity protection of user traffic.
Integrity protection of network control and management data (1.17)	B.2 The NIB and PSCD shall provide integrity protection of network control and management data.
Integrity protection of radio control data (1.17)	B.3 The NIB and PSCD shall provide integrity protection of radio control data.
Integrity protection of configuration data for SDR (1.17)	B.4 The NIB shall provide integrity protection of configuration data for SDR at storage and at transfer.
Integrity protection of cryptographic data (keys, passwords, PINs and access codes) (1.17)	B.5 The NIB and PSCD shall provide integrity protection of all kinds of cryptographic data at storage and at transfer.
Integrity protection of security policies for SDR platform (1.17	B.6 The NIB shall provide integrity protection of security policies for SDR platform at storage and at transfer.
Integrity protection of SDR waveforms and roles login data (1.17)	B.7 The NIB shall provide integrity protection of SDR waveforms and roles login data at storage and at transfer.
Integrity protection of SDR platform SW including cryptographic algorithms and parameters (1.17)	B.8 The NIB shall provide integrity protection of SDR platform SW including cryptographic algorithms and parameters at storage and at transfer.
Integrity protection of SDR platform HW including cryptographic modules (1.17)	B.9 The NIB shall provide integrity protection of SDR platform HW including cryptographic modules.
Voice based authentication of NIB SDR users (1.15)	C.1 The NIB shall support voice based authentication

Needs	Requirements
	of NIB SDR users.
NIB SDR attestation of its configuration to service providers (1.13)	C.2 The NIB shall support SDR attestation of its configuration to service providers.
The NIB must perform the necessary authentication and trust verification of connecting NIBs from other IANs (1.12)	C.3The NIB shall authenticate and verify the trustworthiness of connecting NIBs from other IANs.
Access to the network shall be controlled by using functionalities such as assigning priority to potential users. (2.3)	C.4 The NIB shall support role based access control to the IAN services behind the NIB. C. 5. The NIB shall support assignment of differentiated service levels for connecting NIBs (from other IANs) and PSCDs.
When two NIBs connect on the field, it must be possible for the NIBs to securely authenticate the connecting NIB. (3.1)	C.6 The NIB shall support strong authentication of all connecting NIBs from other IANs.
It must be possible to verify that the connecting NIB is in a trustworthy state prior to giving it access to the IAN. (3.2)	C.7 It must be possible to verify that the connecting NIB is in a trustworthy state prior to giving it access to the IAN.
When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to securely authenticate connecting PSCD. (3.3)	C.8 When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to authenticate the connecting PSCD using strong authentication.
When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN, to verify that the connecting PSCD is in a trustworthy state prior to giving access to the IAN. (3.4)	C.8 When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN, to verify that the connecting PSCD is in a trustworthy state prior to giving access to the IAN.
It must be possible for the NIB to securely verify the detailed security policies that apply for a connecting IAN (behind a NIB) and provide access based on the policies. (3.5)	C.9 It must be possible for the NIB to securely verify the detailed security policies that apply for a connecting IAN (behind a NIB) and provide access based on the policies.
The NIB must be able to update and enforce IAN security policies (3.6)	C.10 The NIB shall prevent unauthorized loading of security policies. C.11 The NIB shall prevent unauthorized establishment of security policies. C.12 The NIB shall securely verify that all security policies are originated from a trusted party. C.13 The NIB shall ensure the integrity of over-the-air download and stored security policies. C.14 The NIB shall check the integrity of loaded security policies. C.15 The NIB shall check the compatibility of loaded security policies with local policies. C.16 The NIB shall log the results of all integrity and

Needs	Requirements
	authenticity checks for received security policies.
When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to securely verify the detailed security policies that apply for the connecting PSCD and provide access based on the policies. (3.7)	C.17 When a PSCD roams to a visiting IAN, it must be possible for the NIB in the visiting IAN to securely verify the detailed security policies that apply for the connecting PSCD and provide access based on the policies.
Prevent loading, installation, instantiation of unauthorized SDR software (1.14)	D.1 The NIB shall prevent any loading of unauthorized SDR software. D.2 The NIB shall prevent any installation of unauthorized SDR software. D.3 The NIB shall prevent any instantiation of unauthorized SDR software.
Verify downloaded SDR software from trusted vendor (1.14)	D.4 The NIB shall securely verify that all downloaded SDR software origin from a trusted vendor.
Ensure confidentiality and integrity of over-the-air software download and stored data (1.14)	D.5 The NIB and PSCD shall ensure confidentiality and integrity of over-the-air software download and stored data. (Detailed requirements: A.1-A.3 and B.1-B.9)[1].
Ensure the terminal operates within allowed frequency bands and power levels specified by local regulators (1.14)	D.6 The NIB shall verify that it operates within allowed frequency bands and power levels specified by local regulators.
After loading SDR configuration parameters, they shall be checked by the radio for integrity and authenticity and for compatibility. (1.18)	D.7 The NIB shall check the integrity of loaded SDR configuration parameters. D.8 The NIB shall check the authenticity of loaded SDR configuration parameters. D.9 The NIB shall check the compatibility of loaded SDR configuration parameters.
The result of an integrity and authenticity check for received SDR configuration parameter set(s) shall be an auditable event. (1.18)	D.10 The NIB shall log the results of all integrity and authenticity checks for received SDR configuration parameter set(s).
NIB SDR policy download, certificate verification, parsing, compiling, loading and activation (1.13)	D.11 The NIB shall support secure (integrity protected and authenticated) downloading of SDR polices. D.12 The NIB shall verify SDR certificates. D.13 The NIB shall be able to securely parse and compile SDR policies. D.14 The NIB shall be able to secure load and activate SDR policies.
The basic security platforms should be capable of	D.15 The NIB shall be able to handle nation specific

[1] This requirement is maybe too general to fit at this level but anyway indicate important requirements on software installation and is included for completeness.

Needs	Requirements
being expanded and enhanced to meet each jurisdiction and nation's individual requirements with reasonable performance impact (2.2).	SDR policies. D.16 The NIB shall be able to handle nation specific SDR policies with small performance penalties.[2]
Strict verification of approved NIB software such as formal verification/evaluation of NIB software (1.9)	E.1 Preferably, the NIB shall only run software subject to formal verification.
The NIB software integrity must always be kept at run time (1.12)	E.2 The NIB shall implement means to ensure the NIB software integrity at run time.
The NIB must implement and enforce IAN to external IAN security policies (1.12)	F.1 The NIB shall implement a policy enforcement engine that prevents any information flows that contradicts the agreed security policies between IANs.
Tamper resistant NIB hardware design (1.10)	H.1 The NIB should be implemented using tamper resistant hardware design.

Table 5: Identified architecture driving requirements.

[2] This is hardly a security requirement and should be considered to be removed from the requirements lists.

5 Discussion

In this report, a detailed security requirements analysis has been performed for *two different* usage scenarios. These two scenarios were chosen based on the current needs of stakeholders, with the aim of having a sound basis for the research issues we expect to tackle at the next project phase. The selected use cases are rather different in their respective set-ups and introduced roles. Anyhow, they have rather many, technical requirements in common. Below, we summarize the main commonalities and differences and discuss directions for the future work in WP3 based on this analysis.

5.1 Common requirements

5.1.1 Communication security

In both scenarios, communication over unsecure channels is needed. This implies basic integrity and confidentiality protection requirements on the communication channels as well as authentication of communication end-points. The first scenario, usage of COTS, does not imply any new challenges in this respect as it is a traditional client server model. The second scenario, the incident network scenario, is a bit demanding as it involves more end-points and entities from several organizations.

Even if communication security is important, we do not expect to spend much time on working with solutions that fulfill these requirements except when they have connection to platform security requirements as those are the most challenging and interesting issues from a research perspective.

5.1.2 Node security

Both analyses have identified security requirements on the involved nodes. While there are equal emphasis on node intrusion protection and node integrity in the requirements from the first scenario, the second scenario have much broader set of requirements with specific requirement on software upgrade and in particular secure policy handling in the nodes. However, especially on the node integrity there are requirements in common that can form the basis for common solutions in the future as well.

5.2 Major differences

The incident network scenario involves SDR units with high security requirement on the radio definition software. These types of requirements are obviously not present in the COTS usage scenario. However, when detailing out trust based security architecture for *both* scenarios working with in depth technology analysis, we will probably see that particular mechanisms with respect to software management could be applied to both scenarios.

In the first scenario, several high level usability and simplicity requirements have been identified. These are general and should in principle also apply to the second scenario even if no such requirements have been identified in the requirements process.

The requirements from the analysis of the incident network scenarios related to cross-organizational co-operation do not appear in the first scenario. However, actually they could be useful for a more general COTS usage scenario where information is shared between several different organizations.

5.3 Suggestions for next project phase

During the next phase of the project, we will work with defining a security architecture that meets at least a selected subset of the identified security requirements. The focus will be on the requirements related to node security, software and policy integrity and platform verification. This implies that we will spend less time on the pure communication security issues. We also expect to give a rather broad overview of state-of-the art technology in the area of trusted computing and secure software management.

6 References

[1] D. Gollmann, *Computer security*, 2nd ed. Chichester: Wiley, 2006.

[2] Encyclopædia Britannica, "Information system," in *Encyclopædia Britannica Online*, 2011.

[3] I. Sommerville and P. Sawyer, *Requirements Engineering: A Good Practice Guide*. Wiley, 1997.

[4] N. Hallberg, R. Andersson, and L. Westerdahl, *Quality-driven process for requirements elicitation: the case of architecture driving requirements*. Linköping, Sweden: Swedish Defence Research Agency, FOI, 2005, p. 12.

[5] "The Euler project." [Online]. Available: http://www.euler-project.eu/.

[6] Euler project, *Deliverable 2.3, End-users requirements, Version 1.1*. 2010.

[7] Euler project, *Deliverable 3.2, General Design, Version 1.0*. 2009.

Appendix 1: ARIES WP3 – Scenario Input: Trusted Communication using COTS

Jonas Hallberg
FOI

Jacob Löfvenberg
FOI

Abbreviations

COTS	Commercial Off-The-Shelf, ready-made products for sale to the general public
IP	Internet Protocol
VPN	Virtual Private Network

Contents

1 Introduction

Secure communications are required in many applications, by individuals as well as by organizations. The level of trust required in the security of the communication varies depending on the users and the setting. An individual living a normal life will probably be satisfied with a lower security and trust level than an organization communicating information that is of great commercial value. In civilian applications communication has traditionally been kept secure by using means of communication for which interception requires physical access, and this access has been prohibited by physical protection and legislation. When this level of protection has not been enough people have had to meet in person.

New communication technology has given rise to new means and methods for communication, foremost of which is the Internet, and IP based communication in general. When communication is based on IP, and certainly on the Internet, the user has little knowledge of the route taken by the information flow. This means that the physical protection of the information infrastructure yields little trust in the security. No single entity has control of all nodes that could possibly be part of the route between the communicating parties, so nobody can tell if the route is secure.

The move from analog to digital transmission and processing has also change the security situation. Unauthorized interaction with analog equipment often requires physical access in combination with complicated and expensive equipment. For unauthorized interaction with digital equipment it often suffices with software tools operated at a (possibly global) distance. They may still be complicated, but they are often very cheap, or even free of charge.

For the above mentioned reasons there is a need for technology securing digital communications. Such technologies exist, both commercially and non-commercially, in the form of cryptographic algorithms used in tools for encrypted communication. In many cases such tools are implemented in software and run on a personal computer. If the implementation is carefully made and without serious bugs, such a communication tool can be secure. However, a problem with running a security application on an ordinary personal computer is that the behavior of the security application may be influenced by other applications running on the same computer. It may be unfortunate interactions with other applications that are otherwise correct, it may be ordinary malware or it may even be an attack by a piece of software aimed at this specific user and security application.

In view of this our opinion is that that to reach a high level of trust in a secure communication tool implemented on a personal computer, a security mechanism is needed to guarantee the integrity of the platform. In some way it must also be possible to communicate this guarantee to the other parties in the communication, so that it can be verified and mutual trust can be established. By using a custom made, dedicated platform for any security applications it is possible to reach very high levels of trust, but in all but the most security focused situations this is far to expensive.

In this report, we present a scenario which we call “Trusted communication using COTS”. This scenario is one of *two* chosen scenarios that will serve as basis for the requirements analysis we will perform in the ARIES WP3. The requirements derivation will be done in three steps:

1. Detailed scenario descriptions (this document)
2. Identifications of needs based on the chosen scenarios
3. Mapping of the needs into requirements

2 Scenario description

2.1 Basic scenario

The situation we consider is the communication between a number of users in an organization called Enjeel, requiring a high level of security, and trust in the platform implementing the secure communication. Due to the mobility of the users, communication over the Internet is deemed to be the only viable solution, especially since they require video conferencing and possibility for file exchange in addition to voice communication. For the communication solution to be economically feasible it has to be implemented using standard components, COTS.

The communication platform of choice is a normal laptop computer. Each user will be given such a computer, equipped with communication software. It is desirable that the computers will also be available for other, non-security related software. Communication between parties is done through an intermediary in the form of an Internet-connected server that resides under the control of the users' organization.

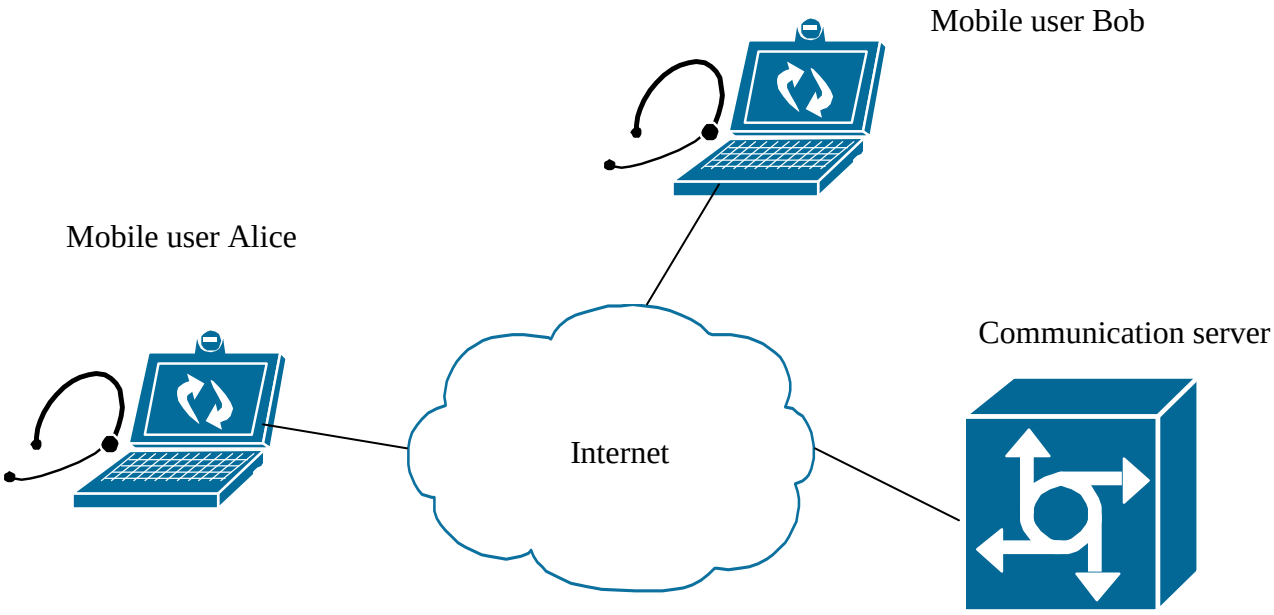

Figure 3: Communication between two parties using a central server.

There is a third party, Eve, who is interested in listening in on the communication between Alice and Bob. Eve is a representative of a resourceful organization called Deamin, willing to invest both time and money in breaking the secure communication, and they are in no hurry. Enjeel has decided that a simple VPN connection, though secure enough in itself, is too susceptible to IT attacks against the mobile computers. Even if one user, say Alice, is very careful with her computer, she has no way of knowing that the user in the other end, say Bob, is in possession of

an uncompromised computer. Thus the Enjeel organization needs a way of ensuring the software integrity of the computers used for communication, and preferably a way for those computers to prove their integrity to connecting parties.

2.2 Network Scenario

A simple variation of the basic scenario is when one or more of the connected parties are replaced by local area networks in which there may be several users. The local area networks are not mobile but are a part of the infrastructure under the control of the Enjeel organisation. In such cases the computers of the users have some level of protection from the Internet since they are not directly exposed.

3 Actors

Within the described scenario there are the following actors (or roles):

- Users (Alice and Bob)
- Attacker (Eve)
- Server

3.1 Users

The users are the mobile parties with the need to communicate. Any user may want to communicate with the server, another user or a group of other users. The users are assumed to be experienced computer users, but not IT experts or security professionals. They are assumed to understand the need for security, but to have a limited acceptance for inconvenience due to security measures. Any security solutions will have to incorporate a reasonable level of usability.

3.2 Attacker

The attacker is an agent of an organization wanting information from the organization of the users. In contrast to the users, the attacker is a highly trained expert, willing to use large amounts of time and resources to acquire information from the users and their organization. The attacker is assumed to be willing to accept some risk of being caught using illegal methods for getting the information, but not to use overt or violent methods.

3.3 Server

The server is the hub of the secure communication. It is assumed to be physically secure, but since it is connected to the Internet it may be susceptible to network attacks. The server is handled by IT experts who also install and handle the computers of the users.

4 Scope and Limitations

The aim of the system for high-security communication is to support the confidentiality, integrity and availability of the communicated information. In order to achieve this, we are interested in upholding the integrity of the computers used for communication and in how to build and distribute trust about this to all the parties involved in the communication. This means that we need to measure the software state of the computers in a secure way in order to be able to trust the computers. This is related to software correctness in the sense that correctness is a prerequisite for trust to be possible. We will however not address issues regarding software development or verification in this project. Instead we focus on the problem of assuring and proving that the intended software, and nothing else, is loaded and running.

4.1 Research issues

Considering the scope and limitations described above, we will address the following research questions:

- What are the needs of the involved parties?
- What requirements should be fulfilled in order to address the identified needs?
- What level of trust can be established regarding the identity of entities reached over an open network?
- To what degree can hardware be trusted?
- How can trust in the integrity of software be established?
- What level of trust can be established without the use of expensive certification?

Appendix 2: ARIES WP3 – Scenario Input: Trust Establishment for Cross-organizational Crises Management

Christian Gehrmann
SICS

Mehran Ahsant
Saab Systems

Abbreviations

IAN	Incident Area Network
JAN	Jurisdiction Area Network
NIB	Network-in-a-Box
PSCD	Public Safety Communications Device
SDR	Software Defined Radio

Contents

1 Introduction

There is an increasing demand for improved communication infrastructures that can support efficient management in case of civil crises such as terror attacks, natural disasters, and large accidents etc., but also for surveillance at large public events and similar. The information systems for these applications have so far mainly been created on national level *and* with diverse systems for different authorities such as the army, the police force, fire brigades and ambulance services. As one currently see a strong need for closer co-operation between different authorities and between organizations in different countries, the old communication infrastructures must be upgraded and *interoperability* between systems is needed.

The road towards new communication infrastructures with good interoperability goes through usage of common interfaces on all levels spanning from the radio interfaces up to the application layer interfaces and data structures. There also exist several initiatives to make this happen. One such initiative is the European FP7 Euler project [1] that aims at creating fully programmable radios, Software Defined Radios (SDR), with standardized software interface. The ultimate goal in that project is to design a system architecture including radio waveform that allows not only interoperability between crises organizations on the fields but also software portability across platforms from different organizations and suppliers.

Interoperability and common software come at the prize of a higher security risk. Common interfaces can be utilized by hostile organizations or individuals to launch attacks against the infrastructures. Similar, flexibility in the form of SDR also open up against new software attacks that threaten to destroy the very core functionality in wireless crises networks for instance. This gives new research challenges on how to guarantee the security of the communication platforms as well as the communication itself. Without appropriate security mechanisms in place, we cannot achieve the confidence and *trust* in the new systems, this in turn, will prevent the introduction/usage of the new more flexible infrastructures.

In this report, we present a scenario we call “Trust establishment for cross-organizational crises management”. This scenario is one of *two* chosen scenarios that will serve as basis for the requirements analysis we will perform in the ARIES WP3. In all, the requirements derivation will be done in three steps:

1. Detailed scenario descriptions (this document)
2. Identifications of needs based on the chosen scenarios
3. Mapping of the needs into requirements

2 Scenario description

The situation we consider is the communication and collaboration between a collection of so-called Incident Area Networks (IANs), which are being deployed on the scene of a crisis as depicted in Figure 3. Each IAN is administered and owned by a public safety organization, and enables communications within this organization, in the area of the event. IANs may also use different waveforms for their internal communications.

A typical IAN consists of

- A vehicle-based "Network-In-a-Box" (NIB), i.e. a fully autonomous and transportable network infrastructure, with base station and all necessary network switching and control functions
- A fleet of user terminals, called Public Safety Communications Devices (PSCDs)

Optionally, this elementary IAN is also connected to the organizations permanent terrestrial infrastructure, which is called a Jurisdiction Area Network (JAN).

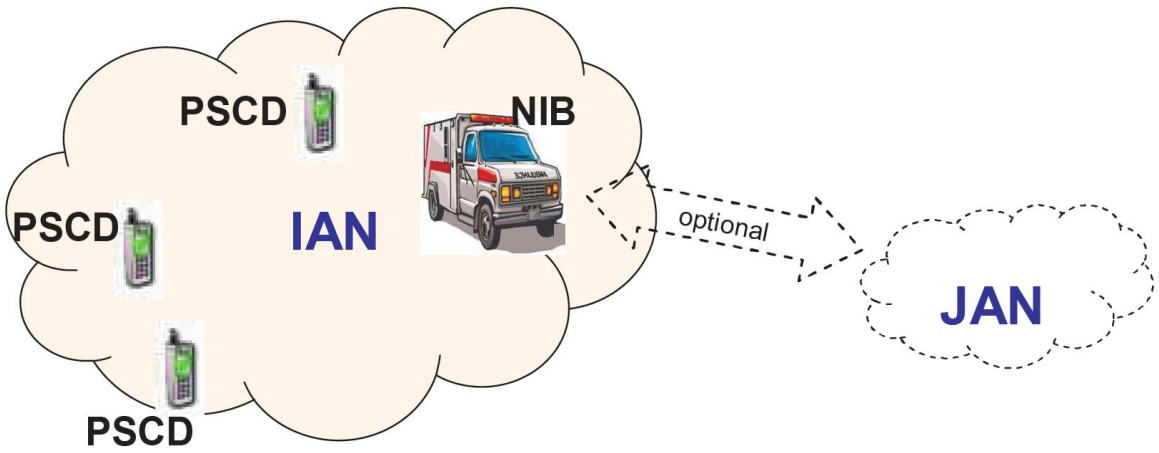

Figure 4: Incident Area Network.

The NIB communication platform might have several radio interfaces. One or several of these interfaces might be SDR based interfaces, which allows switching between all installed waveforms. There might be even a case that requires installing and using new or additional radio waveforms. That is, the SDR can be either pre-configured or updated and configured dynamically when needed.

The PSCD devices typically can only communicate with pre-defined radio and communication protocols.

In addition to the basic IAN scenario described above, we particularly consider two different cross-organizational roaming scenarios:

1. A team from one organization (IAN1) is co-operating at an incident area with a team from another organization (IAN2) and would like to allow connectivity and information exchange between the two organizations at the incident area, see Figure 5. These two organizations are potentially using different radio waveforms and if that is the case, the NIB in at least one of the two IANs must be re-configured to allow connectivity between the two NIBs in the system.
2. One or several people belonging to one crises management organization are working together with people (visiting) in an incident area from another organization and need to be able to share information and communicate with all other people within the hosting IAN, see Figure 6. Potentially, the visiting PSCD is an SDR units and needs to be reconfigured to allow communication with the NIB in the IAN or the NIB SDR is updated with an appropriate waveform and configuration to allow communication with the visiting PSCD.

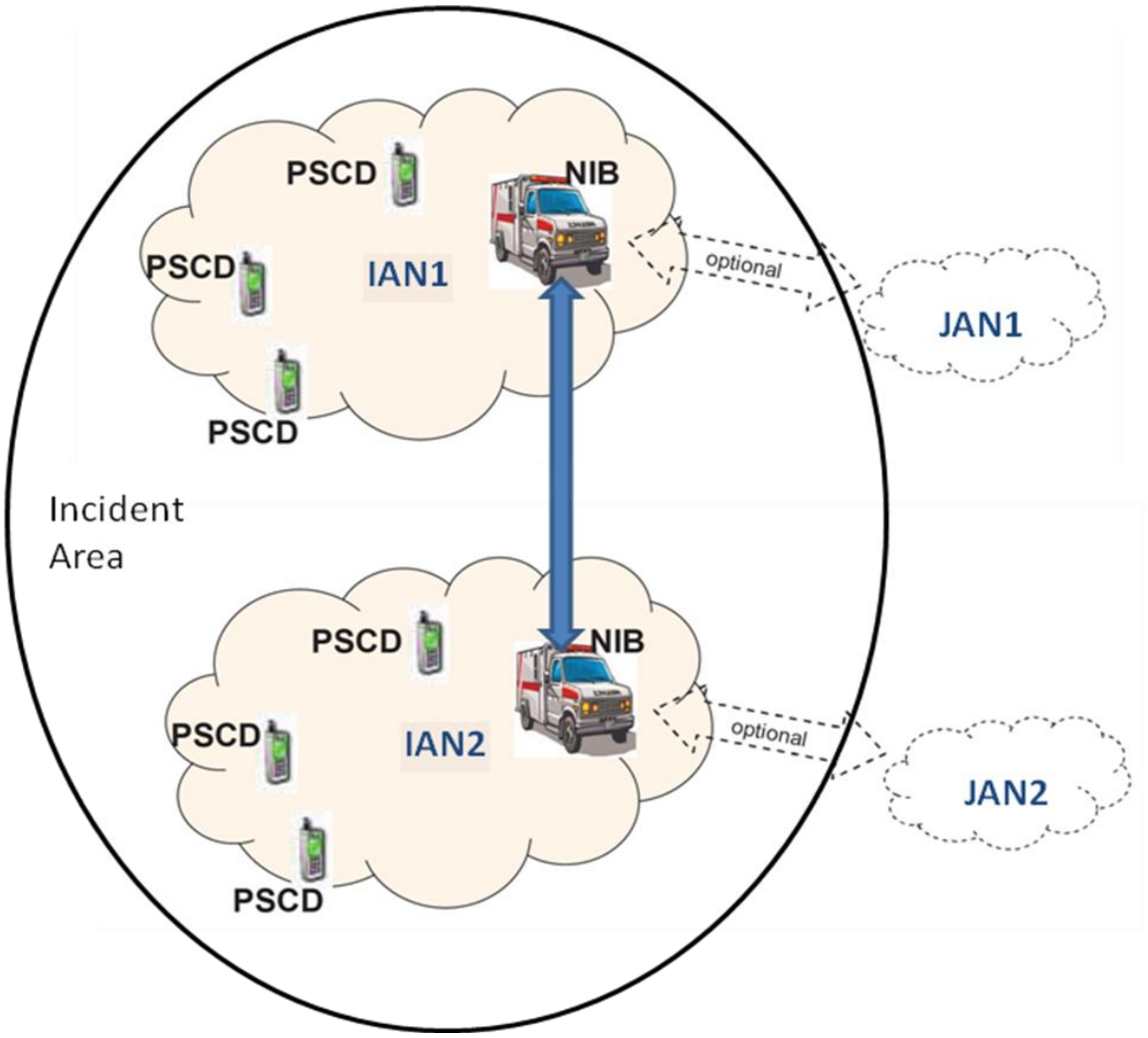

Figure 5: Cross-organizational co-operation at incident area.

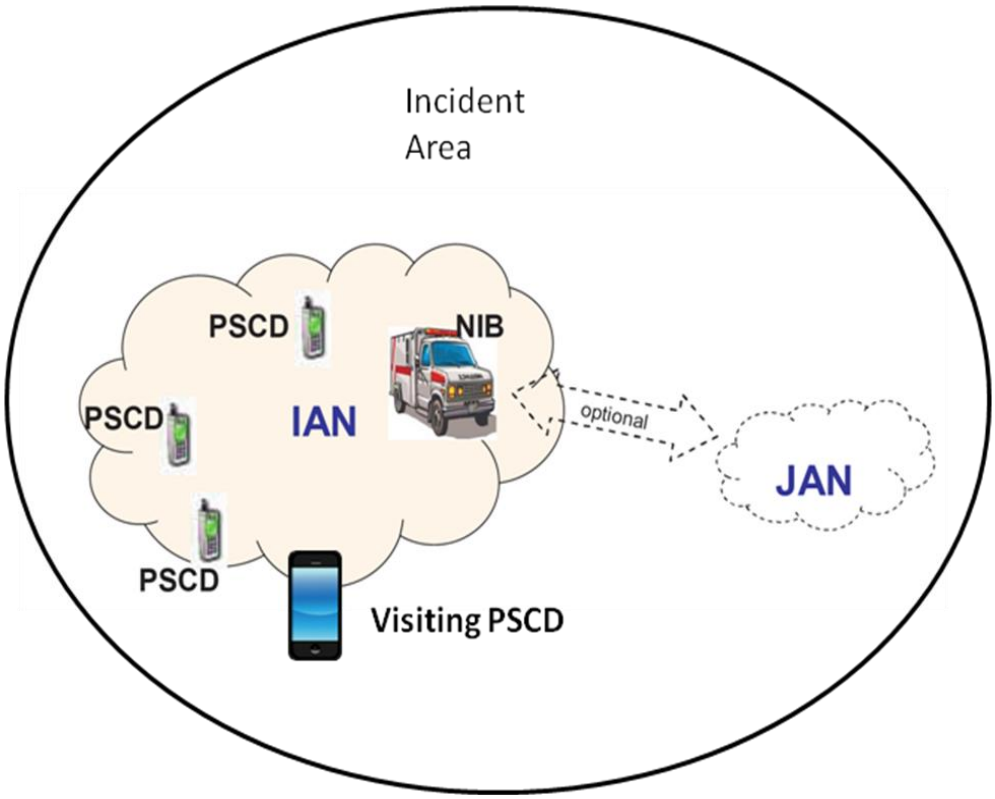

Figure 6: Visiting PSCD.

3 Actors

Within each organization we distinguish between the following actors (or roles):

- The JAN manager
- The NIB manager
- PSCD user
- Attacker

3.1 JAN manager

The JAN manager has the authority to access all information within a JAN and corresponding IANs. It is the responsibility of the JAN manager to issue the credentials to all users within one organization (IAN) and to configure or to delegate the administration of configurations in the JAN/IAN including setting the security policies to another entity.

3.2 NIB manager

It is the responsibility of the NIB manager to configure the NIB including setting the security policies for the IAN that the NIB belongs to.

3.3 PSCD user

The PSCD is the user who uses the PSCD in his/her daily operations.

3.4 Attacker

The attacker tries to impersonate legitimate PSCD and NIB users or tries to get hold of IAN, JAN or secret information or to modify IAN or JAN data or software in order to get hold of information or to destroy the normal operation of the system.

4 Scope

4.1 Limitations

We are interested in investigating the security needs that arise as a consequence of the cross-organizational *as well as* the introduction of SDR units in the crises management systems we have described in Section 2. Our investigation will consider the needs of security and trust for agile and dynamic cross-organizational interactions using SDR-based communications with minimum level of trust in terms of pre-configurations and agreements. The work will be carried out starting from identifying and analyzing the needs of the three actors identified earlier in this document. The ultimate goal is to investigate the mechanisms that are needed to make all parties trust the crises communication infrastructure, when there is direct or indirect interaction between users from different organizations and SDR devices in the systems.

We will here focus on security needs stemming from the SDR, IAN 1 to IAN2 as well as visiting PSCD scenarios. We will primarily *not* deal with security issues related to how information is protected or securely accessed in the JAN or how information between different JANs can be shared.

4.2 Research issues

Considering the limitations we have described in Section 4 above, we have decided to sort the security issues we will address from two different angles:

- SDR life cycle management
- Trust establishment

The SDR life cycle management issues relates to the handling of the SDR modules in the NIB. The trust establishment issues relates to the interconnection of two IANs (through the NIBs) and to allowing communication with a visiting PSCD in a hosting IAN.

4.2.1 SDR life cycle

The SDR life cycle consist of the following major NIB states:

1. PSCD configurations at manufacture
2. First time installation of SDR module
3. SDR module active and running
4. SDR module update

The issues connected to these states include (not at all an exhaustive list):

- What type of hardware support (cryptographic, shielded storage, ROM, keys etc.) do we require/need in the radio platforms
- What type of different models should one support with respect to secure identification of radio platform hardware?
- How the SDR module is securely installed into the platform and how can verify the integrity of the SDR module?
- Different options for securing the SDR execution environment from active attacks. How is the SDR execution environment verified?
- How are the SDR module securely updated? Different update models?

4.2.2 Trust establishment

The issues connected to trust establishment when interconnecting two IANs through two NIBs or when a visiting PSCD connects to an IAN include (not at all an exhaustive list):

- Establish if the connecting NIB or visiting PSCD *and* the network behind the NIB is trustworthy
    - Who owns and runs the NIB or PSCD?
    - Hardware platform and ID of connecting NIB or PSCD?
    - Software configuration of connecting NIB or PSCD?
    - Security policies that applies in the connecting IAN/JAN (IAN merge) case?
    - Security policies that applies for the visiting PSCD?
    - Security policies that applies for the IAN that the visiting PSCD connects to?
- How to configure and enforce security rules for all information that goes to and from the connecting NIB or visiting PSCD?
- Dynamically measure the degree of trustworthiness in the connecting NIB or PSCD

5 References

[1] The Euler project, http://www.euler-project.eu/