



Note

Security Architecture of the FieldCare Demonstrator

Note no

DART/06/05

Authors

Shahzade Mazaher

Date

April 2005

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Title	Security Architecture of the FieldCare Demonstrator
Authors	Shahrzade Mazaher
Date	April 2005
Year	2005
Publication number	DART/06/05

Abstract

This document describes how the generic system model and the related security architecture of the Wireless Health and Care (WsHC) project are applied to the FieldCare Demonstrator. The security threats for the demonstrator are determined first and the corresponding risks evaluated. The security architecture document gives guidance to which security components and security mechanisms that meet the requirements in order to counter the relevant threats.

Keywords	Security architecture
Target group	
Availability	public
Project number	320302
Research field	Computer Security
Number of pages	28
© Copyright	Norsk Regnesentral

Contents

1	Introduction	7
2	FieldCare Scenario	7
3	Mapping to the Generic system model	7
3.1	Security Requirements	10
4	Risk analysis	12
4.1	The Identified Threats	12
4.2	Risks	13
5	Security architecture	16
5.1	Sources	16
5.2	Channel A: Source and MDA	17
5.3	Patient Data Collector	17
5.4	Channels B and C	19
5.5	Channel E.....	19
5.6	Patient Data Consumer	20
5.7	The Central System.....	21
5.8	Emergency Access.....	22
6	Security Implementation	22
6.1	The Inherent Weaknesses of Wireless LAN	24
7	Conclusion	27

List of figures

Figure 1. The Generic System Model	8
Figure 2. The FieldCare Overall System Model.....	9
Figure 3. Distribution of Security Components in FieldCare	26

1 Introduction

This document applies the generic system model and the corresponding security architecture as described in [1], to the FieldCare demonstrator. Work on security specification for ad-hoc wireless networks, described in [5], has also been taken into consideration. While [5] focuses a lot on routing the information, the focus of this document is to describe measures needed to secure the patient data both while in transit (in the network) and when stored and accessed.

For the sake of self containment, the most relevant definitions, figures and tables from documents [1] and [2] are included in this document. But, for more details the reader is referred to the aforementioned documents.

2 FieldCare Scenario

The general setting for the FieldCare demonstrator is access to medical information and communication between the members of the medical team present at the scene of an accident. The detailed architecture of the FieldCare demonstrator is described in [6].

In the FieldCare demonstrator, each injured person, hereafter called patient, at the scene of an accident is assigned a unique ID by means of a MiTag (iButton). The MiTag has the potential to be used also as a repository of all patient data gathered at the scene, which then will be carried by the patient himself. Moreover, other sensors might also be attached to the patient; the output of the sensors is input to a sensor concentrator. The patient data is collected by Medical Digital Assistants (MDA) that the medical personnel use. When a patient's MiTag is registered by a MDA, a FieldCare id-number (FID) is generated by the MDA and associated with the MiTag. All Patient data are associated with the corresponding patient FID. In addition to the sensors, the medical personnel can also enter patient data manually, which is also associated with the patient FID. These MDAs are connected to each other in a wireless LAN and broadcast the patient data that is input to them to the other MDAs on the WLAN. All patient data is therefore readily available to the members of the medical team. One of the medical personnel at the scene assumes the role of coordinator and uses a MDA with extra functionality to support coordination needs called Coordinator Medical Assistant (CMDA). Furthermore, patient data is sent by means of the FieldCare Fields Connector (FCC) to the Central System for an expert medical decision or preparation for patient care on his arrival at the hospital/emergency center. The FCC is the same as a MDA only with the added capability of long distance communication. The medical personnel can access, if needed, patient data in the Central System. In emergency cases, it might be necessary that members of the medical team bypass access rights in order to get hold of crucial information about a patient, e.g., what kinds of drugs a patient is using. The FieldCare system must therefore allow for some kind of emergency logging that ignores, to some extent, access rights.

3 Mapping to the Generic system model

This section maps the components of the FieldCare demonstrator to the components of the generic system model developed in the Wireless Health and Care (WshC) project. The generic system model, which encompasses all the WshC's demonstrators and serves as the basis for the security architecture, is depicted in Figure 1.

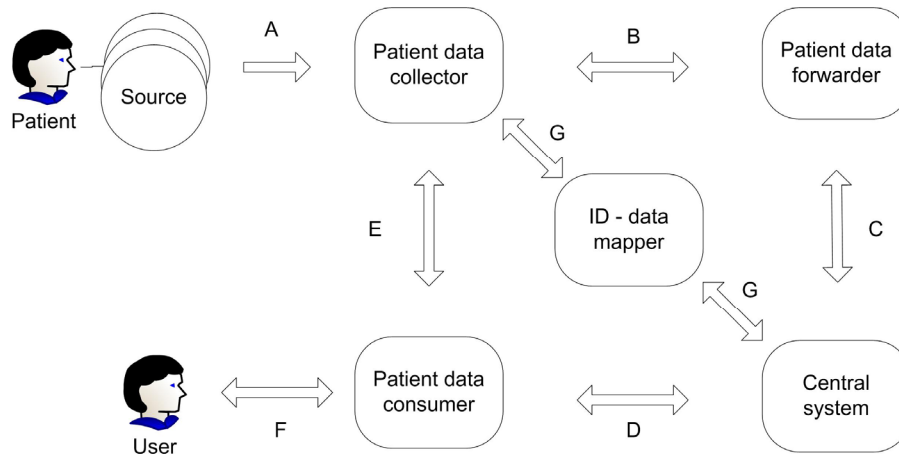


Figure 1. The Generic System Model

The FieldCare demonstrator may consist of the following components:

- **Sensors:** Devices attached to the injured at the scene of the accident to measure vital life parameters, e.g., heartbeat, breathing rate, blood pressure, etc.
- **Sensor concentrator (SC):** A device serving as an endpoint for all the sensors attached to the patient. It acts as the Source component of the generic system model depicted in Figure 1.
- **Medical Information Tag (MiTag):** A personal electronic tag (e.g., an iButton) attached to the patient where medical information is stored¹. The contents of a MiTag can be inserted/read by Medical Digital Assistants or the Central system through physical contact. The MiTag is treated as the Source in the generic system model shown in Figure 1, and the insertion of patient data into the MiTag is not considered².
- **Personal Identification Tag (PiTag):** Similar to MiTag, this is a personal electronic tag carried by the medical personnel and used at the scene of an accident to log onto and authenticate themselves to the MDA (see below). It is considered to be part of the Patient Data Collector (PDCL) in the generic system model, Figure 1.
- **Medical Digital Assistant (MDA):** Typically, a PDA equipped with the FieldCare software installed on it. It may take the roles of both Patient Data Collector and Patient Data Consumer (PDCM) in the generic system model, Figure 1.
- **Coordinator's Medical Digital Assistant (CMDA):** At an accident scene, usually one person is assigned the role of coordinator. CMDA extends the functionality of the MDA with support for coordination activities. But in the security analysis, it will be treated as an MDA and can assume the same roles with respect to the system model. Physically it can be a laptop with a larger screen.
- **FieldCare Connector (FCC):** A computer or a MDA with long-range communication capability. It makes it possible for MDAs to communicate with the hospital, the

¹ Additional security measures may be necessary for devices whose only purpose is *storage* of patient data, in particular procedures for handling such devices in different situations.

² : In the FieldCare Demonstrator, MiTags are primarily used for the identification of the injured people and they store only an identification number for the patient.

ambulance dispatch centers (AMK), and the ambulances. It acts as the Patient Data Forwarder (PDF) in the generic system model, Figure 1.

- **Central System (CS):** the Central System in the generic system model, shown in Figure 1, at the hospital including EPJ.

Note that sensors and sensor concentrators are not yet implemented in this demonstrator, but are natural future extensions. With respect to security, all components that consume sensor data, i.e., Sensor Concentrators, must be trusted to handle unencrypted medical data. A scenario in which the communication between the Sensors and the Sensor concentrator is wireless, e.g., using Bluetooth, introduces more potential points of failure with respect to security, and hence, new security requirements on the source, i.e., the combination of Sensors and the Sensor Concentrator.

In the actual demonstrator, all MDAs communicate via an ad-hoc WLAN set up at the scene of the accident, and all patient data entered on one MDA is automatically replicated on all the other MDAs. In addition, MDAs do not fetch patient data from the hospital.

Moreover, the MDA and the FCC are logically two separate components. But, in the FieldCare demonstrator, they are implemented as the same physical module, i.e., MDAs have capability for long-range communication. Therefore, channel B of the system model does not correspond to any network communication and is internal to the MDA software and patient data is automatically sent to the hospital.

Figure 2 depicts the generic system model as applied to the FieldCare demonstrator. Channel D is shown with a dashed arrow since it is not a part of the current demonstrator, but it is a natural extension in the future. In FieldCare demonstrator, fetching patient data from the Central System (channel D) is done by the MDA, which contains all functionality pertaining to Patient Data Collector, Patient Data Consumer and FCC. The channels C and D typically share the same physical channel and the channels B and E being internal to the WLAN or inside the MDA.

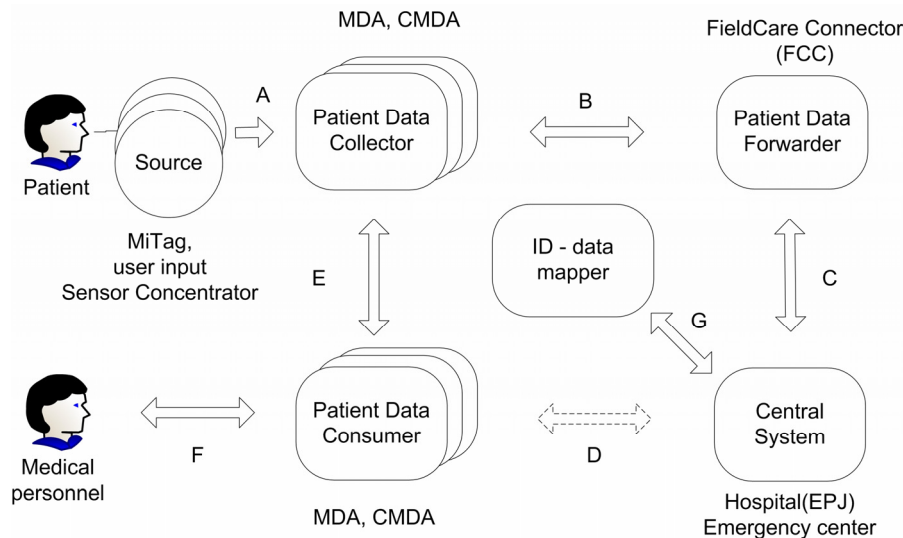


Figure 2. The FieldCare Overall System Model

In the FieldCare demonstrator, the Patient Data Collector component and the Patient Data Consumer components are physically the same component, i.e., a MDA. Moreover, these MDAs are connected via a WLAN, and patient data collected by any of them is automatically distributed to all the others. Therefore, in addition to being a Patient Data Collector, each MDA is also a Patient Data Consumer with respect to the other MDAs and channel E therefore corresponds to the WLAN.

The security requirements on the system model ([1]) are described in [2]. Those that are relevant for the FieldCare demonstrator are listed below in Table 1. Moreover, [2] lists a set of

functional requirements applicable to the reference system model. Security and functional requirements are discussed in more details in the rest of this document.

3.1 Security Requirements

Requirement numbers correspond to those on the system model in [2]. Requirements that are not applicable to the demonstrator are left blank. In the FieldCare demonstrator, the MDA can assume several roles. Therefore, in the table below, the role that the MDA assumes in each context is given in parentheses.

Table 1. Security Requirements of the FieldCare System.

No.	Actor(s)	Requirement
Sec1	Source	Limited storage. Sources shall not store sent data longer than necessary (confidentiality)
Sec2	Channel A	Short-range communication. Sources shall only communicate short range (confidentiality and integrity)
Sec3	Channel A	Confidentiality protection. Patient data should be protected from eavesdropping when transmitted to the MDA (Patient Data Collector)
Sec4	Channel A	Integrity protection. Patient data should be integrity protected when transmitted to the MDA (Patient Data Collector). (Note: this includes protection from interference)
Sec5	Channel A	No automatic roaming. The connection between Source and MDA (Patient Data Collector) shall be manually initiated, i.e., a human actor determines (at some point in time and through a defined procedure) which Sources and MDAs (Patient Data Collector) that shall talk to each other (integrity)
Sec6	Patient data collector	Verify Source identity. MDA (Patient Data Collector) shall verify correctness of the Source identity (integrity and accountability)
Sec7	Patient data collector	Data integrity verification. MDA (Patient Data Collector) shall verify the integrity ³ of patient data
Sec8	Patient data collector	Data modification. MDA (Patient Data Collector) shall not modify patient data, except possibly for aggregation or other defined transformations (integrity)
Sec9	Patient data collector	No unauthorized data access. MDA (Patient Data Collector) shall not give unauthorized actors access to patient data (confidentiality and integrity)
Sec10	Patient data collector	Limited storage. MDA (Patient Data Collector) shall not store data longer than necessary (confidentiality)

³ Data Integrity verification: “Integrity verification” refers to the verification that data has not been altered during transmission from the Source; it does not imply a “sanity check” on the data. Such a sanity check should be implemented somewhere in the system; at least in the Central system before storage of the data.

No.	Actor(s)	Requirement
Sec11	Channels B, C and E	Confidentiality protection. Personally identifiable patient data shall be protected from eavesdropping when transmitted across open networks.
Sec12	Channels B, C and E	Integrity protection. Patient data shall be integrity protected when transmitted across open networks.
Sec13	Central system	Data integrity verification. Central system shall verify the integrity of patient data.
Sec14	Central system	Data origin authentication. Central system shall authenticate the MDA used as Patient Data Collector (integrity and accountability)
Sec15	Central system	No unauthorized access. Central system shall not give unauthorised actors any type of access (view, insert, transform, delete) to the patient data it stores (confidentiality and integrity)
Sec16	Central system	Patient identity. Central system shall know the identity of the patient to whom the patient data pertains (integrity)
Sec17	Central system	Source type. Central system shall know the type of source used to produce the patient data (integrity)
Sec18	Channel D	Authenticate User. Central system shall authenticate the User (confidentiality and accountability)
Sec19	Channel D	Authenticate Central System. Patient data consumer shall authenticate the Central system (integrity)
Sec20	Channel E	Authenticate User. MDA (Patient Data Collector) shall authenticate the User who wants to access the data (confidentiality and accountability).
Sec21	Channel E	Authenticate Patient Data Collector. MDA (Patient Data Consumer) shall authenticate Patient Data Collector (integrity)
Sec22	Patient data consumer	Data integrity verification. MDA (Patient Data Consumer) shall verify the integrity of patient data
Sec23	Patient data consumer	No unauthorized access. MDA (Patient Data Consumer) shall not give unauthorized actors any type of access (view, insert, transform, delete) to patient data (confidentiality and integrity)
Sec24	All components	Emergency access. Where emergency access functionality is available, invocation of emergency access shall override any restriction on read access (availability)
Sec25	All components except Source	Emergency access monitoring. Emergency access shall trigger extended monitoring of relevant events to enable detection of unnecessary access (confidentiality and accountability)

There are two derived security requirements in [2]:

- The Patient Data Collector must be trusted to handle unencrypted patient data. In the FieldCare, the MDAs are trusted units.
- The Patient Data Forwarder is not a trusted entity and must not handle unencrypted patient data⁴. This requirement is not applicable to the FieldCare demonstrator. This is because FCC is a part of each MDA and MDAs are trusted to handle unencrypted data.

4 Risk analysis

Systems have vulnerabilities that can be exploited and are exposed to threats. The probability of these events combined with their impacts at the organizational level determines the risks that the organization may incur.

4.1 The Identified Threats

In [2], the *WsHC Security Requirements* document, a set of threats to the generic system model is identified. A set of threats is also listed in [5], in Section 3.1, *Identifying the Threat*. The threats identified in [2] are more classes of threats than specific instances, while those listed in [5] are of more specific nature. In this section, we classify the threats identified in the latter document (i.e., the more specific threats) under the classes identified in the former document.

Note that some threats to the system cannot be dealt with by the security architecture. They have to be countered by establishing work processes and procedures that must be followed diligently. For example, a member of the medical team must not leave his MDA unattended; if he needs to go away from it for some reason, he must first log off such that the data on the MDA is not compromised and, if possible, he must secure the device such that the device itself is not compromised. These types of threats are out of scope of the security architecture and this document; the same applies to environmental hazards, e.g., earthquake, and physical accidents.

For convenience the *Threat Table* from [2] is included below.

Table 2. Possible threats to the FieldCare System

No.	Actor(s)	Threat
Threat1	All components	Compromised or fake component (physical or logical attack)
Threat2	All components	Destroyed, lost, or stolen component
Threat3	All channels	Compromised or fake (components of) communication infrastructure (physical or logical attack)
Threat4	All channels	Unstable communication infrastructure (physical or logical attack, bad quality, accidents)
Threat5	All components	Software errors (failure in security mechanisms, routing, etc.)
Threat6	All components	Misuse of emergency access

⁴ This is because the number of the trusted components should be kept to the minimum possible in order to reduce the potential vulnerable nodes of the system.

Threat7	All channels	Eavesdropping of communication
Threat8	All components and channels	Denial of service attack (physical or logical attack, bad quality, accidents)

The following table maps the concrete threats ([5]) to the categories identified in Table 2 above. The threats that are out of scope are left out.

Table 3. Mapping of Concrete Threats to Threat Categories

No.	Concrete Threats	Corresponding Categories
CT1	Data modification	Threat1, Threat2, Threat3 and Threat6
CT2	Denial of service	Threat8
CT3	Device cloning	Threat1
CT4	Device theft	Threat2
CT5	Eavesdropping	Threat7
CT6	EMP	Threat2 and Threat4
CT7	Impersonation	Threat3
CT8	Incorrect routing	Threat4 and Threat5
CT9	Jamming	Threat8
CT10	Malicious code	Threat1
CT11	Traffic analysis	Threat3 and Threat17
CT12	War driving	Threat3
CT13	Errors and omissions	Threat5

There are a couple of threats not appearing in Table 3, which put requirements on other aspects of the system. The threat *File deletion* puts functional requirement on the FieldCare system, i.e., the implementation of the system must be such that it makes it hard for users to perform damaging actions, such as file deletion, by mistake. The *Power failure* threat is a safety requirement on the management and operation of the system, e.g., all the critical components threatened by a power failure must have a back up power source available.

In addition to the threats listed in [2], FieldCare is exposed to an additional threat proper to WLANs, described below.

- **Threat9** - Hijacking the session: That is, to inject false traffic into the network on behalf of legitimate users. For example, issuing commands on behalf of legitimate users.

In this section, the threat identifications of the form **Threat#** correspond to those of the threats in Table 2, and those of the form **CT#** to the threats listed in Table 3.

4.2 Risks

Table 4 shows the risks that the FieldCare system is subject to. Each row refers to a threat to the system and gives its probability and its impact. The impact levels are described in the Table 5 and

Table 6 shows the level of risk associated with the possible combinations of probability and impact.

The most meaningful attacks that we envisage against FieldCare system can be categorized in the following classes:

- Getting knowledge of information in the system.** This can be for criminal purposes, i.e., to gain access to sensitive information about a person in order to harm him, or of a more benign nature, e.g., a journalist who is after first hand news. Eavesdropping on the communication by, e.g., journalists, is a main concern with the unencrypted radio communication that is in use today. It is as easy to eavesdrop on communication links that use radio wavelength, especially that, in general, they do not provide for strong encryption. This leads to outsiders getting sensitive information. This attack corresponds directly to Threat7 or CT5. Trying to get knowledge of information by other means, such as device cloning (CT3), device theft (CT4), impersonation (CT7), malicious code (CT10) and traffic analysis (CT11), are considered mainly used in criminal cases and harder to achieve, and as such, less probable.
- Introducing wrong information in the system.** This can be achieved either by directly changing the information, by associating the information in the system to the wrong person, or by preventing the necessary/complete information to reach the system. This will be mostly done for criminal purposes as it is to nobody's benefit but people wishing harm to introduce wrong patient data. This will result in patients not getting the needed or getting the wrong treatment. Introducing wrong data can be achieved by means of data modification (CT1), device cloning (CT3), device theft (CT4), impersonation (CT7), incorrect routing (CT8), malicious code (CT10), and software bugs (CT13).
- Disrupting the proper functioning of the system.** This can be a result of denial of service attacks (CT2, CT9), attempt at destroying (parts of) the system (CT6) and bugs in the system software (CT13). Besides software bugs, the other threats are considered to be of a more criminal nature.
- Refusing access to the needed data.** This refers to a functioning system to refuse access to the data that the user is asking for. This can be a result of a denial of service attack (CT2 and CT9), device cloning (CT3), device theft (CT4), malicious code (CT10) and software bugs (CT13). These threats are also considered to be of a more criminal nature.

Note that in emergency cases, medical personnel need access to some patient data that are of vital importance in the treatment of the patient. The system might refuse them access to the data based on that the user lacks the required access privileges. This is different from the last bullet above and it is not an attack. This is a requirement on the functionality of the FieldCare system; it requires that an emergency access mode, bypassing the regular access control in the system, be implemented.

In summary, benign eavesdropping (e.g., by journalists) is considered to be the most probable threat to the system. Criminal attacks are in general considered to be less probable. The attacks that are judged to be most probably used in malicious attacks are eavesdropping, jamming, session hijacking and to a lesser degree device theft or cloning. There is always a low probability of wrong information in the system, disruption in the proper functioning of the system, and refusal of access to the needed data resulting from bugs in the system.

Table 4. Risk Evaluation of the FieldCare System.

Risk ID	Description	Probability	Impact
---------	-------------	-------------	--------

Risk ID	Description	Probability	Impact
R1*	Eavesdropping on the communication on the scene of the accident with no malicious intention (e.g., journalists)	Probable	Moderate
R2*	Eavesdropping on the communication on the scene of the accident with malicious intention	Occasional	Moderate
R3*	Device theft to get knowledge of information	Occasional	Moderate
R4	Device cloning, impersonation, malicious code, traffic analysis to get knowledge of information	Remote	Moderate
R5*	Device theft to introduce wrong information	Remote	Large
R6	Denial of service attacks (other than Jamming), Device theft/cloning, impersonation, incorrect routing, malicious code to introduce wrong information	Improbable	Large
R7**	Jamming to disrupt the functioning of the system	Occasional	Large
R8	EMP to disrupt the functioning of the system	Improbable	Large
R9*	Bugs in the system software resulting in the disruption of the functioning of the system ⁵	Remote	Large
R10*	Bugs in the system software resulting in refusal of access to the needed data	Remote	Large
R11**	Hijacking the session	Occasional	Large

The asterisks (*) in the table above denote the seriousness of the risk; the more asterisks the higher the risk, and hence, the higher the priority of corresponding countermeasures. Note that the two first threats are the same but with different intensions behind them. But given the probability and the impact of each, the resulting risk is the same.




Table 5. Description of the Impact Levels of Threats and Vulnerabilities.

Consequence level	Description
Catastrophic	Loss of lives.
Large	Danger for patients' life and health. Privacy breach for a large number of patients. Serious economic losses. Serious loss of reputation.
Moderate	No danger for patients' health. Privacy breach for a small number of patients. Moderate economic losses.

⁵ It is assumed that in the development of security critical systems, an adequate software development process, including comprehensive testing is used.

	Moderate loss of reputation.
Small	No danger for patients' health. No privacy breach. Inconsequential economic losses. No loss of reputation.

Table 6. Risk Assessment Matrix

Probability	Impact level			
	Catastrophic	Large	Moderate	Small
Frequent	High (**)			Medium (*)
Probable	High (**)		R1 Medium (*)	Low
Occasional	R7, R11 High (**)		R2, R3 Medium (*)	Low
Remote	R5, R9, R10 High (**)		R4 Medium (*)	Low
Improbable	Medium (*)	R6, R8 Medium (*)		Low
Legend:		High (**)		
		Medium (*)		
		Low		

5 Security architecture

This section discusses the security requirements (Table 1) that apply to the various components of the FieldCare demonstrator and describes security measures that need to be implemented in order to satisfy the security requirements. More general security measures that apply to several components are discussed in Section 6, *Security Implementation*.

5.1 Sources

In the FieldCare demonstrator, there are two types of Sources. The MiTags that are the sources of the Patient-Ids (PID), and the medical personnel who manually enter the data related to the patients.

The security requirement applying to the Source is that data shall not be stored on them longer than necessary (Sec1). In FieldCare, this requirement only applies to the MiTag. But, the MiTag just stores its unchangeable unique id, used as link between the patient and the related data stored in the MDA (or sent to the hospital) and contains no other data. Had it been the case that the MiTag contained patient data, the requirement would imply that the data be kept on the MiTag until the patient comes to the hospital and the related data are stored properly in the hospital's Central System under the patient identity used by that system. The patient data contained in the MiTag storage should be removed immediately after that.

Should MiTags be used for patient data storage, the information available on them must be confidentiality and integrity protected. This is required even if the patient cannot be identified from the data stored on the MiTags. This is because MiTags are attached to patients whom might be identified.

In the case that sensors and Sensor Concentrators (SC) are used, the latter become Sources. They must therefore observe the requirement that they shall not store data longer than necessary.

5.2 Channel A: Source and MDA

Channel A is the communication channel between a source and the corresponding MDA. In this section, we discuss the requirements on this channel with respect to communication with the two types of sources.

The security requirements on the communication channels between the sources and the MDAs are that

- they must be short range;
- patient data must be protected from eavesdropping;
- patient data must be integrity protected;
- the connection between the sources and the MDAs must be manually initiated.

In FieldCare, the communication links between the sources and the MDAs are by nature short range. The unique-id is read off the MiTag, attached to the patient on the scene of the accident, by physical contact between the MDA and the MiTag; the unique-id is therefore transferred correctly to the MDA; patient data is entered manually by the person in charge of the patient.

The second and the third requirements on the list above are also satisfied by the nature of the FieldCare devices and setting. Eavesdropping or tampering with data on the cable connecting the MiTag to the MiTag (iButton) reader is not considered realistic. Patient data being input manually by the health personnel, it can be assumed secure with respect to both confidentiality and integrity given that the health personnel are trustworthy. The trust issue is discussed in the next section.

The fourth requirement above is also satisfied automatically since the MiTag is manually attached to the MDA and a health personnel is associated with a MDA by manually logging on that MDA.

The case where Sensor concentrators, collecting data from many sensors, are also used as sources is discussed in detail in the next section.

5.3 Patient Data Collector

In the FieldCare demonstrator, Patient Data Collectors are the MDAs forming the ad-hoc WLAN. The security requirements applying to them are that they must

- verify the source identity;
- verify the integrity of patient data;
- must not modify patient data;
- must not allow unauthorized access to patient data;
- must not store data longer than necessary.

The issue of trust mentioned in the previous section, is related to the first item on the list above. In order to provide for the confidentiality and integrity of patient data input from the Sources, we said that the health personnel and the MDAs, acting as Source, must be trustworthy.

To establish this trust, the health personnel logging on a MDA must be authenticated by the MDA. We recommend that the PiTag mechanism, proposed in [5], be used in the authentication process, as the initial solution is not flexible enough⁶.

PiTags are almost identical to MiTags except that they store information, e.g., name, title, etc., about their owners. Each of them also stores the hash value of a secret, e.g., a PIN-code, owned by its owner, which is checked by the MDA against the value entered by the user when logging on. Authentication of the Source provides for the first, second and fourth requirements listed above.

Moreover, as proposed in [5], a MDA must not be able to communicate with other MDAs and receive data before the medical personnel using it is authenticated. In other words, a MDA is only allowed to send data on and receive data from the ad-hoc WLAN after the authentication of its user.

The third requirement states that the integrity of the input patient data must be preserved by the MDA. Therefore, patient data can only undergo defined transformation, and in that case, the information about the kind of transformation applied to it must follow the data. MDAs keep the history of the patient data and do not allow changing/replacing the data already entered. New patient data is only added. This, to some extent, guarantees the integrity of the data that is already entered.

As for the last requirement, all **patient** and **user** data entered during the current emergency session should definitively be removed automatically at log-off time. How long each MDA should stay on and when it should be turned off depends on the routines and procedures used at the scene of the accident and whether patient data is available in the ambulance or at the hospital. Note that by removing all patient and user data at log-off time, the MDA is made ready for a new emergency situation with a new (or same) user and a new patient.

Now we consider the case that sensors and a Sensor Concentrators (SC) are also used, and the SC is therefore a Source. A wired communication between a SC and a MDA is considered to be secure enough; security should be considered when the communication is wireless. For the sake of simplicity, we assume that the sensors are wired to the SC; if the communication between those is also wireless, the discussion about the communication between the SC and the MDA applies, to some extent, to the communication between the sensors and the SC.

The two issues here are

- mutual authentication, i.e., the SC knows it is talking to the right MDA and the MDA know it is receiving data from the right SC, and
- confidentiality and integrity, i.e., protecting the privacy and the integrity of the data.

Confidentiality and integrity are secondary to authentication, i.e., without having the latter, the former is not important.

The mechanism used in providing mutual authentication depends on the capabilities of the SC. If the SC has enough computational power, then a public key based authentication can be performed. The SC needs to know the certificates of all possible MDAs to which it is allowed to talk, and similarly, the MDAs need to contain the certificates of the potential SCs with which they might communicate. Confidentiality and integrity can then be achieved by establishing a session key and encrypting the patient data with it. This session key can either be generated by the SC and sent to the MDA during the authentication process (or later), or established by means of cryptographic algorithms.

⁶ A set of valid PIN codes are hard-coded in the FieldCare prototype.

If the SC is a small, not very powerful device, then PKI based authentication is not an alternative. One possible way of achieving authentication is by transferring a shared secret to the SC via physical contact. That is, to touch the SC with an electrical contact that transfers the bits of the shared secrets. This, of course, requires that SCs provide such a capability, but there are many scenarios that could benefit from such a capability and most probably SCs will be equipped with it in the future, if not already. For example, in the FieldCare demonstrator, this capability also ensures that a MDA talks to the proper SC and not the neighboring SC, which is within range. Another alternative would be to preprogram the SC with an encryption key/pin code. In that case, the MDA must know the key/pin code of the SC it is responsible for.

In addition, there might exist standard security solution for the communication link between the SC and the MDA, e.g., if the communication is via Bluetooth.

The described solution also satisfies the last two requirements, integrity of patient data and manual initialization of the communication, of the previous section.

5.4 Channels B and C

In the FieldCare demonstrator, channel B is local to the MDA and therefore does not need any special security measures. Patient data is transferred to the hospital's Central System via channel C, which is over communication links, such as GPRS, GSM, Internet, etc. or a combination of them.

In the current implementation, channel C is simplified to being the same WLAN as the one that MDAs use to communicate. As a result, patient data gets replicated to the hospital node as well. Security requirements on channel C therefore apply to the WLAN.

- confidentiality of the patient data;
- integrity of the patient data.

To provide for confidentiality of the patient data in transit, cryptographic security mechanisms must be used. Due to the sensitivity of information and the relative ease of eavesdropping on communication over radio wavelength, strong cryptography is needed. Integrity of data will be provided by the solution to the authentication requirement put on the Central System. Security solutions for these requirements are discussed in more details in Section 6, *Security Implementation*.

5.5 Channel E

Channel E is the direct communication channel between the Patient Data Consumer and the Patient Data Collector. As mentioned earlier, this channel corresponds to the WLAN established among the MDAs, and it is short-range as assumed in [1]. In addition to the requirements of the previous section, viz., confidentiality and integrity, this channel has the requirements that

- Patient Data Consumer (a MDA) must authenticate the Patient Data Collector (a MDA);
- Patient Data Collector (a MDA) must authenticate the user, e.g., a paramedic.

The first requirement implies that whenever a MDA sends data to another MDA, the receiver must authenticate the sender. In addition, to satisfy confidentiality, the data must be encrypted with a symmetric (secret) key. Authentication is an expensive process; it is therefore strongly recommended that all MDAs be authenticated when joining the ad-hoc network. It must be impossible for a non-authenticated node to join the network. The authentication must be mutual, i.e., the joining node must also authenticate the network node it is talking to. This is needed in order to prevent the new node to join by mistake a neighboring WLAN, which is within range. By doing so, all MDAs in the role of Patient Data Consumer have authenticated all the other MDAs that play the role of Patient Data Collector with respect to them. As part of or after the authentication, a session key can be established for encrypting patient data. That is, the first two

MDAs joining the WLAN agree on a session key that is passed to the other nodes, using public-key cryptography, as they join the ad-hoc net.

Each MDA that is in an operational state has been authenticated when joining the ad-hoc net and has authenticated its user, a member of the medical team, by means of his PiTag. One can therefore say that a MDA, in the role of Patient Data Collector, has authenticated the user (a medical personnel) at the MDA acting as Patient Data Consumer.

5.6 Patient Data Consumer

In the FieldCare demonstrator, Patient Data Consumers (PDCN) are the MDAs forming the ad-hoc WLAN. They are consumers with respect to the other MDAs, acting as collectors and sending them patient data. The security requirements applying to them are that they must

- verify the integrity of the patient data;
- must not allow unauthorized access to patient data.

Integrity of data will be handled by the authentication solution discussed in more detail in Section 6, *Security Implementation*.

In the current FieldCare demonstrator, access to data stored at the Central System is not implemented. MDAs, acting as PDCN, automatically receive patient data from other MDAs, acting as Patient Data Collectors. The authentication solution proposed in the previous section would provide for data integrity and its verification.

Each MDA authenticates its user upon log-on, which satisfies the second requirement, on the list above, since its user has the right to access (view, insert)⁷ all information stored on it.

Now we consider the case where access to patient data at the central system is implemented. That is, MDAs, acting as PDCN, can access patient data at the Central System via channel D. Requirements on channel D are as follows:

- Central System (CS) shall authenticate the user;
- Patient Data Consumer (MDA) shall authenticate the Central System.

The first requirement can be achieved in two ways.

- The CS trusts the authentication done by the MDA of its user, a member of the medical team, and authenticates only the MDA; or
- The CS authenticates directly the user (of the MDA). In this case, the MDA should provide for the necessary functionality.

The second alternative has the advantage that patient data are guaranteed to be sent to an authenticated person. That is, if a MDA, which is on, falls into the hands of a third party, that third party cannot use it to fetch data from the CS. This latter alternative will most probably be used in practice and the medical personnel will directly log onto the Electronic Patient Journal (EPJ) system at the hospital to access patient data.

To satisfy the second requirements, a MDA must authenticate the CS when they need to fetch data from it. This can be done using public key authentication. The requirements on channel C from Section 5.3, guarantee the confidentiality and integrity of the exchanged data.

⁷ In the FieldCare Demonstrator, patient data can only be inserted; all previously entered data is kept and the user is not allowed to delete or change them.

In the current implementation of the FieldCare demonstrator, channel D is physically the same as channel C, i.e., the WLAN. Therefore, all requirements on channel D apply also to the WLAN as well.

5.7 The Central System

The security requirements applying to the hospital's Central System (CS) are that it

- must verify the integrity of the patient data;
- must authenticate the Patient Data Collector;
- must not allow unauthorized access to patient data;
- must know the identity of the patient to whom patient data pertains;
- must know the type of source used to produce the patient data.

To be able to authenticate the Patient Data Collector, a MDA, each of them must have a pair of private-public key. That is, key certificates must be used as the basis for such authentication. Public-key authentication will also provide for data integrity verification.

The fourth item on the list above requires that all data stored in the Central System can be traced back to the patient to whom they pertain. In the FieldCare demonstrator, patient data collected at the scene of an accident is sent to the hospital's Central System for storage. There are two cases depending on whether a patient at the scene of the accident could be identified or not.

In the former case, patient's identification data is entered in the MDA along with the other collected information. When sent to the hospital, the Central System, knowing the patient's identity, stores the corresponding data⁸. In the latter case, the identity of the patient is not known and the Central System is only able to store the patient data under the PID generated by the MDA at the scene of the accident. The patient data must therefore be stored in a temporary storage until the patient is fully identified. The data stored in that way is always traceable back to the patient via the patient's MiTag unique-id. When the patient arrives at the hospital, it is recommended to issue a *hospital-id*⁹ for him, to replace the PID and the MiTag unique-id, until his identity is established and the corresponding data is moved from the temporary storage to the permanent storage (EPJ) under patient's real identity. That means that the CS must provide functionality for temporary storage of patient data under some other type of provisory identity. Note that most EPJ-systems have support for patients whose identity is not known. A temporary patient-identification is generated and is associated later with the real patient-id when this becomes known.

In the actual FieldCare demonstrator, the hospital, i.e., the Central System, is simulated and the Central System's functionality is simplified to only the reception of the patient data sent by the FCC (a MDA also). Therefore, the third and the last requirements, on the list above, are not relevant for the demonstrator. But, for the sake of completeness, they are briefly discussed below.

To prevent unauthorized access to patient data, access control mechanisms, preferably based on roles, must be put in place. Of course, authentication is assumed as a precondition for access control. The case of access in emergency mode is discussed in the next section.

For the Central System to know the type of the source of the patient data, this information must be stored along with the patient data and sent to the Central System. In the current FieldCare demonstrator, this source is always medical personnel and can be entered automatically by the

⁸ If need be, the Central System can generate a unique patient identifier according to its own scheme, based on the patient's identification data.

⁹ The hospital-is is generated according to some rules defined by the hospital.

MDA software. If there is a need for further subcategorization, the category of each member of the medical team can be part of the information on his PiTag and read by the MDA upon log-on.

5.8 Emergency Access

If a medical personal is for some reason prevented to log onto the system on his MDA it could have bad consequences. A main requirement of the system as a whole is that security related functionality (or other functionality) of the system should not contribute to loss of lives.

To avoid situations like this, one may allow some kind of emergency access. It is not clear how important such access is. But if it should be used in the system several precautions should be done.

The FieldCare system may therefore allow for some kind of emergency login that ignores, to some extent, access rights. The solution proposed in [5][4] is not satisfactory. It allows anyone to log-on in an emergency mode but restricts access to the patient data (PEJ) at the hospital. That is, a person trying to log onto a MDA will be logged in the emergency mode by providing a wrong PIN code three times in a row. That person, not being authenticated, does not possess the necessary credentials (called a Competence Role in [5]) to access to the data at the hospital, thus, safekeeping the confidentiality of the patient data at the hospital. But, that person can then enter patient data on the MDA and see data gathered by the other MDAs.

This scheme contradicts the very purpose of emergency access mode, which is access to information about the patient not available at the scene of the accident. Allowing any individual to enter data in to MDAs is not important. It is hard to imagine a scenario where there are no medical personnel available at the scene of an accident, who can log on in the proper way and enter the data, but there is a MDA available to be used by non-medical persons, e.g., passersby.

In addition, the issues of authentication and access control are mixed up. Authentication establishes the identity and access control, based on the identity and the corresponding credentials, decides what data can be accessed. In our view, for the sake of confidentiality, only medical personnel should be able to access patient data. Therefore, everybody using a MDA must have been authenticated by that MDA. To what extent an authenticated person can access data depends on that person's access credentials. In an emergency access case, where it is vital for the patient, access control rules can be relinquished in favor of availability of data. One can also apply some restrictions on the type of patient data that are made available in an emergency access mode.

The scheme we propose requires authentication for access to the MDAs, which can enter an emergency mode at the user's discretion. In an emergency mode, the Central System, when receiving a request for patient data, first authenticates the user, i.e., the medical personnel using the MDA, and then provides the data even though the user does not have the required access credentials for the request. This implies that a MDA marks the request with the emergency access status and that the Central System recognizes the emergency access status.

As required by the second item on the list above, for the purpose of accountability and confidentiality, all events related to emergency access must be logged. The logged information must at least contain the identification of the person who made the request, what was requested, time of the request, and if possible, an identification of the MDA.

6 Security Implementation

This section summarizes briefly the security solutions described in Section 5 and discusses more general security solution that are needed by the different components of the FieldCare demonstrator.

To provide for authentication and confidentiality cryptographic measures are needed. As mentioned in [1], *Security Architecture in Wireless Health and Care*, Section 5.2, centralized key managements based on symmetric cryptography, such as Kerberos, rely on an on-line service accessible to all the components at all times. In the FieldCare system model depicted in Figure 2, this is not appropriate for channels that may be implemented asynchronously, such as B and C. Moreover, in the FieldCare demonstrator, channel C, i.e., the communication link between the site of the accident and the hospital, may lack stability or have high latency due to traffic volume. This is not acceptable in the FieldCare demonstrator where access to the needed keys and credentials is highly important. Therefore, as proposed in [1], the Patient Data Collector, the Patient Data Consumer, and the Central System, i.e., the MDAs and the Central System, should be equipped with certificates and public-private key pairs, i.e., the use of PKI is recommended. In addition, for the sake of availability and reliability, we propose that the Certificate Authority's public key and the other MDAs' certificates and the Central System's certificate be available on local storage in each MDA. This implies that all MDAs must have a Security Administration front-end, as depicted in Figure 3.

The symmetric key alternative to public key authentication is to equip each MDA with a common key. Only those MDAs having this key can then connect to the system. This is not recommended as stated in [1], but can be temporarily accepted in the demo.

Note that storing keys and credentials on the MDAs will replace the current solution of storing IP addresses of all allowed nodes on each node.

In the rest of this section, references of the form (*Sec#*) refer to the security requirements of Table 1 on page 10.

The key pairs are used for the following purposes:

- MDAs authenticate each other when joining the ad-hoc WLAN (Sec21, Sec23);
- MDAs use them to provide confidentiality. That is, to encrypt symmetric keys that they generate for encryption or for the establishment of a symmetric key for encryption (Sec11). Note that there are algorithms for the establishment of symmetric keys that do not make use of public keys. The same applies to the communication between the FCC, also a MDA, and the Central System at the hospital (Sec11).
- The Central System uses it to authenticate the MDAs (Sec14).

By using public keys or other cryptographic algorithms (after authentication has taken place), it is possible to establish a secret encryption key, between the communicating nodes. Using such a secret key provides for confidentiality. Moreover, since this key is only known to authenticated nodes, it provides for integrity as well (Sec12, Sec13, Sec22): data encrypted by it cannot be changed without being noticed, and since no third party knows it, data encrypted with it cannot be injected in the communication link.

A health/medical system should only accept certificates issued to the medical personnel and equipment. That is, the certificates must either contain the purpose for which they were issued, i.e., a type, or they must be issued by some special Certification Authority, e.g., a hospital CA. This is to prevent the use of private certificates in security attacks against the system. For example, an individual with a certificate issued by a CA trusted by the hospital, could authenticate himself with the hospital and send some false patient data to the hospital, which stores it away as valid data. With a special purpose CA or a typed certificate in place, people who are not part of the medical personnel and equipment not belonging to the hospital would not be able to obtain the necessary certificate. Note that the authentication of the Source is done by means of PiTags (Sec6, Sec9).

The report commissioned by the Norwegian Ministry of Modernisation "*moderniserings-departmentet*" on requirements for a Public Key Infrastructure (PKI) for the government was submitted on November 2004 [3]. The implementation of security in FieldCare must therefore take the requirements from that reports into consideration. The report defines certificate profiles and the possible extensions, including a *Key Usage* field. This field can be used, as proposed

above, to set the usage to some value showing that the certificate's purpose is for digital signature, and possibly, encryption of symmetric keys, within health care.

In general, the above mentioned document must be taken into consideration when implementing the proposed security solution for the FieldCare demonstrator.

Meta-data should be used to provide traceability of patient data gathered on the field. The minimum information that is needed in the metadata is

- the type of the source (Sec17),
- the identity of the medical personnel who has entered it on the MDA,
- the identity of the patient: the PID can be part of it but any other identifying information such as patient name, birthday, ID number, etc., if available (Sec16),
- the type of (permitted) transformation that it has undergone, if any (Sec8), and
- the time and date of its generation.

In the current FieldCare demonstrator, MDAs are the main components and they have no need for access control mechanisms (Sec23), whereas the Central System is reduced to a minimum and access to the data it contains is not part of the demonstrator. But, in a more realistic setting, role based access control mechanisms must be put in place at the Central System (Sec15). The case for access to patient data in the emergency mode (Sec24) is elaborated on in Section 5.8.

Accountability should be provided by logging all the relevant events. As mentioned earlier, the Central System must log all access to patient data made in an emergency mode (Sec25). In addition, it might be useful that the MDAs log all data entry by the user and all reception of data sent by the other MDAs.

If Sensor Concentrators are used as sources, they have to provide for confidentiality and integrity (Sec3, Sec4, Sec7). In the case of a wired communication to the Patient Data Collector (MDA), the short-range communication over cable is secure enough and no security measures are needed. In the case of a wireless communication, the risk of a threat is higher and they must therefore have some security infrastructure, as proposed in [1], available on them. To provide for integrity, a checksum can be added to the data before sending. Security issues related to Bluetooth communication links are discussed in [4].

Some of the security requirements of Table 1 are satisfied by establishing procedures (Sec1) or providing functionality in the software components (Sec8, Sec10). All security requirements from Table 1 not referred to in this section are satisfied automatically by the nature of the FieldCare demonstrator.

Figure 3 shows the distribution of security components in the physical components, such as MDAs and Sensor Concentrator, and the logical components, such as the Central System simulated on a MDA, of the FieldCare demonstrator.

6.1 The Inherent Weaknesses of Wireless LAN

There are threats associated with the nature of WLANs. An attacker with proper equipment can easily launch a denial of service attack (jamming) by flooding the frequency range used by WLAN, so that it ceases to function. This can be a threat with even non-malicious intent as more technologies use the same frequencies and cause blocking. Cordless phones, baby monitors, and other devices like Bluetooth, operating on some of the same frequency ranges, can disrupt a wireless network.

The most widespread Wireless LAN standard today is IEEE's 802.11. This standard has many security issues related to it, in both 802.11b and 802.11a.

WLAN security has two aspects: data protection, i.e., encryption, and network access control, i.e., authentication. In IEEE's 802.11, the solution to data protection is Wired Equivalent Policy

(WEP), which is not strong enough. Moreover, control information are not encrypted and therefore leak information to eavesdroppers. 802.11 offers three solutions for network access control:

- Service Set Identifier (SSID), i.e., to join an ad-hoc WLAN all wireless stations must be configured for an ad-hoc mode and share the same SSID;
- Shared Key Authentication; i.e., to use a shared manually preset, static WEP key;
- Configuring the Access Point (AP) to only accept selected MAC addresses (presumably stations in ad-hoc mode can also be configured this way).

These measures are today easily overcome with widely available hacker's tools.

A new version of this standard (802.11i) aims to fill the holes of the above mentioned standards. This standard builds around the 802.1X standard, which offers the Extended Authentication Protocol (EAP) and its companion for LANs, namely, EAP over LAN (EAPoL). 802.1X is a standard for both wired and wireless networks and defines a framework on the top of 802.11. In a wireless ad-hoc network, nodes must initiate an EAPoL conversation and authenticate with each other. 802.1X also allows for session keys to protect the communication both with respect to confidentiality and integrity. The standard IEEE 802.11i was launched in 2004. Some products that support this standard are already in the market.

Cryptographic authentication and strong encryption on the channels B and E secures the communication in an insecure version of the IEEE 802.11. Thus, IEEE 802.11g may temporarily serve as an alternative to IEEE 802.11i in the demonstrator before the latter is common available.

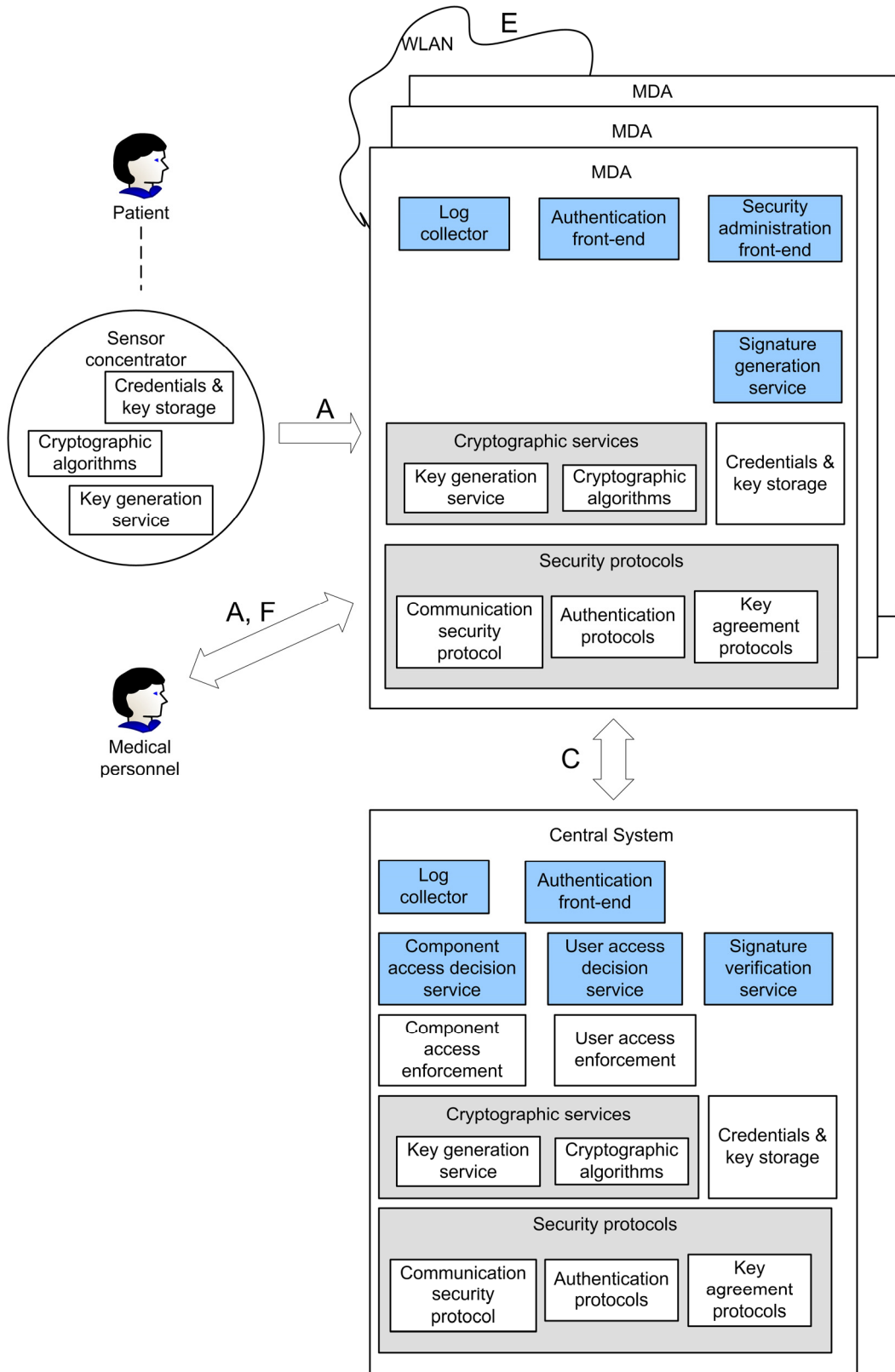


Figure 3. Distribution of Security Components in FieldCare

7 Conclusion

This section concludes the document with pointing out the most important threats against the FieldCare system and proposing the solutions to be adopted in order to counter them.

Table 7 shows the risks with highest priority from Table 4. The threats with negligible risks are left out.

Table 7. FieldCare's list of high priority risks

Risk (probability x impact)	Threat	Solution
R7** (Occasional x Large)	Jamming to disrupt the functioning of the system	Out of scope of this document
R11** (Occasional x Large)	Hijacking the session	Authentication based on PKI + symmetric key encryption (see below)
R1*/ R2* (Probable x Moderate) / (Occasional x Moderate)	Eavesdropping on the communication on the scene of the accident with no malicious (e.g., journalists) / malicious intention	Symmetric key encryption
R3*/R5* (Occasional x Moderate)/ (Remote x Large)	Device theft to get knowledge of / to introduce wrong information	Out of scope of this document (Work procedures)
R9*/ R10* (Remote x Large)/ (Remote x Large)	Bugs in the system software resulting in the disruption of the functioning of the system / refusal of access to the needed data	Out of scope of this document (adequate Software Engineering Methodology with emphasis on testing)

The table above shows that the most critical threats to the FieldCare system are hijacking the session and eavesdropping on the communication. The previous section proposed solutions for both of these threats. The solution to the first threat, involves public key cryptography (for authentication) while the solution to the second threat involves symmetric key cryptography. Note that, in some cases, the symmetric key was established using public key cryptography.

Also note that with respect to session hijacking, authentication plus symmetric key encryption will prevent a session-hijacker from introducing data in the system. This is because since he has not been authenticated, he does not know about the secret key established for encryption by the nodes participating in the WLAN, and therefore his messages will not be accepted by the system. But, this will not prevent him from flooding the network with data packages, since impersonating as a legitimate WLAN node is easily done; WLAN authentication, i.e., which data packages are accepted by a node, is briefly described in Section 6.1.

The lack of an approved CA-organization by the authorities has hindered the widespread use of public key technology. As a result, one might want to use symmetric key technology instead of public key technology for both authentication and the exchange of symmetric encryption keys.

To achieve this, one needs to have a symmetric key for each pair of entities in the system that need to authenticate with each other or need to exchange encrypted data. For this solution, one must address three issues

- an authority, person or system, to generate secret keys and record them,
- a safe off line mechanism to propagate each key to the entities in the corresponding pair, and
- to equip each entity with a secure storage for keeping the shared keys.

Since each entity in the system will most probably communicate with several other entities in the system, the entity would need to keep many secret keys and associate them with the right entity-pairs, i.e., each entity must keep a local mapping between the other entities and the secret keys it shares with them.

Moreover, to increase security, it is advisable to have separate secret keys for authentication and for encryption. This will double the number of keys needed in the whole system. In sum, the management of secret keys will be a tremendous challenge to the system.

A more practical solution would be to use public keys with each hospital having its own local CA issuing certificates to all entities in the system that need it. The only issue would be if hospitals need to communicate with each other. This can be solved by agreement between hospitals to recognize each other's CAs.

Therefore, the use of PKI for authentication and exchange of symmetric encryption keys is recommended.

References

- [1] Arnesen, R. R., Danielsson, J., Vestgården, J. I. and Ølnes, J. *Wireless Health and Care Security Architecture*. Technical Note no. 1006, Norsk Regnesentral. February 2004.
- [2] Arnesen, R. R., Danielsson, J., Vestgården, J. I. and Ølnes, J. *Wireless Health and Care Security Requirements*. Technical Note DART/03/04, Norsk Regnesentral. December 2004.
- [3] *Kravspesifikasjon for PKI i offentlig sektor* available at http://www.odin.dep.no/filarkiv/234033/Kravspek_PKI_v102.pdf
- [4] Rivertz, H. J. *Bluetooth Security*. Technical Note DART/05/05, Norsk Regnesentral. Mars 2005.
- [5] Skaar, T. I. And Thorjussen, T. E. Security Specification, Access Control and Dynamic Routing for Ad-Hoc Wireless Networks Applied to Medical Emergencies.
- [6] Svagård, I., Gorman, J., Skaar, T.I. and Thorjussen, T.E. *Wireless Health and Care – FieldCare Demonstrator Architectural Description*. Technical Report, SINTEF. December 2004.