Privacy protection in a mobile Biomedical Information Collection Service

by

Øyvind Børthus
Tomas Mikael Engh

**Thesis in partial fulfilment of the degree of
Master in Technology in
Information and Communication Technology**

**Agder University College
Faculty of Engineering and Science**

**Grimstad
Norway**

May 2005

ABSTRACT

This report presents a model in a mobile health care environment and uses a combination of existing technologies to build a privacy protection scheme. This work covers security issues in both the wireless and wired network, and proposes solutions to these issues. A framework using PKI to distribute digital certificates combined with strong encryption using the AES algorithm is described. Using this framework in combination with a RBAC model using location control we present some principles that will ensure privacy in a mobile wireless biomedical information collection service.

Keywords: RBAC, security, medical privacy, AES, location control.

PREFACE

This thesis is submitted in partial fulfillment of the requirements for the Sivilingeniør / Master of Science degree at Agder University College, Faculty of Engineering and Science. This work was carried out under the supervision of associate professor Rune Fensli and Professor Vladimir Oleshchuk.

We would like to thank our guidance councilors Rune Fensli and Vladimir Oleshchuk for advice throughout the project period.

We would also like to thank Didrik Widding at Well Diagnostics for practical information of ebXML and Khanh Tuan Le at ChipCon for ZigBee chips information.

Grimstad, May 2006.

Øyvind Børthus and Tomas Mikael Engh

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

ABBREVIATIONS

3DAM - Three Dimensional Access Matrix

3DES - Triple Data Encryption Standard

A2DP - Advanced Audio Distribution

AES - Advanced Encryption Standard

AFH - adaptive frequency hopping

AFH - Advanced Frequency Hopping

AP - Attending Physician

APL - Application Layer

APS - Application Support

AuC - Authentication Centre

BIP - Basic Imaging Profile

BTS - Base Transceiver Station

CA - Certification Authorities

CAMEL - Customized Application for Mobile Enhanced Logic

CBAC - Context Based Access Control

CDC - U.S. Centers for Disease Control and Prevention

CF - Compact Flash

CPA - Collaboration Protocol Agreement

CPP - Collaboration Protocol Profile

CPU - Central Processing Unit

CRL - Certification Revocation List

DAC - Discretionary Access Control

DES - Data Encryption Standard

DMA - Direct Memory Access

DSD - Dynamic Separation of Duty

DSH - Data Set Hierarchies

DTD - Domain Type Definition

DTE - Domain and Type Enforcement

ebXML - Electronic Business Extensible Markup Language

ECG - Electro Cardio diagram

EDGE - Enhanced Data rates for GSM evolution

EDI - Electronic Data Interchange

EDR - Enhanced Data Rate

EDR - Enhanced Data Rate

EHR - Electronic Health Record

EMS - Enhanced Message Service

FFD - Full Function Device

FTP - File Transfer Protocol

GAP - Generic Access Profile

GGSN - Gateway GPRS Support Node

GHz - Giga hertz

GPRS - General Packet Radio Service

GSM - Global System for Mobile Communication

HID - Human Interface Device

HTML - Hypertext Markup Language

ID - Identification

IPSec - IP Security

ISM band - Industrial, Scientific and Medical band

ISO - International Standardization Organization

ISP - Internet Service Provider

LOC - Location

MAC - Mandatory Access Control

MAC - Medium Access Control

Mbit - Megabit

Mbit/s - Megabit per second

MCU - Main Control Unit

MEDAC - Medical Database Access Control

MHz - Mega hertz

MIME - Multipurpose Internet Mail Extensions

MMS - Multimedia Message Service

MS - Mobile Station

NAT - Network Address Translation

NHN - National Health Network

NIST - National Institute of Standards and Technology

NSA - National secure Agency

NWK - Network

OBS - Objects

OPS - Operations

OSI - Open Systems Interconnection

P - Patient

PA - Permission Assignment

PAN - Personal Area Network

PDA - Personal Digital Assistant

PGP - Pretty Good Privacy

PHINMS - Public Health Information Network Messaging System

PHY - Physical

PKI - Public Key Infrastructure

PPTP - Point-to-point tunneling protocol

PRMS - Permissions

PSTN - Public Switched Telephone Network

QoS - Quality of Service

RAM - Read Only Memory

RBAC - Role Based Access Control

RFD - Reduced Function Device

RGP - Regular General Practitioner

SAFER - Secure and Fast Encryption Routine

SD - Secure Digital

SDSD - Spatial Dynamic Separation of Duty

SDU - Service Data Units

SHA - Secure Hash Algorithm

SIG - Special Interest Group

SIM - Subscriber Identity Module

SMS - Short Message Service

SMTP - Simple Mail Transfer Protocol

SOAP - Simple Object Access Protocol

SPINS - Security Protocol for Sensor Networks

SRBAC - Spatial Role Based Access Control

SSD - Static Separation of Duty

SSH - Secure Shell

SSL - Secure Socket Layer

SSSD - Spatial Separation of Duty

TLS -Transport Layer Security

UA - User Assignment

ULH - User Location Hierarchies

UMTS – Universal Mobile Telecommunications System

URH - User Role Hierarchy

VPN - Virtual Private Network

XML - Extended Markup Language

ZC - ZigBee Coordinator

ZDO - ZigBee Device Object

ZED - ZigBee End Device

ZR - ZigBee Router

1 INTRODUCTION

1.1 THESIS DEFINITION

There is a lot of research on new technology in electronic health care systems, and wearable sensors can be attached to the human body to record different biomedical signals, such as ECG, blood pressure, glucose analysis and respiratory parameters in a tele-home-care context. These sensors can communicate with a handheld device using a wireless interface, and the handheld device forwards the data to a database placed within the National Health Network (NHN) using mobile technology like GSM or GPRS. There are a few different proposed solutions to the technical setup of such systems using various technologies for the different parts of the system.

It is important to focus on the security aspects in wireless networks communicating to a secured database in the NHN. For access to the medical information, it is important to maintain privacy and security. A wireless environment is especially exposed to intruders, and has special challenges towards confidentiality and message integrity.

Evaluation of security protocols and algorithms can lead to new principles for protection of the recorded medical information sent from a sensor on the patient to an electronic health record (EHR) placed within NHN. A scenario should be developed in order to show the actual threats and necessary security precautions.

The Data Inspectorate has very strict rules of privacy protection; in addition there are several laws and regulations to be followed for designing a solution that can guarantee privacy protection in a mobile biomedical information collection service. This project will propose some principles which should be independent of the actual technology used in order to give general design recommendations.

1.2 GOAL OF THE WORK

The goal of this project is to propose some principles on how to maintain the security and privacy in a mobile health care network. The security and privacy has to be maintained in the short range wireless network, mobile communication, and between the different locations connected to the NHN. The principles should be independent of lower layer technologies, and hence can easily be adapted to several different scenarios.

1.3 STATUS IN RELATED WORK

There is some research on similar scenarios as ours, but the security aspects of those scenarios are very limited. CodeBlue [1] is a project under development by researchers from Harvard University and Boston University. This project group has developed a prototype structure for internal use in hospitals. This is to a certain degree similar to our scenario in the way that a patient is carrying a sensor that uses a wireless interface to transfer medical data to a PDA, and the PDA transfers the data wireless to a PC-system. The main difference from our project is that this prototype system is based on an ad hoc sensor network infrastructure. Results from experiments using CodeBlue is presented in the paper Sensor Networks for Medical Care [2], where they conclude that an important shortcoming of the CodeBlue project is a lack of security.

A project focusing on the security in sensory networks is SPINS [3]. SPINS describes possible methods to solve the security problems associated with wireless medical sensors. Some of the problems arise because of limited processing power, and this limits the use of long crypto keys and heavy algorithms. This paper proposes methods to use in sensor network environments. SPINS consists of SNEP and Tesla. SNEP deals with data confidentiality, two-way data authentication and prove “fresh data”. Tesla deals with authenticated broadcasting for severe resource limited environment.

Besides SPINS [3] and CodeBlue [1] we have found very little information about projects relating to our research problems. Most projects are currently only focusing on the sensor itself, and do not take the security and privacy problems related to using such sensors into considerations. This may be because they don’t need heavy security, or they don’t yet have a working solution. Very limited official information is available on the security aspects in related scenarios.

1.4 REPORT OUTLINE

Chapter 1 is the introduction of the project. It includes the background for the project, the thesis definition, our goal with this project, and the status in related work.

Chapter 2 describes our scenario. It gives a description of how a wireless sensor is used, how the data it records is handled and stored, and how this data is used by medical personnel to help the patient. This chapter also gives a few important elements restricting our solution. It states research questions that describe what areas we aim to research and what issues are most important in that area.

Chapter 3 presents the laws and legislations relevant to a security solution in a medical environment. This chapter aims to describe what guidelines these laws and legislations put on our project.

Chapter 4 presents important wireless technologies. We describe the most relevant wireless technologies, and what possibilities they can give us.

Chapter 5 presents important security functions. We give a description of the most important hashing and encryption protocols, and try to evaluate their strengths and weaknesses.

Chapter 6 presents important mechanisms to ensure privacy. We describe various variants of role based access control mechanisms and how they can solve privacy issues in our scenario.

Chapter 7 contains our solution. We give propose our solution, and give a description on how we ensure security and privacy in the various parts of our scenario.

Chapter 8 contains the discussion about our solution. We discuss why we chose the various elements in our solution, and how well the solution protects security and privacy.

Chapter 9 gives a conclusion to our work and gives a brief description of elements that need further development in this project.

Chapter 10 contains references used in this report.

2 SCENARIO

2.1 GENERAL OVERVIEW OF THE SCENARIO

In this project we will try to find a solution to ensure privacy in a mobile wireless medical environment. We have defined a scenario based on information from [4], [5] and a phone interview with Didrik Widding [6] from Well Diagnostics as a starting point to help us find a solution.

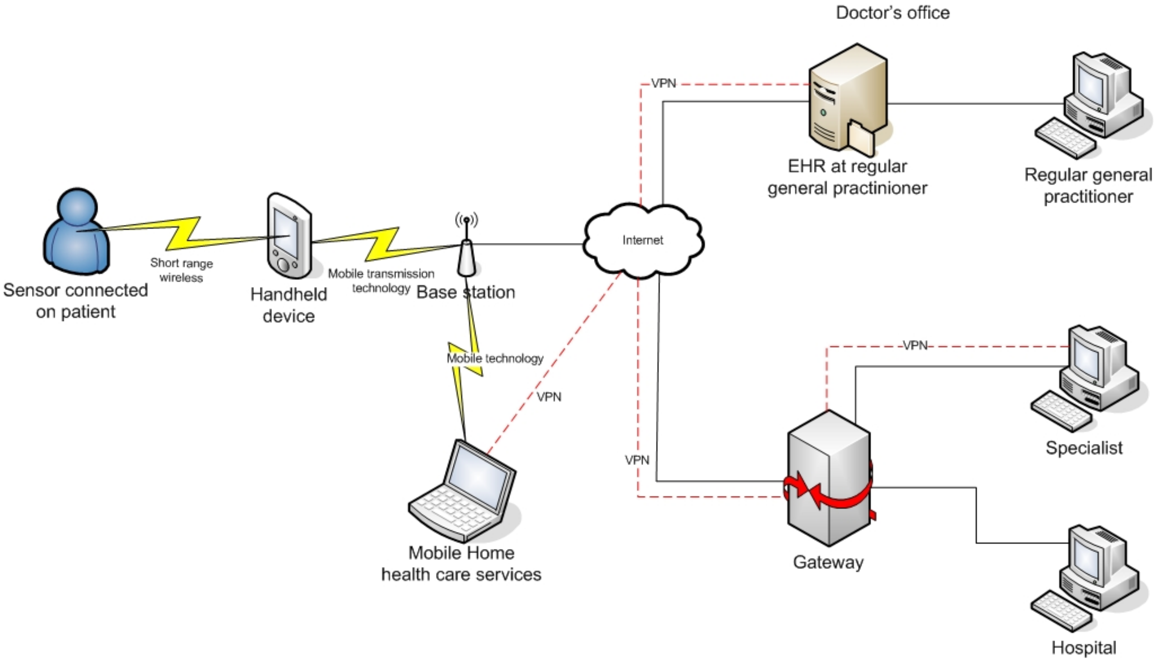

Doctor's office
VPN
EHR at regular general practinioner
Regular general practitioner
Sensor connected on patient
Short range wireless
Handheld device
Mobile transmission technology
Base station
Internet
Mobile technology
VPN
VPN
VPN
Specialist
Mobile Home health care services
Gateway
Hospital

Figure 1: Scenario

The use of a mobile wireless sensor gives the patient the possibility of being at home and doing his or hers normal daily activities while being monitored, but it also creates the need for new mechanisms for privacy protection [4]. For the patient to stay in his normal environment gives several benefits for both the patient and the quality of the monitoring. The patient will be more relaxed and the recordings will not be affected by the stressful situation at a hospital.

A mobile wireless sensor is a compact electronic electrode attached to a patient that can measure different biomedical signals. In this scenario we are using a sensor for electrocardiogram (ECG) recordings as an example. This sensor will continuously measure and wirelessly transmit sampled ECG-recordings using a built-in RF-radio transmitter. The RF-radio receiver converts the ECG-samples by the use of a microcontroller before transmitting the ECG-samples to a standard personal digital assistant (PDA). The sensor measures ECG-signals with a sampling frequency up to 1000 samples per second [86]. The signal is digitalized with 10 bit resolution, requiring up to 10 kb/s of bandwidth plus overhead to transmit to the PDA. The range of the RF-radio signal is up to 10 meters. The transmitter chip used by the sensor described in [4] is a RF-transmitter CC1050 from ChipCon, operating at 869.700 MHz, with a bit rate of up to 76.8kbit/s. The sensor will transmit continuously, and will be attached to the patient for 3 days to a week at a time. The sensor is a disposable unit, and will only be used once.

A PDA is used to receive the information from the sensor [4], and will often have 400 to 600 MHz processor, 64 to 128 MB of internal memory and a memory card with capacity of more than 2 GB for storing data. The PDA has both a short range wireless RF-radio device and a GPRS card installed. The PDA is an “intelligent” unit, using automatic arrhythmia detection algorithms for analyzing the signals from the sensor and decides if the recordings are within normal values. As long as the signals are within normal values the PDA will regularly send an extract of the recordings to an electronic health register (EHR) connected to the Internet by the use of GPRS communication. If an abnormal ECG activity is encountered, the PDA will store 1 minute of the ECG recordings and then transmit the recordings to the EHR server.

The wireless sensor will be attached to the patient by his attending physician, AP. The attending physician is the doctor with the main responsibility for the treatment and diagnostics of the patient’s current medical condition. The attending physician will most often be the patient’s regular general practitioner, but in can also be a doctor at a hospital or another general practitioner. The AP is responsible for the local EHR to where the recorded information is sent and then stored. The EHR server is located at the AP responsible for the sensor; usually this is the patient's regular general practitioners office.

The AP will use the recorded information to help make a diagnosis and to give better medical treatment. According to the Personal Health Data Filing System Act he is also the one who can give co-workers who need access to the patients' health information in order to give medical treatment [4]. The AP will have access to the information, and if needed he can request a second opinion from a cardiology specialist. This requires him to grant access to the specialist, and this might be problematic due to the sensitive nature of the information and the administrative organization of the medical system. There is also a need to grant access to mobile home health care personnel. In case of emergency the ambulance personnel might need access to information in order to give correct first aid, or a community nurse who visits the patient at home to provide daily health care.

Norsk Helsenett [5], the Norwegian national health network is a closed network for electronic communication and cooperation. Norsk Helsenett is owned by the 5 different health regions in Norway. This network connects hospitals and other medical facilities either by using a secure VPN connection or being directly connected to NHN's network. The regions do not have a common set of message types or standards, resulting in difficult communication and cooperation [5]. Several message standards are used to transport electronic medical information; a few examples are Journal+, MediLink, and InfoEDI [6] [5]. There is a wide variety of messages, depending of the data transferred. Each type of message will have different content and values, and they will be transported in different ways. These transmissions need various security and privacy protection.

2.2 RESTRICTIONS

In this scenario there are several restrictions on how we can form a solution. Due to the low processing and memory capacity of the sensor, the possible security and privacy methods and transmission bandwidth are significantly limited. Once the information is transported to the PDA it needs to be analyzed and then transmitted to the EHR. This message transportation uses mobile transmission technology and the internet in our scenario, and thus needs a stronger level of security. There are some factors we have to take in considerations when selecting security and privacy protection mechanisms; for example battery capacity, bandwidth, processing capacity, and memory in the PDA. The PDA must be able to analyze and transmit data for several days continuously. The data must be protected during the transportation but also when stored in the EHR.

2.3 THREATS

There are several security and privacy threats relevant to this scenario. From a medical standpoint it is very important that the sensor only receives data from the correct sensor, and not from other devices in the same area. Keeping the integrity of the data is also very important to avoid false alarms or incorrect normal signals. The data must also be protected in such a way that possible attackers cannot get access to personal information about the patient.

For the transmission of data from the PDA to the EHR, and between users in the national health network many of the same threats applies. Integrity, security and privacy must be protected when sending electronic messages containing sensitive medical and personal information. The electronic messages contain a lot more sensitive information than the data packets sent from the sensor and thus require a higher level of security protection. Non repudiation is especially important when sending messages regarding medication and diagnosis.

A big threat to privacy in a wireless medical environment does not come from deliberate attacks, but from within the organization. Medical personnel that has unnecessary permissions to the EHR is a threat to the patient's privacy. Access to medical journals stored in an EHR must be restricted exclusively to medical personnel that need access to a patient's medical record in order to give the patient medical treatment. There are many different roles in the health care service and they need different levels of access to information. Effective and secure ways of controlling access rights must be implemented.

In a wireless environment it is always a possibility to loose the connection between the wireless devices involved. The signal from the sensor can be hindered by walls or getting out of range, and the signal from the PDA to the base station can be lost when driving through a tunnel or other reasons, even when the user is inside the house. The loss of such signals is not a threat to privacy, but mechanisms to handle such events are important.

2.4 RESEARCH QUESTIONS

Based on the scenario, restrictions and threats described above, we have formulated several research questions:

1. What laws and legislations regulate the use, storage and transportation of sensitive medical information? Important research issues are to find out what restrictions laws and legislations have on our choice of solution.
2. What wireless transportation technologies are available and how do they suit our needs, both for a short range and a long range transmission? Important research issues are bandwidth, range, availability, coverage area and supported security solutions.
3. What mechanisms are available to ensure security and integrity during transmission? Important research issues are provable security strength, processing speed, and versatility.
4. What mechanisms are available for identification and authorization of users? Important research issues are security, user-friendliness and suitability to a distributed medical environment.
5. What electronic message standards are available? Important research issues are versatility, standardization and security.
6. What mechanisms are available to ensure confidentiality and privacy? Important research issues are adaptability and security.

3 LAWS AND LEGISLATIONS

The use and management of sensitive medical information is regulated by several laws and legislations in Norway. In [7] some relevant laws and legislations, and how they affect the use of electronic health records are presented.

The purpose of the Personal Health Data Filing System Act [8] is to contribute to giving the national health services information and knowledge without violating the protection of personal privacy. §13 in this act states that the person responsible for the EHR can grant co-workers access to the information on the EHR. Access can only be granted to persons who need information to perform treatment, and in accordance to current regulations on client confidentiality. The Norwegian Data Inspectorate has stated [11] that based on §13 accesses can only be granted to personnel within a hierarchical organization context. This ruling prohibits access to the local EHR from personnel outside of the hospitals organizational domain, for example regular general practitioners. The managing director of the hospital is responsible for the EHR and the security mechanisms needed. Before sending information from the EHR system he has to make sure the receiving organization has fulfilled all security recommendations.

The purpose of the Patients Rights Act [9] is to ensure that the population has equal access to healthcare services by granting all patients rights towards the National Healthcare Services. §5 in this act states that the patient has the rights to have access to his medical journal. Based on the intention of this act, one can claim that the patient himself is the proprietor of the information in the EHR.

The Personal Data Act [10] states: "*The purpose of this Act is to protect natural persons from violation of their right to privacy through the processing of personal data. The Act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.*" The act contains requirements to protect against unauthorized access to the EHR. Based on this act the patient can decide how he wants to be protected and to whom he wants to grant privileges to information in his medical journal.

The Norwegian Data Inspectorate [12] has announced that transport of personal information outside of the attending physicians control must be encrypted using DES 128 (3DES) equivalent or better. The Data Inspectorate has not composed any instruction on what security measures are sufficient. The liable organization must do an assessment of what security objectives and strategy is needed, and decides what an acceptable security level in the given situation is. The Data Inspectorate can however review the assessments done by the liable organization. There are no direct requirements to the software used, but these will be part of the review done by the inspectorate.

4 WIRELESS TECHNOLOGIES

4.1 SHORT RANGE WIRELESS TECHNOLOGIES

The sensor prototype used in our scenario uses an RF-radio chip with no security mechanisms implemented. Our research showed at an early stage that Bluetooth or ZigBee were clearly better choices when considering data rate and supported mechanisms to ensure security and integrity, and we focused our research on these two short range wireless standards.

4.1.1 Bluetooth

Bluetooth is a short range radio standard designed for low power consumption. It was initially developed by Ericsson, and later formalized by the Bluetooth Special Interest Group. On June 14, 2002 the Bluetooth standard was published as IEE 802.15.1. In 1998 the Bluetooth Consortium was formed by Ericsson, Intel, IBM, Nokia and Toshiba. Bluetooth is intended to replace cables for portable and/or fixed devices [13]. Bluetooth has been updated to new versions several times, and the 2 current core specification versions used now are 1.2 and 2.0 [14]. Version 2.0 is fully backwards compatible, but supports higher data rates than 1.2.

4.1.1.1 Technical characteristics

Bluetooth operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec [14]. The adaptive frequency hopping (AFH) was designed to reduce interference between wireless technologies using the 2.4 GHz spectrum. The AFH detects other devices and avoid the frequencies used and can take advantage of the available frequencies. The AFH hops among 79 frequencies at 1 MHz intervals to give high interference immunity. The range of Bluetooth devices range from 1 to 100 meters depending on the device class used. Class 1 devices use a power of 100 mW giving it a range of up to 100 meters, class 2 uses 2.5 mW and have a range of up to 10 meters, and class 3 uses 1 mW and have a range of up to 1 meter. Class 2 is the most commonly used. Version 1.2 has a gross data rate of up to 1Mbit/s and Version 2.0 with Enhanced Data Rate (EDR) has a gross data rate of up to 3 Mbps. The effective transfer rates are respectively 723.1kbit/s and 2.1Mbit/s.

4.1.1.2 Connection

Bluetooth devices communicate in small groups of up to 8 devices, called a piconet, as shown in figure 2. One device plays the “master” and the rest (up to 7) devices are “slaves”. Data can be transferred between master and 1 slave at any given time, and the master switches between slaves in a round robin fashion. Simultaneous transmission from master to multiple slaves is possible, but rarely used.

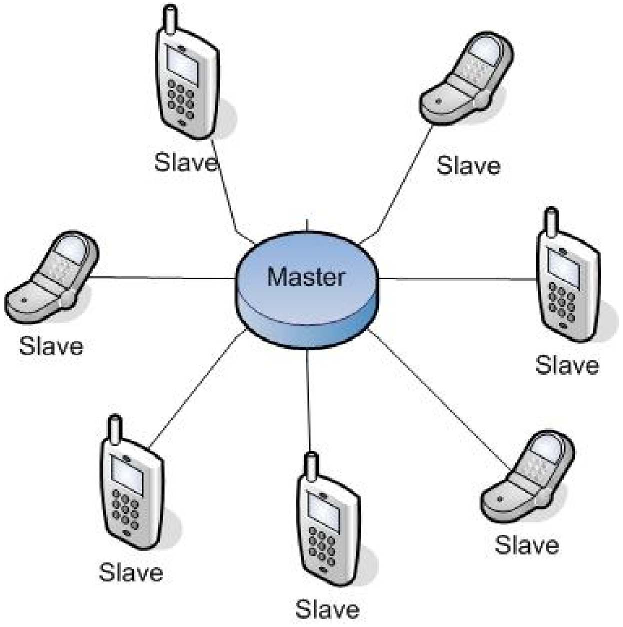


Figure 2: Piconet

A Bluetooth device will transmit the following sets of information on demand:

- Device name
- Device class
- List of services

- Technical information

Any device can perform an inquiry to find other devices with which to connect, and any device can be configured to respond to such inquiries. If the device trying to connect knows the address to the device, it will always respond to inquiries with the information mentioned above if requested for it. Use of the devices services may require pairing or owner accept, but the connection itself can be established by any device and held until it goes out of range.

All devices have a unique 48 bit address, but these are generally not shown in inquiries and instead user friendly “Bluetooth names” are used. These names can be set by the user and most devices come with a standard name set by the manufacturer. All devices also have a 24 bit class identifier, providing information about what class of device it is, for example mobile phone, headset or computer.

Bluetooth devices can be paired to establish a trusted connection. By user input (a pin code) they can learn a shared secret key known as a “passkey”. A device can then cryptographically authenticate the identity of another device. With some devices, like wireless earphones, it is impossible for the user to enter a pin code, and the device has a fixed pin code, which can be entered into the peer device. Trusted devices can also encrypt information they transmit so no one can “listen in”. The encryption can be turned off, and the passkey is stored in the device’s memory, and not in the Bluetooth chip itself. The trusted connection can be canceled by either device at any time. Devices will generally require pairing or user input before it allows a remote device to use its services.

4.1.1.3 Profiles

In order to communicate with other Bluetooth devices a device must be able to interpret certain Bluetooth profiles [14]. These profiles define the possible applications. 24 profiles are defined and adopted by the Bluetooth SIG, for example:

- Generic Access Profile (GAP) which provides the basis for all other profiles. This profile describes which features must be implemented in all Bluetooth devices, generic procedures for discovering and linking to devices, and basic user-interface terminology

- Basic Imaging Profile (BIP). This profile is designed for sending images between devices and includes the ability to resize, and convert images to make them suitable for the receiving device.
- Human Interface Device Profile (HID) provides support for devices such as mice, joysticks, keyboards, etc.
- Advanced Audio Distribution Profile (A2DP). Also referred to as the AV profile, it is designed to transfer a stereo audio stream like music from an MP3 player to a headset or car radio.

4.1.1.4 Security

On the link layer Bluetooth uses the SAFER+ algorithm for authentication and key generation, and E0 stream cipher for encrypting packets [14]. The link layer security is independent of possible application layer security.

The SAFER+ (Secure and Fast Encryption Routine) algorithm is a block cipher with block size of 128 bits, and a default key size of 128 bits[14][15]. The cipher uses 8 rounds with 4 stages; a key-mixing stage, a substitution layer, another key-mixing stage, and finally a diffusion layer. Figure 3 shows the inner structure of SAFER+, which consists of:

- KSA - A key scheduling algorithm that produces 17 different 128-bit sub keys.
- 8 identical rounds.
- An output transformation - which is implemented as a XOR between the output of the last round and the last sub key.

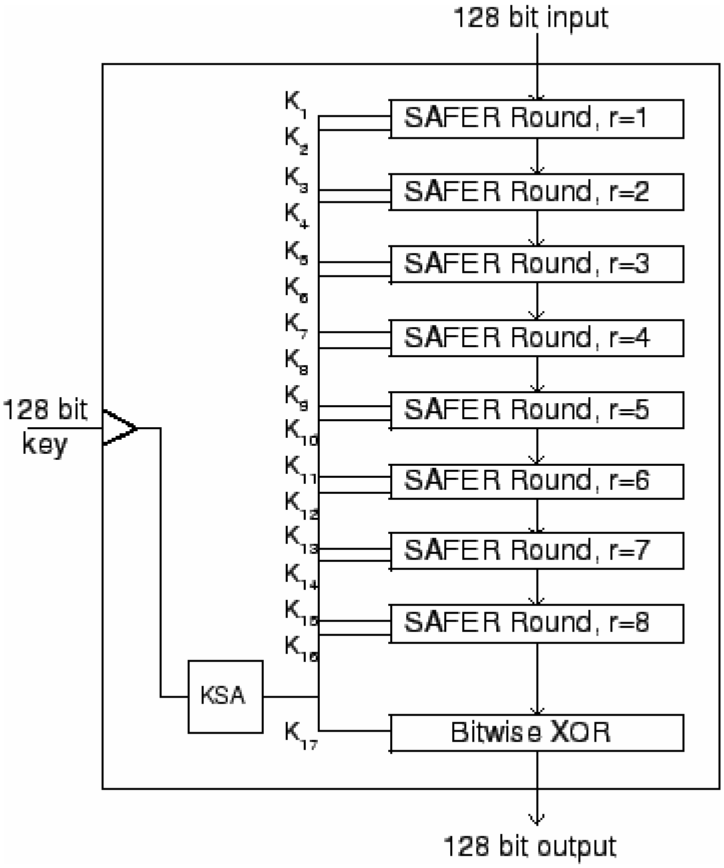


Figure 3: Inner design of SAFER+ [17]

The E0 is a stream cipher [14][16]. It generates a sequence of pseudorandom numbers and combines it with the data using a XOR operator. The key length is usually 128 bits, but may vary. For each iteration E0 generates a bit using 4 shift registers of different length (25, 31, 33, 39 bits), and two internal states, each 2 bits long. For each clock cycle, the registers are shifted and the two states are updated with the current state, the previous state and the values in the shift registers. Four bits are then extracted from the shift registers and added together. Then the algorithm XORs that sum with the value in the 2-bit register. The first bit of the result is output for the encoding.

E0 is divided in three parts:

1. Payload key generation
2. Key stream generation

3. Encoding

The setup of the initial state in Bluetooth uses the same structure as the random bit stream generator. We are thus dealing with two combined E0 algorithms. Using the 128-bit key, Bluetooth address on 48 bits and the 26-bit master counter an initial 132-bit state is produced at the first stage. The output is then processed by a polynomial operation and the resulting key goes through the second stage, which generates the stream used for encoding. The key is a multiple of 2 varying from 8 to 128 bits length. 128 bit keys are generally used. These are stored into the second stage's shift registers. 200 pseudorandom bits are then produced, and the last 128 bits are inserted into the shift registers. It is the stream generator's initial state.

Shaked and Wool showed in [17] that the PIN code used by some devices to add security can be easily broken, even on an old computer. They described a passive attack, in which an attacker can find the PIN used during the pairing process. They used less than 0.3 seconds to crack a 4 digit pin, as used by most devices using a pin code, on a Pentium III 450MHz computer and even faster on a new 3 GHz Pentium IV. If two Bluetooth devices perform pairing in a hostile area, they are vulnerable to this attack.

In august 05 Lu, Meier, and Vaudenay [18] presented an attack on the E0 stream cipher. Using a conditional correlation attack developed and optimized against Bluetooth two-level E0 they attack a recently detected flaw in the resynchronization of E0. Their best attack finds the original encryption key for two-level E0 using the first 24 bits of $2^{23.8}$ frames and with 2^{38} computations. This is the fastest and so far only practical known-plaintext attack on Bluetooth encryption.

4.1.2 ZigBee

4.1.2.1 Overview

ZigBee Alliance was incorporated in August 2002, and announced the ZigBee standard in December 2004. The ZigBee standard was released public in

June 2005. The ZigBee Alliance consists of a group of non-profit companies of leading semiconductor manufacturers, chip suppliers, wireless IP suppliers, technology providers, OEMs, test equipment manufacturers, and end-users. Since the membership is open for everyone, the ZigBee Alliance is growing rapidly. The promoters in the ZigBee Alliance are BM Group, Ember, Freescale Semiconductor, Honeywell, Mitsubishi Electric, Motorola, Philips Samsung, Siemens, and Texas Instruments. In addition to the promoters, the ZigBee Alliance has almost 200 members [19]. Other wireless transfer methods are focusing on transferring large amount of data as fast as possible, but ZigBee is going the other direction. It focuses on low powered devices with a need for security and sending small amounts of data. The ZigBee standard was created to *"enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard"* [20]. The most common devices that use ZigBee are industrial automation, remote metering, embedded sensors, medical devices, smoke and intruder alarms, interactive toys, building automation and home automation.

4.1.2.2 General technical characteristics

ZigBee operates in the European 868 MHz ISM band with one channel, the American and Australian 915 MHz ISM band with 10 channels or the 2.4 GHz ISM band with 16 channels. The data rate is 250 kbit/s in the 2.4 GHz band, 40 kbit/s in the 915 MHz band, and 20 kbit/s in the 868 MHz band [22] [27]. Transmission range is typical between 10 and 75 meters. The ZigBee protocol supports up to 65 536 nodes. It has handshaking for transfer reliability.

4.1.2.3 Stack architecture

The ZigBee stack architecture (figure 4) is based on the standard seven layer OSI (Open Systems Interconnection) model [21].

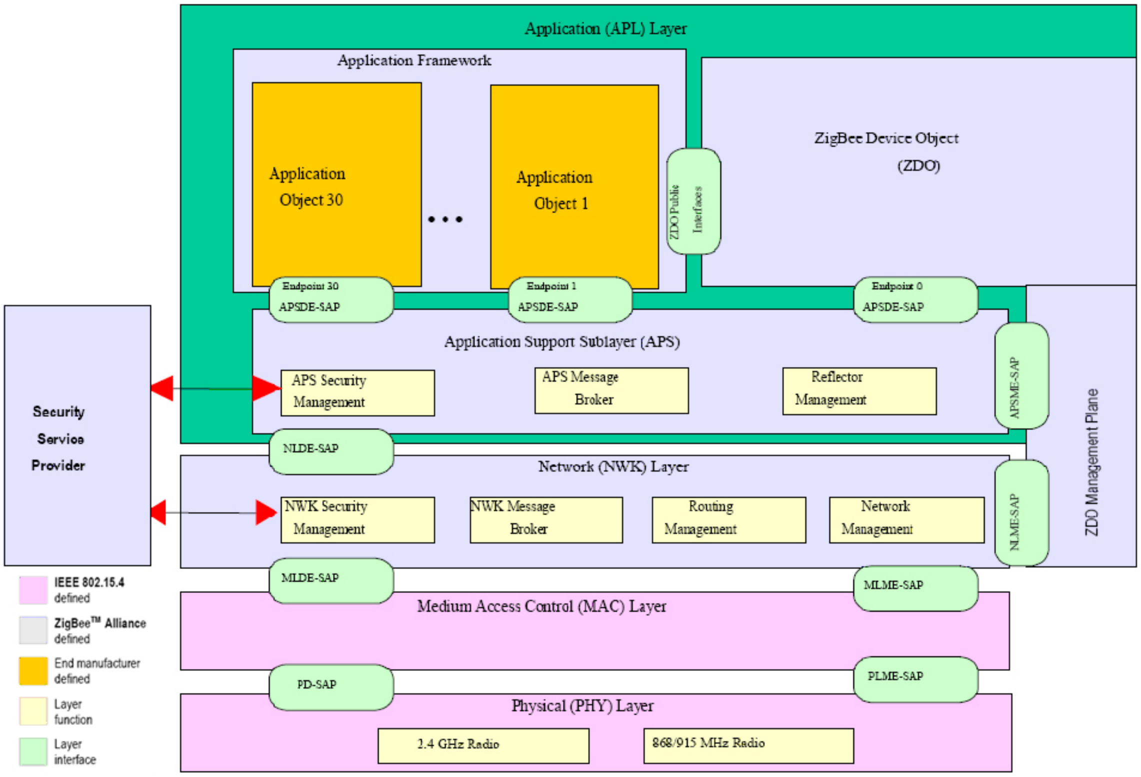


Figure 4: ZigBee stack architecture [25]

The IEEE 802.15.4-2003 standard [23] defines the lower two layers in the OSI model, the physical (PHY) Layer and the Medium Access Control (MAC) Layer. The ZigBee Alliance uses these two layers as their foundations for their development [22]. As we can see from the gray layers in figure 4, they are providing the Network (NWK) Layer and the framework for the Application Layer (APL), which include Application Support (APS) sub-layer, ZigBee Device Object (ZDO), and the manufacturer-defined application objects.

Physical Layer

The IEEE 802.15.4-2003 standard defines the physical layer. This layer operates in two separate frequency ranges, the 2.4 GHz band and the 868/915 MHz band [24]. Figure 5 shows the two layers.

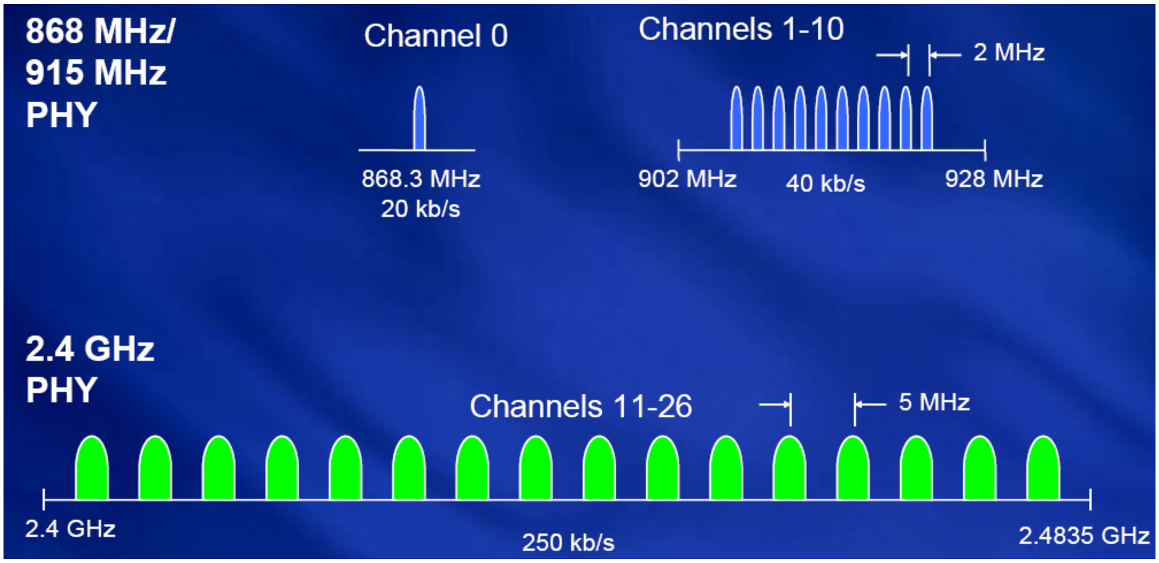


Figure 5: Data rate in the physical layer [24].

Medium Access Layer

The MAC layer in [23] is controlling the access to the radio channel. The mechanism used is called CSMA-CA. The MAC layer also transmits beacon frames, synchronization, and provides reliable transmission mechanisms.

Network Layer

The network layer has 3 main functions: join and leave networks, apply security, and route frames to their destinations [22]. In a coordinator device, the network layer has the responsibility to start a new network and discover what kind of application services nearby devices. It also assigns addresses to newly assigned devices. The network layer supports star, cluster three and mesh topology (see chapter 4.1.2.5).

Application Layer

As mentioned above, the APL layer consists of Application Support sub-layer (APS), ZigBee Device Object (ZDO) and manufacturer-defined applications [22]. The APS is responsible for maintaining the tables for binding i.e. the ability to match two devices and forward the messages between two devices. The ZDO define the role of a device in the network (network coordinator, coordinator, or end device), initiate and/or respond to binding requests, and establish a secure connection.

4.1.2.4 Security

ZigBee has several different security mechanisms [25], and are found in the MAC layer, NWK layer and the APS layer. Among them are freshness, integrity, authentication, and encryption.

- The freshness checks prevent replay attacks. It uses incoming and outgoing freshness counters that are reset every time a new key is created.
- The integrity checks prevent anyone from modifying the message, and supports up to 128 bit message integrity.
- Authentication is handled either in the network level or the device level. The network level authentication is achieved when using a common network key. This will prevent attacks from outsiders, and it has very little memory cost. The device level authentication is achieved when using unique link keys between pair of devices. This prevents attacks from both outsiders and insiders, but has a higher memory cost.
- ZigBee supports 128 bit AES encryption. This encryption can be used either at network level or device level, and is handled the same way as authentication. The encryption can be turned on or off without impacting the freshness, integrity or authentication.

ZigBee can also add security to frames. Figure 6 shows how the ZigBee Security can add headers to the data frames at the MAC, NWK, and APS layers.

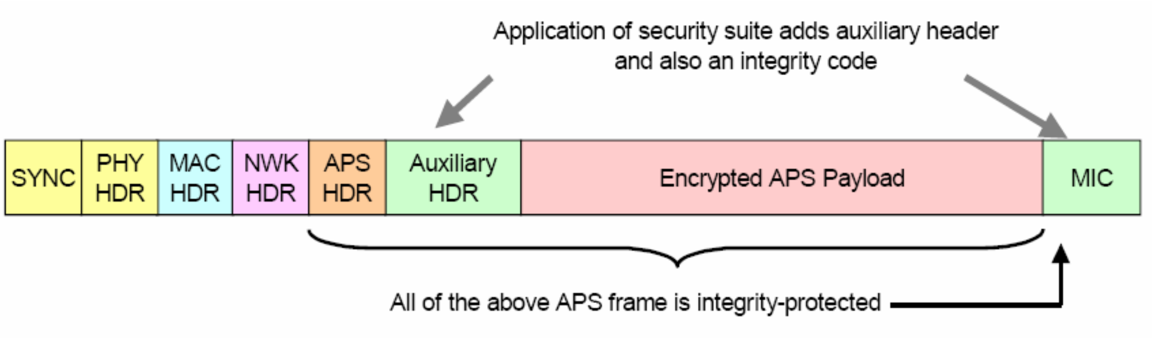

Application of security suite adds auxiliary header
and also an integrity code
SYNC
PHY HDR
MAC HDR
NWK HDR
APS HDR
Auxiliary HDR
Encrypted APS Payload
MIC
All of the above APS frame is integrity-protected

Figure 6: Security to the data frames [25]

4.1.2.5 Topologies

ZigBee supports 3 types of topologies [22]: Star, Cluster tree and Mesh.

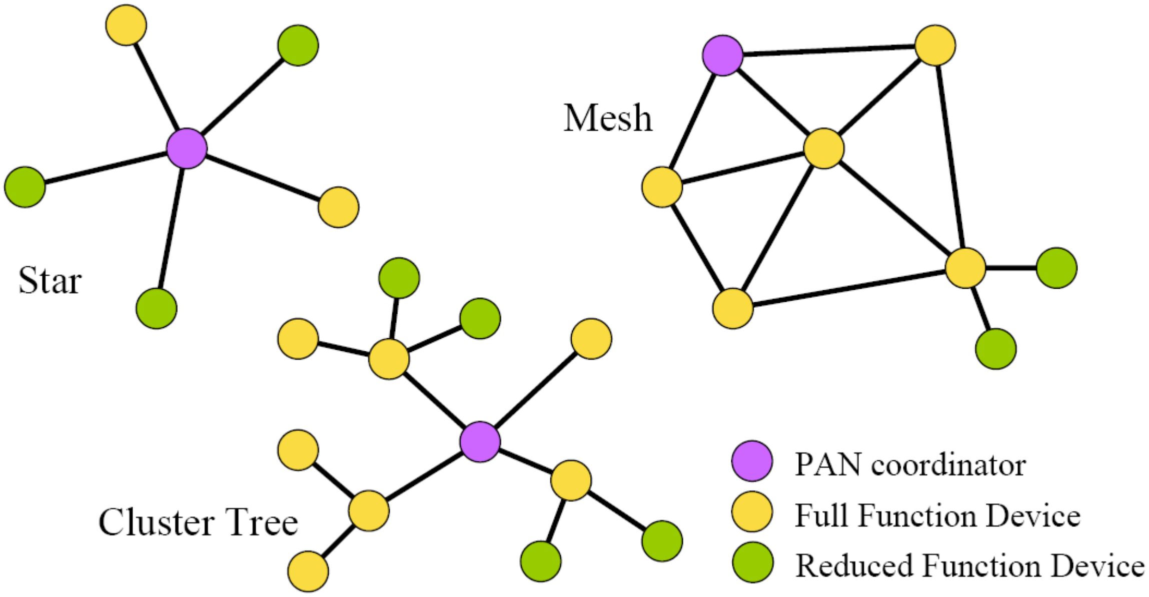


Figure 7: ZigBee topologies [22]

Star topology

In a star topology the network is controlled by a PAN coordinator (network controller). All end devices can only talk to the coordinator. The coordinator is almost always in a listening mode, except when new end devices are trying to connect. The star topology supports up to 65 536 end devices [22]. It is a very simple layout and has low latency [26].

Cluster tree topology

In a cluster tree topology [22] the tree structure is rooted at the PAN coordinator. The coordinator initiates the network, and the children (end devices) routes through parents in a hierarchy. It uses a multi-hop topology to increase the network range. The cluster tree topology is not ideal for network devices that require low latency [26].

Mesh topology

The idea with mesh topology [22] is that messages can be routed from any source to any destination. The way this is done is that every FFD is functioning as a router for all its neighbors. Like cluster tree topology, the mesh topology uses multi-hop topology to increase the network range. It has high reliability, since the messages can go many routes. If one or more of FFD disconnects, the messages still gets to the destination, but uses another route than it normally does. This way it is self configuring. Since this topology depends on the routers, it may not be ideal for battery driven networks, as the routers will have relatively large power consumption [26].

4.1.2.6 Device types

ZigBee coordinator (ZC)

Only one coordinator is required in each ZigBee network [26]. It is the most capable device in the network, and initiates the formation. It is the root of the network tree, and might bridge to other networks. It acts as a PAN coordinator (FFD) and as a router when the network is formed. The ZC also acts as a repository for security keys. The coordinator is also assumed to be the trust centre. The trust centre is responsible for allowing new devices into the network and for distributing keys. It is possible for the trust centre to be a dedicated device.

ZigBee Router (ZR)

The router is an optional component [26] in a ZigBee network. The routers associate with the ZC or with other previously associated ZR. The ZR acts as a coordinator (FFD) and is used as a local address allocation/de-allocation device.

It is used in multi-hop routing of messages. The ZR also looks after its own ZEDs.

ZigBee End Device (ZED)

The ZED contains very little functionality [26]. It is limited to communicate with its coordinator. The ZED is not allowed to associate or participate in routing. It requires the least amount of memory and is therefore cheaper than ZC or ZR. It has low power consumption since its parent puts it to sleep.

4.1.2.7 Discovering devices

When a new device is installed in the network, it will initiate queries to discover already active ZigBee devices in the network. The request is either an IEEE address request [22], which is unicast, or a NWK address request [22], which is broadcast. When the unicast request is sent, it assumes the NWK address is known. When the broadcast request is sent, it carries the known IEEE address as payload. The response on these queries is dependant on the three device types mentioned above: ZED, ZR and ZC.

- The ZED is responding the query by sending its own IEEE or NWK address.
- The ZR is responding the query by sending its own IEEE or NWK as well as the IEEE and NWK address of all the other devices connected to the ZR.
- The ZC is responding the query by sending its own IEEE or NWK as well as the IEEE and NWK address of all the other devices connected to the ZC.

4.1.2.8 Keys

There are 3 different key types [25] used in ZigBee; master key, link key and network key. The master key is used as basis for long term communication between devices, and can be either factory installed or be set up over the air or using out-of-band mechanisms. The link key is used for security between two devices. The link key is also used to authenticate devices to the coordinator device. The network key is used for security in a network. The link and network keys can be factory installed, be set up using a symmetric key-key exchange handshake or be sent from the trust center.

4.1.2.9 Hardware

A wide range of ZigBee transceivers that are suited for use in a wireless sensor are available on the commercial market, from suppliers like ChipCon, CompXs, Helicomm Inc. and others. Newer models can come with built in hardware support for data encryption and authentication using AES on the link layer. An example of such a chip is the ChipCon CC2510 [28]. The CC2510 is a powerful 2.4 GHz ISM band System-on-Chip designed for low-power and low-voltage wireless communication applications. This chip includes a dedicated 128-bit AES coprocessor to minimize the MCU usage when encrypting. It also has a dedicated DMA controller which moves data from a peripheral (in our case the sensor) to the memory with almost no intervention from the MCU. This way the MCU workload is reduced to a minimum. The chip has a 32KB of programmable flash memory and 4KB of RAM. This chip is developed to be energy efficient and have a low unit cost.

The ZigBee device installed in the PDA will most likely be an SD or CF card. Since our PDA must have a GPRS card, which usually is a CF card, the ZigBee card will be an SD card. An example of a ZigBee SD card is produced by C-Guys [29]. They are a company that specializes in developing different SD and SDIO devices, such as SD controllers, memory cards, adapters and card readers. One of their products is a ZigBee SDIO card for use in PDA. The SDIO card is using the standard ZigBee frequency, the 2.4 GHz ISM band, has 250 kbps data rate and 10 meter range.

4.2 MOBILE TRANSMISSION TECHNOLOGIES

4.2.1 GSM

GSM (global system for mobile communication) is the most popular and successful digital mobile telecommunication system in the world. At the end of March 2006, there were 1.79 billion GSM subscribers in over 200 countries [30]. The main goal of GSM [31] was to allow users to roam internationally between mobile operators. The system should provide voice services compatible to ISDN and other PSTN (public switched telephone network) services. Since the GSM system is digital, it is considered a second generation mobile phone system (2G), and replaced the first generation analog systems. In Europe GSM is using several different frequency specters, most common are GSM 900 and GSM 1800 [32]. GSM 900 is using 890-915 MHz for uplinks and 935-960 MHz for downlinks. GSM 1800 is using 1710-1785 MHz uplink and 1805-1880 MHz downlink. Typical transmission power is 2W for GSM 900 and 1W for GSM 1800 due to smaller cell size [31]. The main GSM service is telephony, and is offering at least as good quality as analogue telephones with 3.1 kHz bandwidth. Some other services GSM provide are SMS/EMS/MMS (short message service/ enhanced message service/ multimedia message service), free emergency numbers, identification, redirection, and forwarding. The users authenticate themselves with a SIM (subscriber identity module) card rather than with the mobile station (MS). GSM 900 is allowing data rates up to 9600 bit/s for non-voice services.

GSM security

GSM offers several security services [31], and they are found either in the SIM card or the AuC (authentication centre, a separate system in the network that contains the algorithms for authentication and the keys for encryption). The SIM card stores personal data and a secret key K_i, and is only accessed with a four digit PIN number [31]. After MS authenticates itself, the MS and BTS (base transceiver station) encrypts all voice and data. There are 3 types of algorithms: A3 for authentication, A5 for encryption and A8 for generation of the cipher key. The algorithms are very weak, but it is possible for the network providers to use stronger algorithms for encryption or user can provide stronger end-to-end encryption. To encrypt the messages, a key K_c is created by using the individual key K_i and a random number by generated by the A8 algorithm. The K_c key is calculated both in the MS (SIM) and the network, and is not transmitted over the air interface.

4.2.2 GPRS

GPRS (general packet radio service) is a packet-oriented operation in the

GSM system, often called 2.5G, since the technology lies somewhere between 2G and 3G (2nd and 3rd generation mobile technology) [33]. The idea behind GPRS is that all or some GSM-channels (time slots) are combined to one channel with higher capacity [31]. While GSM was primarily designed for voice transmission, GPRS is a more data-oriented transmission. The transmission is packet-oriented so that many users can transfer data when they need it, and don't use bandwidth when they have nothing to send. This type of transmission is especially designed for frequent transmission of small volumes of data, e.g. typical web requests or web response. The overall goal is the provision of a more effective and cheaper packet transfer for typical Internet applications that rely solely on packet transfer. The ISP is usually taking charge for the data volume transferred instead of charging for the connection time [34]. By doing it this way, the user is "always on", and no connection has to be set up for the transfer.

For each new GPRS radio channel, the GSM can locate between one and eight time slots within a TDMA frame [31]. All time slots can be shared by the active users. It is possible to get a transfer rate to 170 kbit/s if you have max slots and are using the fastest coding, but a more realistic bit rate is 30-80 kbit/s [33]. CS-4 is the fastest coding scheme, but the least robust. This coding is available near the Base Transceiver Station (BTS). CS-1 is the slowest coding scheme but is most robust and is available when the Mobile Station (MS) is further away from the BTS. The GPRS operators usually reserves at least one time slot per cell to guarantee a minimum data rate. Table 1 [31] shows the typical data rates for GPRS if used together with GSM.

Table 1: GPRS data rates in kbit/s

Coding scheme	**1 slot**	**2 slots**	**3 slots**	**4 slots**	**5 slots**	**6 slots**	**7 slots**	**8 slots**
CS-1	9.05	18.2	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	80.4	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	93.6	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	149.8	128.4	149.8	171.2

Users can specify a QoS-profile themselves. This determines the service precedence (high, normal, low), reliability class and delay class of the transmission and user data throughput.

The latency of GPRS is incurred by channel access delay, coding for error correction, and transfer delay in the fixed and wireless parts of the network. Due to these parts involved, the latency is very high, even with small packet sizes [31]. A round trip is often higher than 1 sec, even with packets as small as 128 byte. Table 2 shows some examples of the delay classes with different service data units (SDU) sizes.

Table 2: Delay classes in GPRS according to [35]

	SDU size 128 byte		**SDU size 1024 byte**	
Delay class	**Mean**	**95 percentile**	**Mean**	**95 percentile**
1	<0.5 s	<1.5 s	<2 s	<7 s
2	<5 s	<25 s	<15 s	<75 s
3	<50 s	<250 s	<75 s	<375 s

GPRS Security

A MS (Mobile Station) that are using GPRS are considered a part of the internet and are assigned a private IP address [31]. The operator translates the IP address into global addresses at the GGSN (Gateway GPRS support node) using a NAT (Network Address translation) [31]. The advantage of this approach instead of giving the MS an “ordinary” IP address is to protect the MS against attacks. The private IP addresses are not routed through the internet, so it is impossible to reach an MS from the internet. Other security mechanisms are the same as GSM.

4.2.3 EDGE

EDGE (enhanced data rates for GSM evolution) is a digital enhancement of GSM, and the next step towards 3G and UMTS (EDGE is also called 2.75G [36]). EDGE is using an enhanced modulation scheme and other techniques to get data rates up to 384 kbit/s using the same carrier size and frequencies as GSM. EDGE does not require any changes in the GSM core networks, but the base stations have to be upgraded [37]. Besides better data rate, the most important addition to GSM is CAMEL (customized application for mobile enhanced logic) [31]. CAMEL [38] is an intelligent network support, and the services offered are especially effective when a subscriber is roaming between international network operators. Examples are no-prefix dialing and seamless MMS messages from other countries [37]. EDGE is backward compatible with GPRS, and will use GPRS as transmission in those areas without EDGE support. Norway's largest telecommunication company, Telenor, has very good national EDGE coverage [39], and offers a download rate of 100-200 kbit/s and upload rate of 50-75 kbit/s.

4.2.4 UMTS

UMTS (universal mobile telecommunication system) is a third generation mobile technology used in Europe and Japan, and the 3G successor of GSM [40]. To avoid very high implementation cost, UMTS try to reuse as much GSM/GPRS technology and infrastructure as possible [31]. It is especially designed for high-speed services like video telephony. All signals use the same frequency band, a 5 MHz wide band licensed to network operators [31]. The signals are multiplied with a chipping sequence which is unique to each user. If someone tries to tap the signal, it would appear as noise to him if he don't know the spreading code [31]. In its initiation phase, UMTS has a theoretical bit rate of 384 kbit/s in high mobility situations, and up to 2 Mbit/s in stationary user environments [41]. It takes twice as many base stations as GSM to achieve the same coverage, and to get fully fledged UMTS features including Video on Demand, a base station need to be set up every 1-1.5 km [31]. Some of the downsides of UMTS (as it is today) are: very poor coverage, poor battery life on the MS, impossible to provide complete UMTS features in rural areas, and lack of consumer demand for 3G [31] [40].

5 SECURITY

5.1 HASHING

Hash functions are the most versatile of all cryptographic primitives [49]. It can be used for encryption, authentication, and a simple digital signature. The typical use of a hash function is digital signatures. The idea behind hashing is to take a long string of bits (or bytes) as input, run a hash function, and produce a fixed length hash sum [43]. If you have a message (m) and a hash (h), you are signing h(m) instead of signing m. The reason for signing h(m) is that the message (m) are usually very large, up to millions of bits, but the hash function are usually between 128 and 256 bits, thus making it much faster and more effective.

One of the practical problems with selecting a hash function, is that there's only a couple methods to choose from [42]; the SHA family and MD5. There are a couple of alternatives, but they have not been tested thoroughly enough to trust them. A typical hash function is shown below.

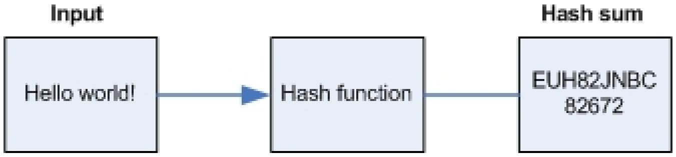


Figure 8: A typical hash function

5.1.1 MD-5

MD5 [44] is a cryptographic hash function used to verify data integrity. It was developed by Ronald Rivest in 1991 to replace MD4, because MD4 proved to have some security weakness.

When using MD5, the message is split into blocks of 512 bits [45]. The last block is padded, and includes the length of the message. MD5 has 128-bit hash value that is split into four words of 32 bits, each with a compression function *h*' with four rounds. Each round mix the message block and the state, with a combination of addition, XOR, AND, OR and rotation operations on 32-bit words. This way each message word is used four times. After the four rounds of the *h*' function, the input state and the result are added together to produce the output of *h*'. The structure of operating 32-bits words is very efficient on 32-bits CPUs.

One of the basic ideas behind hash functions [45] is that it is collision resistant. There are no known attacks on the MD5 function, but a collision of the compression function occurred in 1996. For modern applications, the 128-bit hash size is insufficient, and it is possible to find real collisions in about 2^{64} evaluations of the hash function. This made security experts to recommend a replacement. One of them was SHA-1.

5.1.2 SHA-0

SHA (Secure Hash Algorithm) [46] is a set of cryptographic hash functions. The first standard was just called SHA, but is now referred to as SHA-0. It was developed in 1993 by NSA (National Secure Agency) and published as a US government standard. It was found a weakness in this function, and NSA developed a fix which they published as an improved version called SHA-1.

5.1.3 SHA-1

SHA-1 [55] is the successor of SHA-0 (and MD5) [46], and was developed in 1995. It is used in a wide area of security applications, like TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-0 and SHA-1 is based on the same principles as MD4 and MD5 [55], and produces a 160 bit message digest with a maximum size of 2^{64} bits. It is, unfortunately, 2-3 times slower than MD5.

SHA-1 has a 160-bit state consisting of five 32-bit words [55]. It uses four rounds that consist of a mixture of 32-bit operations. SHA-1 uses a linear recurrence to stretch the 16 words of a message block to the 80 words it needs, to ensure that each message bit affects the mixing function at least a dozen times.

The main problem with SHA-1 is the 160-bit result size. Collisions can be generated in only 2^{80} steps, but it is reported that it can be generated in as few as

2^{63} steps [47]

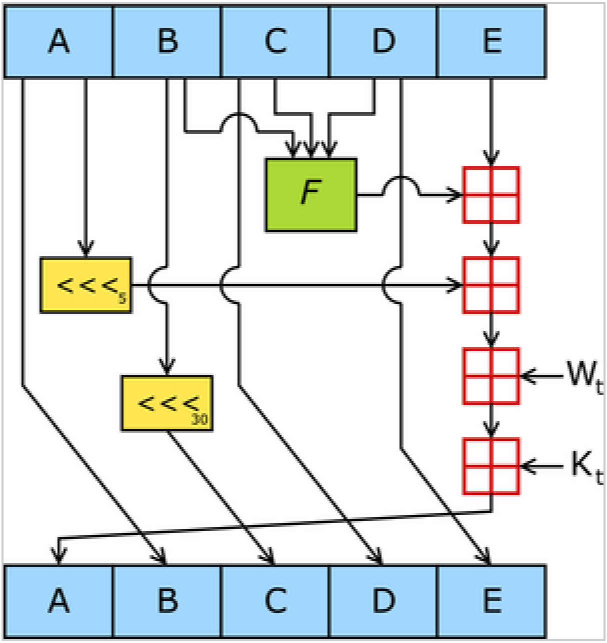


Figure 9: SHA-1. Source [46]

Description: A-E is a 32 bit word. F is a non-linear function that varies. <<<s denote a left bit rotation by s places, and s varies for each operation. ⊞ denotes addition modulo 2^{32}. Kt is a constant.

5.2 ENCRYPTION

5.2.1 3DES

The Norwegian Data Inspectorate has stated that data files have to be encrypted with at least 128 bit 3DES encryption to be counted as secure [12]. 3DES [48], or Triple DES, is a block cipher formed from the Data Encryption Standard (DES) [49] by using it three times. There are two variations of this method: 2TDES and 3TDES. The difference between them is that 2TDES is using 2 different keys, and 3TDES is using 3 different keys.

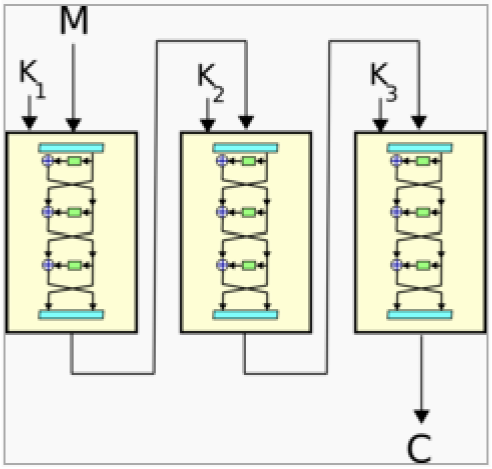


Figure 10: Three successive encoding with DES [48]

3TDES has following specification: Three 56-bit DES keys = 168 bits + parity bits = 192 bits. The effectiveness is counted as only 112 bits because of the exposure to the man-in-the-middle attacks. The best know attack on the 3TDES requires 2^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions and 2^{88} bit memory.

3TDES is not longer considered a very good encryption method. It is being replaced by its successor, AES with its better security mechanisms. AES has a larger block size, longer keys, freedom from crypto analytic attacks, and proves to be up to six times faster than 3TDES.

5.2.2 AES

Advanced Encryption Standard (AES) [50], also known as Rijndael is a block cipher. In 2000 NIST, National Institute of Standards and Technology, chose Rijndael as the new encryption standard for the US government. NIST selected the Rijndael algorithm in front of 4 other competitors based on the combination of security, performance, efficiency, ease of implementation and flexibility [51].

Rijndael is a block cipher and uses a substitution-linear transformation network with 10, 12 or 14 rounds, depending on the key and block size. The key and block size can be individually specified to 128, 192 or 256 bits. A data block to be encrypted by Rijndael is split into an array of bytes, and each encryption operation is byte-oriented. Only block size of 128 bits is adopted in the AES standard. The AES does not describe how to handle and distribute keys, and need a secure key management infrastructure to maintain its high level of security. AES is about 6 times faster than 3DES in software implementations.

5.2.2.1 Overview of the AES cipher

This overview of the AES algorithm is based on information from the AES standard [52], [49] and the wikipedia.org [50] page on AES. AES is a block cipher with a fixed block size of 128 bits and a variable key size of 128, 192 or 256 bits. The 128 bit message input block is segmented into 16 bytes. The data structure for their internal representation is a 4 x 4 matrix. Like the DES algorithm, AES comprises a plural number of iterations of a basic unit of transformation: “round”. Depending on the size of the key, AES uses 10, 12 or 14 rounds. A round transformation in AES is denoted by: Round(*State, RoundKey*).

State is a round-message matrix, and is treated as both input and output and a length of 128 bits; *RoundKey* is a round-key and is derived from the input-key via key schedule. All round-keys are 128 bits, also when the encryption key is 192 or 256 bits. The key schedule is an algorithm for computing the sub-keys for each round in a product cipher from the encryption (or decryption) key. The execution of a round will cause the elements in of State to change value. For encryption the State input to the first round is the plaintext message matrix, and the output from the last round is the cipher text message matrix. For decryption they are respectively cipher text and plaintext message matrix.

Each round, except the last round, consists of 4 stages:

1. SubBytes
2. ShiftRows
3. MixColumns
4. AddRoundKey

All rounds are identical with the exception of the final round, which does not include the MixColumns transformation. The round transformations are invertible for the purpose of decryption.

5.2.2.2 SubBytes

This function provides a non-linear substitution on each byte of State. In the SubBytes step, each byte in the array is updated using an 8-bit S-box. A substitution box (or S-box) is a basic component of symmetric key algorithms, and takes some number of input bits, m, and transforms them into some number of output bits, n. This operation provides the non-linearity in the cipher. The S-box used is derived from the inverse function over GF(2^8), known to have good non-linearity properties. Non-linearity is an important property for a block cipher to prevent differential cryptanalysis.

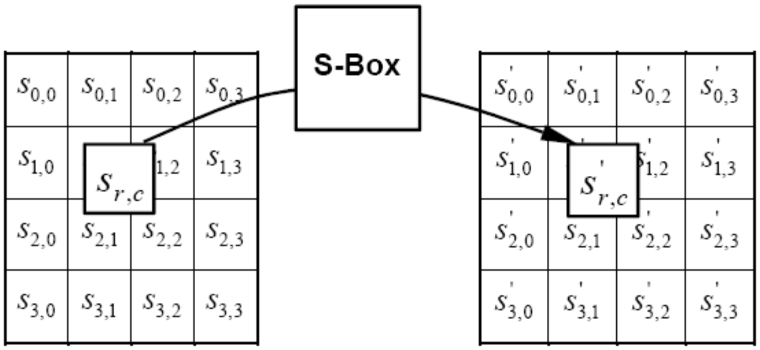
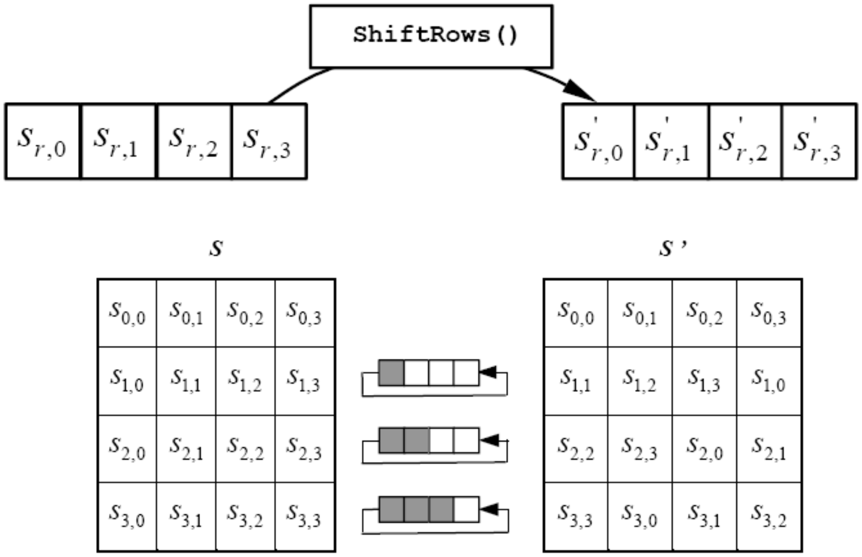

S-Box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{r,c}$ $_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{r,c}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Figure 11: AES SubBytes [52]

5.2.2.3 ShiftRows

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state.


ShiftRows()
$s_{r,0}$ $s_{r,1}$ $s_{r,2}$ $s_{r,3}$
$s'_{r,0}$ $s'_{r,1}$ $s'_{r,2}$ $s'_{r,3}$
s
s'

s			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

s'			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

Figure 12: AES ShiftRows [52]

5.2.2.4 MixColumns

In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Each column is treated as a polynomial over GF(2^8) and is then multiplied modulo $x^4 + 1$ with a fixed polynomial $c(x) = 3x^3 + x^2 + x + 2$.

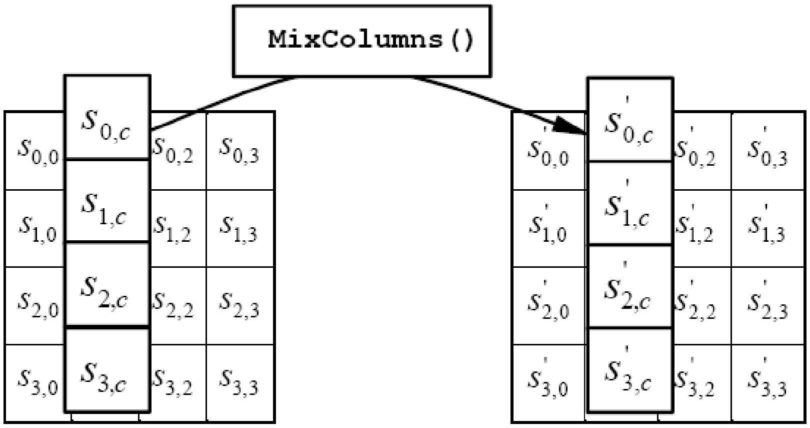

MixColumns()
$s_{0,c}$
$s_{1,c}$
$s_{2,c}$
$s_{3,c}$
$s_{0,0}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,c}$
$s'_{1,c}$
$s'_{2,c}$
$s'_{3,c}$
$s'_{0,0}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,2}$ $s'_{3,3}$

Figure 13: AES MixColumns [52]

ShiftRows and MixColumns are intended to achieve a mixture of the bytes positioned in different places of a plaintext message block.

5.2.2.5 AddRoundKey

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using the key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR. This stage provides necessary secret randomness to the message distribution.

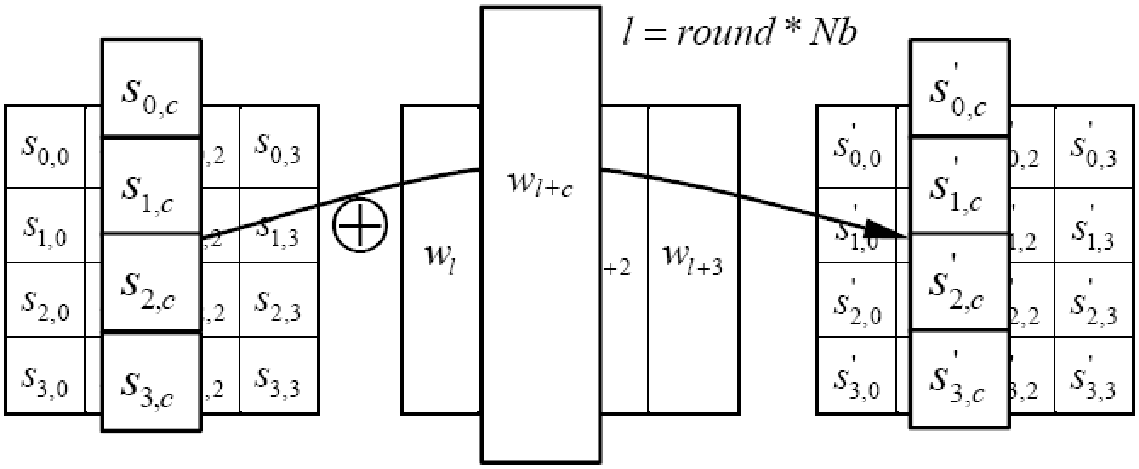


Figure 14: AES AddRoundKey [52]

To decrypt, we invert the 4 functions of each round, and implement them in reverse order. The AddRoundKey is its own inverse and the same for both encryption and decryption.

5.2.2.6 Security in AES

Three different key lengths, 128,192, and 256 are supported by AES, making it possible to choose stronger security or better efficiency. All key lengths are secure enough to be used for most levels of classified information. Only for extreme security requirements is it required to use 192 or 256 bit key lengths. The American National Security Agency has conducted a research on the strength of the AES algorithm [53] stating:

"The design and strength of all key lengths of the AES algorithm (i.e., 128,

192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths."

The security of AES can be affected by poor implementation of the algorithm itself in hardware, firmware or software, or insecure supporting key management infrastructure. The most common attacks on a block cipher are attacks on implementations of the cipher with a reduced number of rounds. As of 2006, the best known attacks are on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys. AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The [51] states that unless an attack much more efficient than exhaustive search is discovered, the AES cipher will remain secure for well beyond 20 years.

5.3 KEY MANAGEMENT

5.3.1 PKI

Public Key Infrastructure (PKI) is a policy to establish a secure method for information exchange [49]. It is also a set of integrated services and administrative tools to create and manage applications based on public keys. This includes cryptographic methods, the use of digital certificates, certification authorities, and the system to manage the process. There are two key elements [49] in PKI: Public Key Cryptography and Certification Authorities (CA).

5.3.1.1 Public Key Cryptography

Public Key Cryptography is a form of cryptography and uses a pair of cryptographic keys designed as a private key and a public key, which are related mathematically [49]. The private key is kept secret by the user and the public key may be widely distributed. Generally, if user Bob shall send a message to user Alice, Bob will contact Alice and ask for her public key. Alice sends Bob her public key, and Bob uses it to encrypt his message. Bob will then send Alice the message, encrypted with Alice's public key, and the only way to decrypt the message is to use Alice's private key [54].

Some examples of public key techniques are: Diffie-Hellmann, DSS, ElGamal, RSA, and various Elliptic Curve techniques [56].

5.3.1.2 Certification Authority (CA)

A CA is responsible for establishing and vouching for the identity of certificate holders [54]. A CA also revokes certificates if they are no longer valid and publishes certificate revocation lists (CRLs) to be used by certification verifiers. The certificates are issued by a CA based on information provided in the certification request and settings contained in a certification template. A certification template is the set of rules and settings that are applied against incoming certificate requests. The most common digital certificates in PKI use the X.509 Digital Certificate format and usually contain the following [54]:

- The user's public key
- The user's identity, such as name and e-mail address
- The validity period of the certificate
- The digital signature of the issuer, which attest to the validity of the binding between the user's public key and the user's identifier information.

There are different levels of certificates based on the need for functions. As a general rule, the higher level of the certificate, the stricter are the policies for verifying [54]. PKI supports hashing to keep the integrity of the data.

5.3.2 Smart card

Smart cards are pocket sized plastic cards with embedded integrated circuits. There are 2 broad categories of cards; memory cards and microprocessor cards [57]. The standardization of smart card systems is an ongoing process. One of the standards most referred to is the ISO-7816 standard.

A memory card contains non-volatile memory that can store information and perhaps some specific non-programmable security logic [58]. An example of a memory card is a prepaid phone card. They can also be used as a high security alternative to magnetic stripe cards. Memory cards can only perform fixed operations.

Microprocessor cards contain memory and microprocessor components. These cards can process data on the card and can used for a variety of applications. Microprocessor cards can provide secure access to networks, be used as SIM card in mobile phones and as electronic wallets [58].

Smart cards are engineered to be tamper resistant and are very suitable to hold personal digital signatures that can be used as authentication to grant access to secure networks [58].

5.4 ELECTRONIC MESSAGE STANDARDS

In the Norwegian Health Network there are several different message standards used today. The five regions have developed their own solutions to secure message structures. The “S@mspill 2007” [59] strategy is being developed to improve electronic interaction between the regions. One of the initiatives in this strategy is to develop a coordinated implementation of electronic message standards. “Kompetansesenter for IT i helse- og sosialsektoren”, KITH, [60] is responsible for developing standards for secure electronic interaction in the health and social services sector. Several standardized messages are developed for the most routine exchanges of structured information, for example epicrisis, physician referral, requisition, and laboratory test results. These electronic messages are made in conformity to different message standards, like EDIFACT, XML and ebXML.

5.4.1 EDI, EDIFACT and XML

Electronic Data Interchange (EDI) is the computer to computer exchange of structured information, by agreed message standards [61]. EDI is specific interchange methods agreed upon by national or international standards bodies for the transfer of business transaction data. The EDI standards were designed to be independent of lower layers and can be transported using standard Internet protocols like SMTP or FTP. There are 3 major standards, only one of which is international; UN/EDIFACT (United Nations/Electronic Data Interchange for Administration, Commerce, and Transport) [62].

The EDIFACT standard is developed under the United Nations and has been adopted by the International Organization for Standardization (ISO) as the ISO 9735. The standard describes the formats, character sets, data elements, and syntax to be used in EDIFACT conforming messages [62]. EDIFACT has a hierarchical structure, with the top element being a message. A message is a sequence of groups and segments. Each group or segment can be marked as mandatory or conditional, and may be specified to be repeated. A group is like a message a sequence of groups or segments. Detailed information about the various defined message standards can be found at [62]. The European Electronics industry adopted UN/EDIFACT as the global standard for traditional EDI applications.

Message standards based on XML are competing against EDIFACT. An EDIFACT message is smaller than a XML message, but the XML message is easier to understand for humans. An example of an XML based message standard is RosettaNet [63]. The RosettaNet standard is an open standard, and defines message guidelines and implementation frameworks for interactions between companies. Another emerging standard based on XML is the ebXML standard.

5.4.2 ebXML

ebXML [64], Electronic Business Extensible Markup Language, is an international initiative established in 1999 by The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the Organization for the Advancement of Structured Information Standards (OASIS). UN/CEFACT and OASIS have joined forces to initiate a worldwide project to provide a standardized way to exchange business data expressed in XML, from one computer application to another or between people and computers. ebXML is an open standard based on XML that that enables the global use of electronic business information in an interoperable, secure and consistent manner [64]. ebXML has five layers of data specification, including XML standards for:

- Business process specifications
- Collaboration protocol profiles and agreements

- Core data components
- Messaging
- Registries and repositories

The ebXML e-business framework is not in itself a standard, but is a container for several key standards administered by UN/CEFACT and OASIS. The following 5 ebXML standards are approved by International Organization for Standardization (ISO) as the ISO 15000 standard, under the general title, Electronic Business eXtensible Markup Language:

- ISO 15000-1: ebXML Collaborative Partner Profile Agreement [65]
- ISO 15000-2: ebXML Messaging Service Specification [66]
- ISO 15000-3: ebXML Registry Information Model [67]
- ISO 15000-4: ebXML Registry Services Specification[68]
- ISO 15000-5: ebXML Core Components Technical Specification, Version 2.01[69]

5.4.2.1 Business Process Specifications

One of the objects of ebXML is to capture and describe trading partners' business practices and interactions systematically, and represent them accurately and independently of any specific way of implementing those transactions. The business process specifications [64] contain the models of the interactions describing the services among trading partners. They identify the trading partners and their roles in the interactions, detail the associated messages exchanged, including the data content within such messages. The business processes used in ebXML can be captured as XML documents or represented in UML. Since ebXML specifications are designed as modules, it is optional for an industry that has already described its processes, messages, and core components to apply this specification. The development and management of business process specifications will most likely be done by industry organizations and standards bodies, and not individual companies.

5.4.2.2 Collaboration protocol profiles and agreements

ebXML uses the term collaborative process for the business process used to exchange messages or establish e-business services [64]. The ways that parties can exchange data are captured in an XML document called a *collaboration protocol profile* (CPP). These CPPs are often listed in ebXML registries and are useful in the process of finding new trading partners. A CPP indicates specific capabilities supporting business processes, with references in ebXML business process models. The CPP is an XML document describing three main functions of the company's e-business capability:

- Process specifications. Defines electronic business functions and services supported by the company.
- Document exchange. Specifies services provided to connect the process specifications to the transport functions for sending and receiving, including encryption and decryption and additional digital signatures.
- Transport. Identifies the services supported for sending and receiving e-business messages.

Because the CPPs list the capabilities of companies the intersection of them can be used to find common ground when negotiating a collaboration protocol agreement (CPA). The parties use business process definitions in the CPAs to configure their e-business systems when exchanging messages. The contents of the CPA are based on each company's CPP which makes both parties interested in making certain that the CPPs and CPAs are accurate and current. The CPPs are listed in the registry, but the CPA is a concern only to the two companies and would not likely be indexed in an industry registry open to public view. The CPA provides a set of concrete and tangible interactions between the trading partners and as a result both sides can enforce the conduct of these interactions.

5.4.2.3 Core Data Components

An important aspect of the ebXML standard is interoperability, defined here as the ability for companies in different industries to exchange and understand data among different business areas and technologies. In order to achieve this, ebXML defines a series of common data items called core components that appear in different business messages but have common meaning [64]. These common meanings enable companies using business terms in one industry to relate to their counterpart in another industry. The specification of core components can get complicated and political, and will likely be done by industry organizations and standards bodies. An example of a core component can be a person buying goods; he can be called customer, client, or end user. The context of a core component provides the specific business meaning of the data item, as determined by the business process and other variables, while the core component itself provides the basic interchangeable part.

5.4.2.4 Message Services

The ebXML message services is a standard that makes it possible to exchange electronic business documents between trading partners using standard communications protocols like HTTP or SMTP. The ebXML Message Service Standard describes the message structure used to package payload data between parties, and the behavior of the Message Service Handlers that send and receive messages [64]. The standard is independent of both the payload and the communications protocol used.

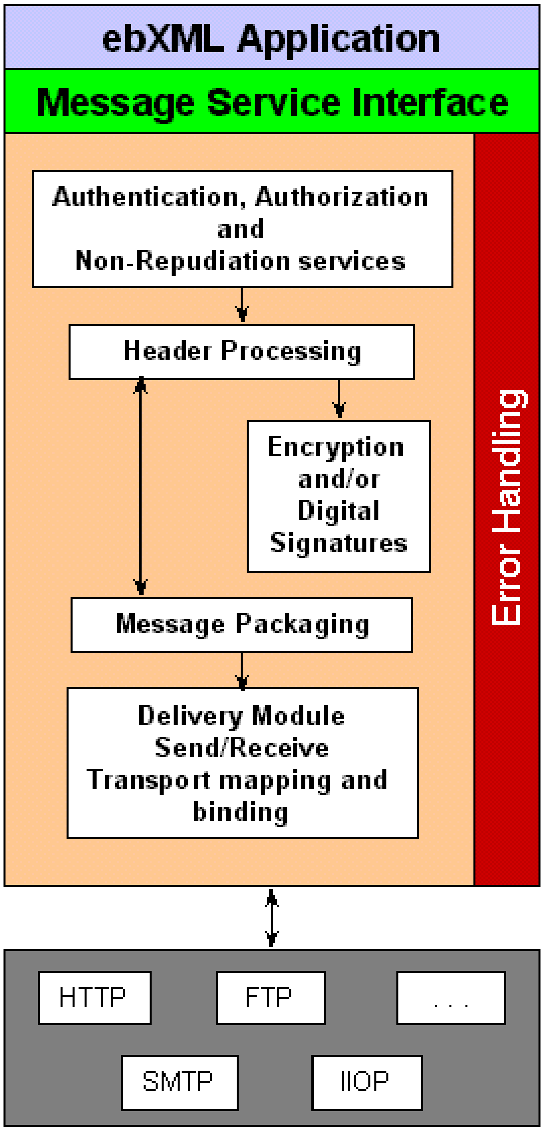

ebXML Application
Message Service Interface
Authentication, Authorization and Non-Repudiation services
Header Processing
Encryption and/or Digital Signatures
Message Packaging
Delivery Module Send/Receive Transport mapping and binding
Error Handling
HTTP
FTP
. . .
SMTP
IIOP

Figure 15: ebXML Message Service Handler Components [66]

Services

Figure 15 shows the structure of key functions provided by ebXML message services to exchange business messages between trading partners:

- Message header processing: Creates the message headers by using data from end user application, collaboration protocol agreements and digital signatures and more.
- Message header parsing: On the receiving end the message service extracts the data from the headers for processing.

- Security services: This includes creation and interpretation of digital signatures and authentication of the partners and authorization for further access.
- Reliable messaging: Defines reliable delivery of messages with rules for persistence, retries, error messages, and acknowledgements.
- Packaging: This function includes the envelopes for the messages as a whole, as well as dividing the message into containers for headers and payload.
- Error handling: This function reports an error to the parties when the message handler or user application encounters an error.
- Message service interface: Connects user applications to the message service handler.

Message Package

Figure 16 illustrates how ebXML configures the message as a series of layers. The outermost envelope is provided by communication protocols like SMTP or HTTP [64]. Everything within this envelope includes the message specifications as defined by ebXML. A MIME envelope encompassing the total soap with attachments package is the next layer in the structure. Within this package come two MIME containers, each with its own envelope, one for the ebXML headers and one for the payloads.

ebXML leaves the definition of the payload to the discretion of the sender[66]. A message can carry multiple payloads if necessary. However the message manifest, a part of the header, must list each payload in the message. The content of a SOAP envelope is defined as an XML file and includes the overall ebXML but is itself a complete basic SOAP document, and has to parts, corresponding to a SOAP header and body. The headers contain important addressing, security, and management details [64].

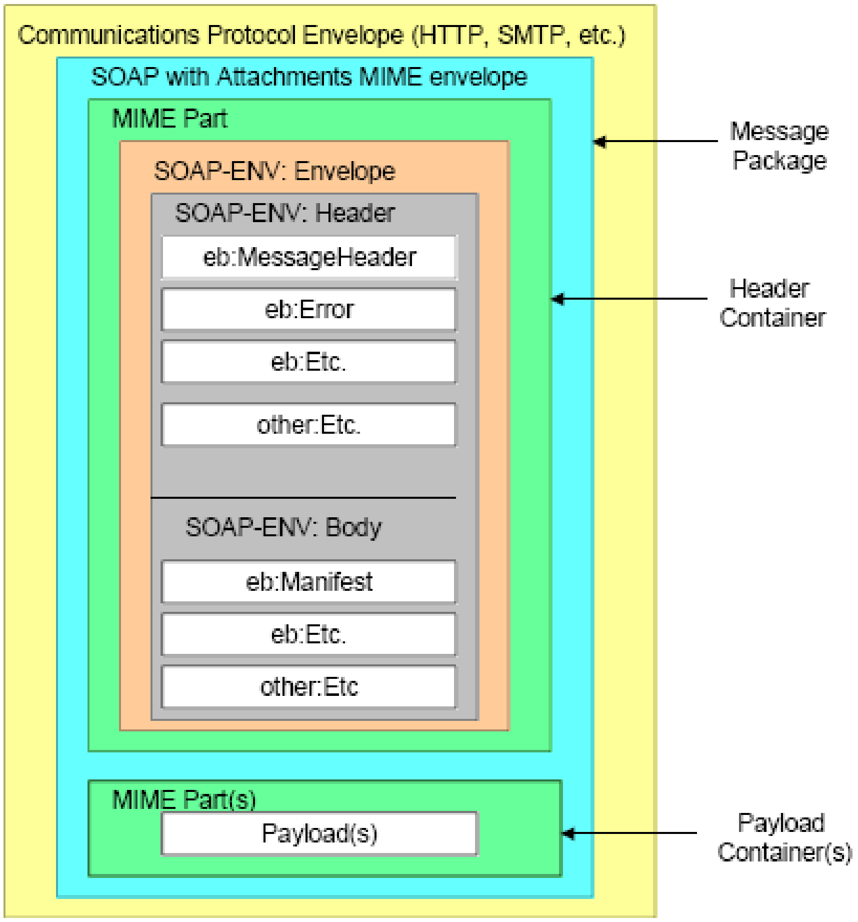


Figure 16: ebXML Message Structure

The message header is a required element and contains fields like: From, To, CPAId, Message Data, SequenceNumber, Version and other required or optional fields.

The specifications recognize and list some of the risks inherent in a business messaging service, and recommend a series of countermeasures. Inherent risks are unauthorized access, data integrity attacks, confidentiality attacks and more. Technical countermeasures discussed in the document include the use of digital signatures both on original messages and receipts, XML encryption and trusted date/time stamps. The countermeasures are either requirements or recommendations.

5.4.2.5 Registries and repositories

The terms registry and repositories are according to the ebXML registry specification [67]:

The ebXML Registry provides a set of services that enable sharing of information between interested parties for the purpose of enabling business process integration between such parties based on the ebXML specifications. The shared information is maintained as objects in a repository and managed by the ebXML Registry Services defined in the ebXML Registry Services Specifications.

The ebXML Registry architecture consists of a Registry Service and ebXML Registry Clients [64]. The Registry Service provides the methods for managing a repository. The client is an application used to access the registry. The Registry Service is comprised of a set of interfaces used to manage objects and inquiries associated with the registry. The two primary interfaces for the Registry consist of:

- A Life Cycle Management that provides methods for managing objects within the registry
- A Query Management Interface that controls the discovery and retrieval of information from the Registry.

ebXML envisions registries as open resources that companies can access at any time and find the objects they need to conduct business electronically. The objects can be DTDs, XML schemas, business process models or collaboration protocol profiles. The registries attach *metadata*, XML attributes, to the objects to classify the objects and enable management of them throughout their lifetime.

5.4.2.6 Existing implementations

ebXML has been adopted by the UK's National Programme for Information Technology (NPfIT) [70]. A central component of the National Health Service (NHS) Care Records Service is the Transactional Messaging Service (TMS) Spine using the ebXML Messaging Service OASIS Standard. ebXML is used to provide reliable messaging functionality. National services such as the Electronic Booking Service (Choose and Book) and Electronic Transmission of Prescriptions are accessed using pairs of XML request and response documents.

These documents are transported within the NHS network as ebXML messages. A gradual implementation of the ebXML services has started with the Electronic Booking Service in a few GP surgeries in London and Yorkshire. It is foreseen that by 2010 the NHS Care Record and electronic prescriptions will be fully up and running.

The U.S. Centers for Disease Control and Prevention (CDC)[71], an agency of the Department of Health and Human Services, operates the Public Health Information Network Messaging System (PHINMS), with state and local health agencies, clinical facilities and medical labs across the U.S. PHINMS makes use of ebXML's Messaging Service and Collaboration Protocol Agreement specifications.

5.5 VIRTUAL PRIVATE NETWORK

The scenario described in chapter 2.1 depends on secure data transfer between the different domains and users. Some of the data transfer uses electronic messages, but some is regular network traffic like database access. The messages can be encrypted to protect the content, but the database access needs to be protected in a secure network. In a distributed and mobile network like the one described in our scenario much of the data traffic will use the Internet, and needs to be protected.

The definition of VPN is "*A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures*" [72].

A VPN makes it possible to share resources in a secure way over an insecure public network like the Internet. There are 3 important VPN technologies used: secure, trusted and hybrid VPN. Only secure VPN is relevant to our scenario. Secure VPN uses an encrypted secure "tunnel" to transport data over a public network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data.

Tunneling allows the use of the Internet, to convey data on behalf of a private network in a secure way. There are several secure VPN protocols, like IPsec, SSL and PPTP [73]. A properly chosen, implemented, and used secure VPN protocol can provide secure communications over unsecured networks, and provide protection of confidentiality and integrity, and sender authentication to ensure privacy.

Secure authentication is very important when using a VPN solution. Authentication mechanisms can make use of what you know (pin code, password), what you have (smart card) or what you are (fingerprint, retinal scan) [73]. The use of one of the above will give weak authentication, but the use of two will give a much stronger authentication.

6 PRIVACY

"Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [74].

6.1 RBAC

Role-Based Access Control [75] is a newer model of Mandatory Access Control (MAC) [76] and Discretionary Access Control (DAC) [77]. RBAC is an approach to restricting system access to authorized users. With RBAC, access decisions are based on the roles that individual users have as part of an organization. Roles are created for various job functions. The permission to perform certain operations is assigned to specific roles. Users are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions or to get access to particular data. Figure 17 shows the RBAC model.

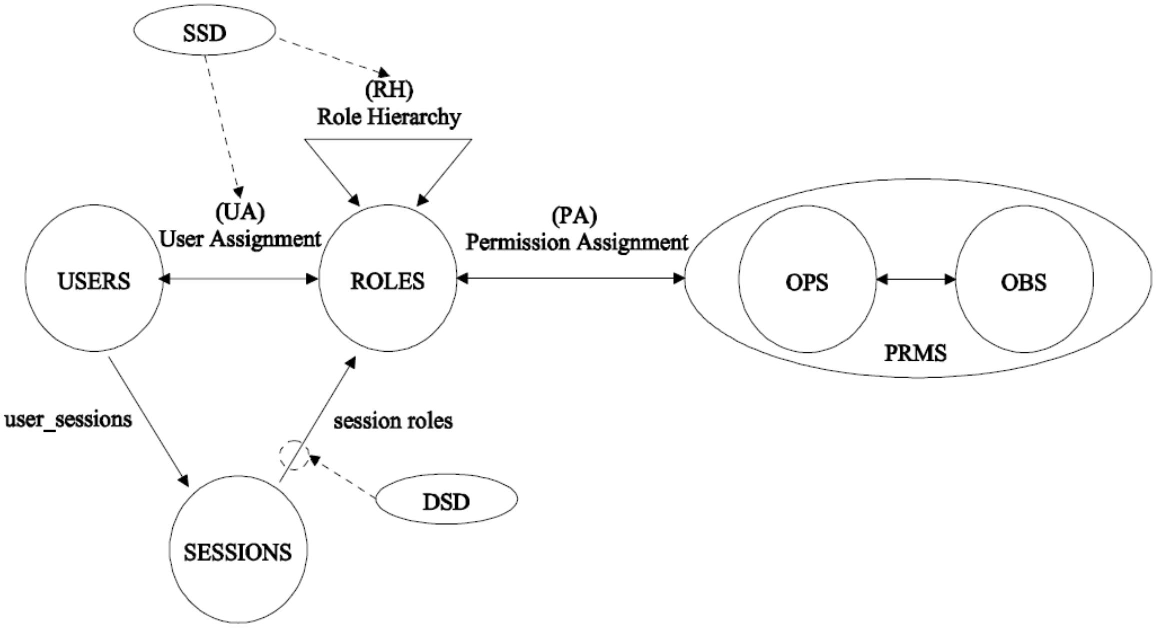


Figure 17: The RBAC model [84]

The RBAC [75] model consists of five basic elements: Users, Roles, Objects (OBS), Operations (OPS), and Permissions (PRMS). Users are defined as humans, machines, networks and autonomous agents. Roles are considered a job function. Objects are the elements the roles have permission to operate. Permissions are the rights to each role. RBAC uses two relations to model the assignments of roles to users, and permissions to roles. The relations models are called User Assignment (UA) and Permission Assignment (PA), as shown in figure 17. This way a user can have many roles, and a role can many users. Likewise, a role can be granted several permissions, and a permission can be given to several roles.

RBAC follows the concept of least privilege [75], meaning a role only has as much rights as it need to perform its duties. RBAC provides administrators with the capability to place constraints on role authorization, role activation, and operation execution. These constraints have a variety of forms. Constraints include cardinality and mutual exclusivity rules which can be applied on a role-by-role basis. The use of roles adapts well to a medical environment with doctors, nurses and other well-defined jobs. Simple administration and separation of duty are other important elements.

6.2 CONTEXT-BASED ACCESS CONTROL

A context-based access control scheme [78] begins with the protection afforded by either a user-based or role-based access control design and takes it one step further. Access control decisions in a user-based or role-based framework answer questions similar to “Should this person (or a person who performs this job function) be allowed to access this type of data?” The equivalent context based question would be, “Should this person (or a person who performs this job function) be allowed to access this type of data as it applies to this particular patient?” Context-based access control takes into account the person attempting to access the data, the type of data being accessed and the context of the transaction in which the access attempt is made.

The purpose of context based access control is to have a privacy and security policy that still allows special events to be handled correctly, without the need to create new roles or give individuals additional rights. By adding additional elements into a user based or role based access control scheme, one can develop solutions that are context based.

6.3 DAFMAT

The DAFMAT authorization framework [79] consists of two components, Hybrid Access Control Model and a Logic-driven authorization engine. DAFMAT support three types of authorization: normal, emergency and context-based. The support of these three types of authorization is the most powerful feature of DAFMAT.

The Hybrid Access Control Model is a combination of RBAC and DTE [78]. Users are assigned roles, and they get all their permissions from their given role. A user can have multiple roles and multiple users can have the same role. To implement the concepts in RBAC you need to use a lower level access mechanism. One such access mechanism is Domain and Type Enforcement, DTE [78], where subjects have a domain label objects have a type label. The users are subjects, and the attributes in a database are objects. Each Domain-Type pair has a set of allowable access modes associated to them. The data structure that gives the access modes for all Domain-Type pair is called the Domain-Type Access Matrix. The operations allowed to a subject are given by its assigned Domain.

The Logic-driven authorization engine [79] has two functions:

- The engine formulates the user authorization request based on the user actions. The request is designated one the three types (normal, emergency and context-based) of authentication.
- It approves the authorization requests if the current request is valid.

The main authorization entities in the DAFMAT model are user, role, subject, and object-type. The limitation of this framework is that it does not model purposes and data policies.

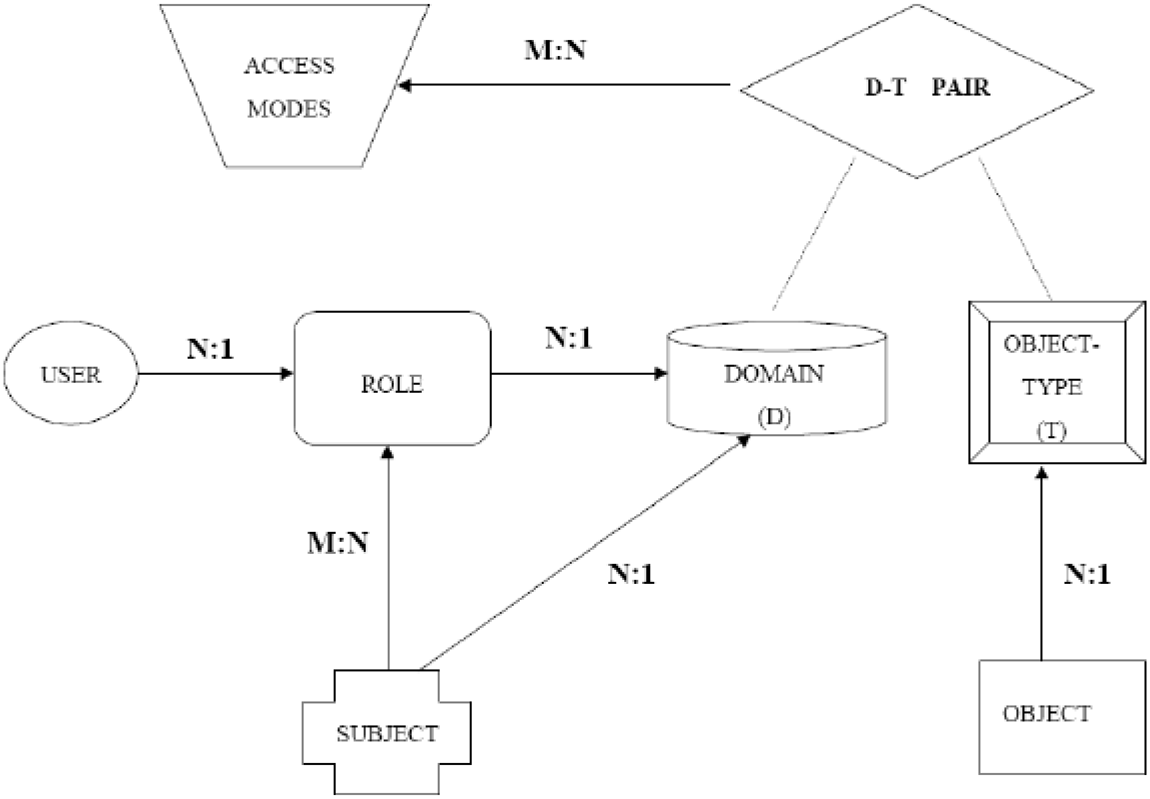


Figure 18: The DAFMAT model [79]

The tasks of the different entities are:

- **Role:** Represent the job position. The definition of a role is “a job function within the organization that describes the authority and responsibility conferred on a user assigned to the role” [80]
- **Subject:** These are programs, user agents or executables that are invoked by a user to carry out business process functions with delegation of certain roles.
- **Domain:** The domain is a high-level enterprise functional area within which role should perform. In our case this can be a doctor in a hospital who performs tasks within the hospital domain.
- **Object-Type:** An Object-Type represents a group of objects that carry related information and can be processed in a similar way.

6.4 PARBAC

Since DAFMAT [79] has some limitations on model purpose and data policy, PARBAC [81] will try to compensate these limitations by expanding DAFMAT to add the authorization entities purpose and policy. When a user requests access to certain data, the business purpose and privacy policy that pertains to that patient will be checked, in addition to his role and permission.

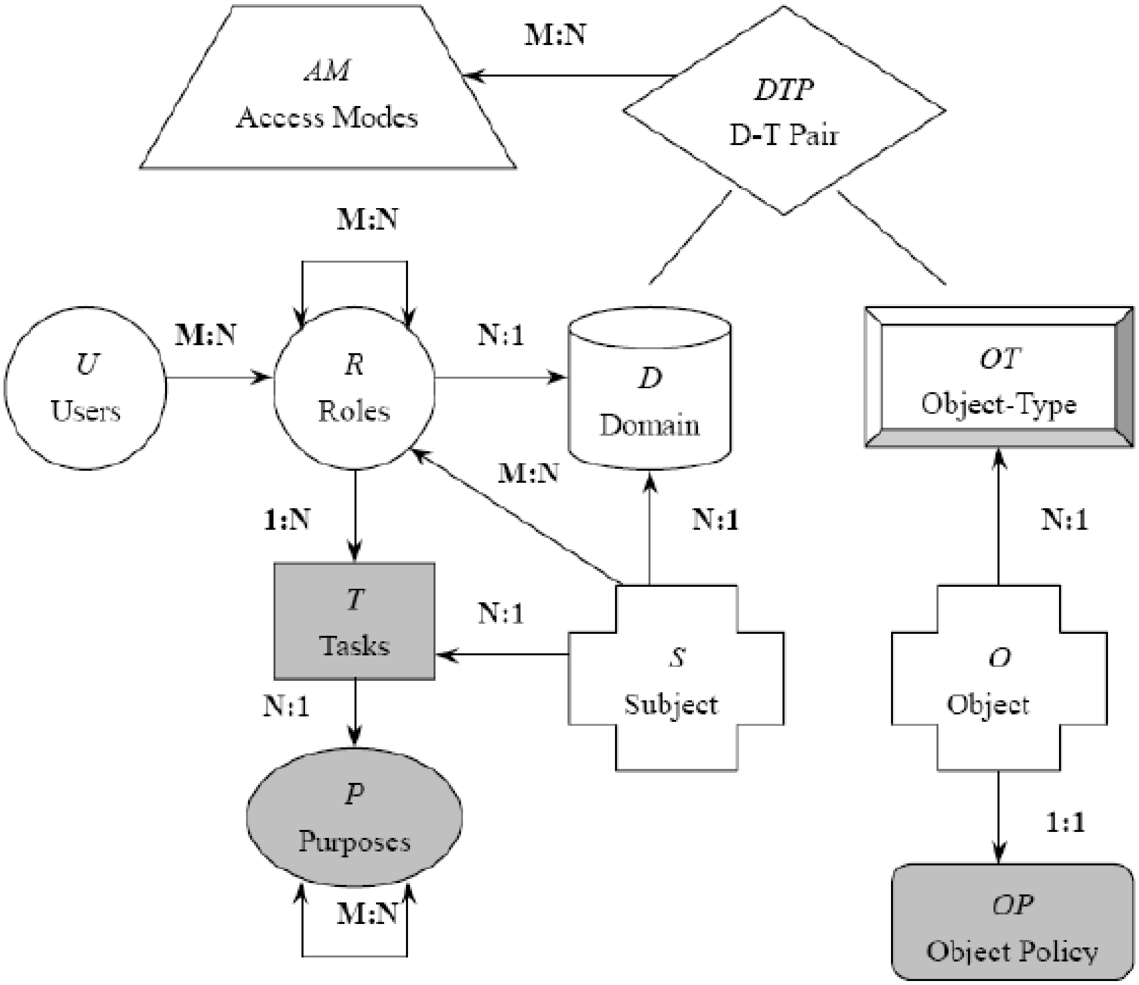


Figure 19: The PARBAC model [81]

The new entities in PARBAC:

- **Purpose**: The Purpose entity is also referred to as business purpose. This is a concrete and specific purpose of an action.
- **Tasks**: The purpose cannot be directly associated with <Role, Permission> pairs. The reason is that the system can't decide the

purpose of a role if two roles have the same permission for different purposes and a user is assigned to both roles. Tasks function as an intermediate entity between roles and purposes. A role invokes one or more subjects in order to perform some task.

- **Object-Policy**: This is a data usage policy, which means that every user's personal information should have separate policies. In our case, this policy will be based on the privacy policy of the owners of the medical database combined with the user's special preferences.

Even though this model has some features that can be used to ensure data privacy, it has its downsides too. This model is built upon a trusted system, so if the object policy is changed in any way, it may affect the security. The PARBAC model can also only protect the data privacy of the users, and does not consider other privacy issues, such as privacy invasion by data mining and anonymity. The task of implementing the logic-driven authorization engine is complicated and makes this method more difficult to implement

6.5 MEDAC

All of the security components availability, integrity, and confidentiality have to be satisfied in health care environments. MAC [76] and DAC [77] both have their limitations in achieving this security, but a combination of these two has been proved to satisfy the security requirements. This combination is a security policy called MEDAC (MEdical Database Access Control). The MEDAC security policy is based on the Bell-LaPadula security model [82]. The basic idea with MEDAC is: All authorized users will have access to the database, with its account associated to a predefined user role. The user role represents the user task in the application, and every user role has a clearance level and a category set. The category set depends on the user role and the sets of data it need to access. The clearance level represents the trustworthiness of the user role. The data sets are assigned a sensitivity level and a category set. The sensitivity level reflects its sensitivity depending on the context, content, exterior factors, or specific situations. The category sets depends on the use and the nature of the data set.

6.6 DIMEDAC

The main feature in DIMEDAC [83] is location control combined with RBAC. DIMEDAC security policy is developed to provide privacy in distributed database systems. The most important feature used to accomplish this is the user location control. The access to a certain subject from a certain location depends on the role activated by the subject, the sensitivity of the data to be accessed, and the location from where the subject is accessing.

The user location can be viewed in two ways:

a) As a site, that is a workstation from where a user logs in the system.

b) As an administrative domain, that is a part of an organization where a unique administration policy is in effect. Possible types of administrative domains in medical applications can be clinic, department, and hospital.

We assume that in distributed medical database systems each user acts in the context of an administrative domain wherein a local security policy is in effect. The privileges of a given user role should be reduced when acting remotely. Depending on whether the access is local or remote, two different ways of location control is performed, as shown in figure 20.

Local access

Layer 0: During the identification and authentication procedure the site of the user is assigned as the initial set of user locations. The final set of user locations depends on the user role that will be activated during the next layer 1.

Layer 1: The user activates a role, from the set of initially defined roles at his home-location that corresponds to his specific task. The possible user locations related to the activated user role are added to the user location set. The final set of user locations is used in subsequent remote accesses during the same session.

Remote access

Layer 0: During the identification and authentication procedure the user has to be identified to the remote site of the distributed database. However, the home site of the user could also perform the remote user identification and authentication.

Layer 1: The user activates a similar (or the same) user role in the target-site, depending on the specific user task and the trustworthiness of the administrative domain from where the user is accessing. The activated remote user role forms the ability of the user to access a number of data sets at the target-site, on the basis of the need-to-know requirements of the user that have been already satisfied by his local security administrator. However, this fact means that every local security administrator can decide about the authorization of subjects of its administrative domain on objects of other domains. It is obvious that there must be a limit in the penetration that other administrators can do in the access control policy of each administrative domain. This can be accomplished in the next layer by eliminating the user role permissions set on the basis of the assigned set of user locations.

Layer 2: For each subsequent user access request, the set of permissions to be examined is related not only to the specific user role but also to the set of user from where the user is accessing.

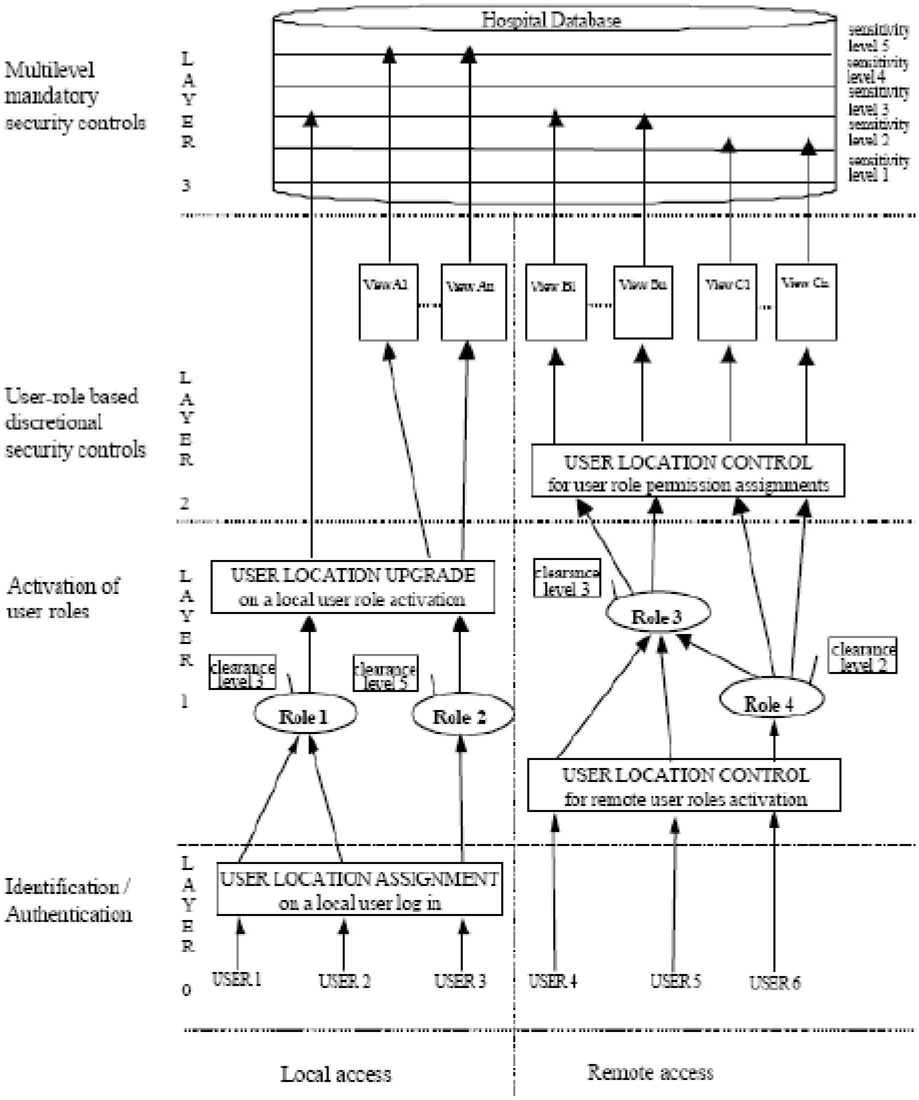


Figure 20: The DIMEDAC model [83]

DIMEDAC is defined on RBAC components and supports both MAC and DAC [83]. The access control mechanisms are the hyper node hierarchies and the three dimension access matrix. Hyper node hierarchy concept is a way of associating users, data or locations with their given security level. There is a strong similarity between the concept of a security label (consisting of the security level and the set of categories) and a role. As a result, security levels can be implemented by means of the position (depth) of each role in the hierarchy and categories can be derived from the ancestor nodes reached when moving to the root of the hierarchy. All hyper nodes are connected by a link or a branch. Hyper nodes connected by branches constitute a hyper node hierarchy (HNH, figure 21), where multiple inheritances are supported. The HNH concept is used to construct User Role, Data Set, and User Location hierarchies.

The User Role Hierarchy (URH) includes at least the role "All Users", in the lowest level. We then add roles to appropriate levels and connect them with links and branches. The nodes at the top of the hierarchy have the lowest level of clearance. To derive a clearance level we initialize the level to be 1 and the category to be an empty set. We then find the entry of the role and move towards the top of the hierarchy, adding 1 to the level every time we follow a branch to a higher level. This is repeated until we reach the role "All Users" and have all nodes that combine the category set.

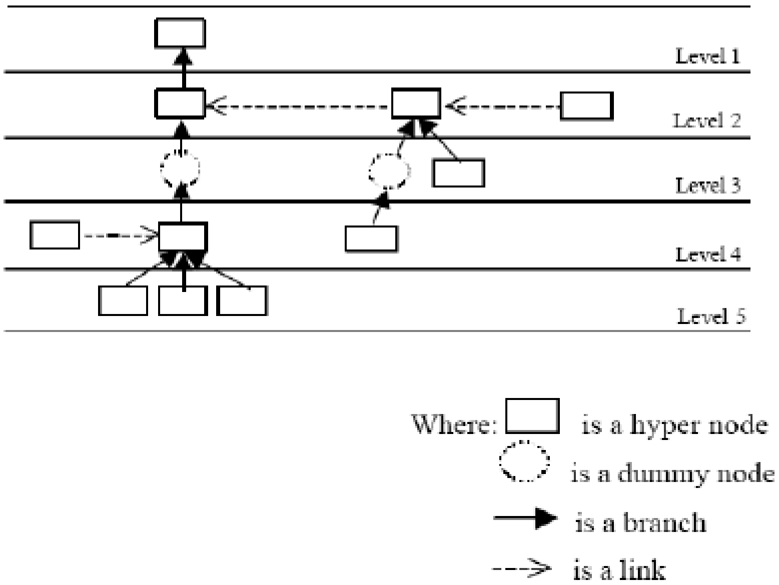


Figure 21: Hyper Node Hierarchy [83]

Data Set Hierarchies (DSH) are constructed in a similar way, except that the data sets on top of the hierarchy are of the highest level. To derive the sensitivity level we initialize the level to 5 and subtract while moving to the top of the hierarchy.

User Location hierarchies (ULH) have the highest domains at highest levels and sites as leaves. Locations can be either physical locations or organizational domains.

When we add the user location dimension to a classic access matrix we get a three dimension access matrix, 3DAM (Figure 22).This matrix can be implemented as multiple access matrices, one for each administrative domain. A user role UR in a user location UL has the authority to access data set DS with an access mode AM. An authorization rule of this kind can be expressed with a quadruple (UR, UL, DS, AM).

In a large distributed system, it is difficult to have a centralized administration of access rights. DIMEDAC proposes a use of global and local access control mechanisms. Authority to administer regional objects can be granted to the regional security administrator. Control over the regional administrators can be centrally administered, but they can have considerable autonomy within their regions. This process of delegation can be repeated within each region to set up sub regions and so on. By separately defining each one subject (global or local user role) and its permission set to access remotely any defined object of the system from any defined location we can reduce authorized privileges of a given global user role. The perspective is to reduce authorized privileges of a given global user role while its location is going farther on.

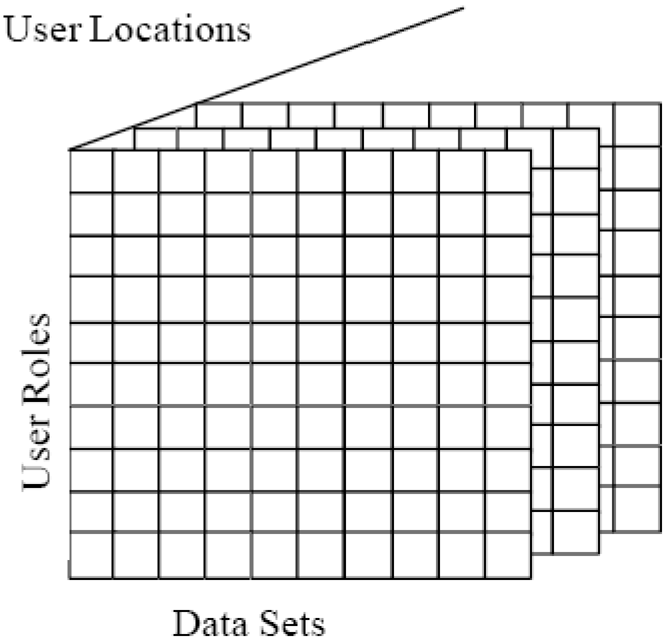


Figure 22: The three-dimension access matrix (3DAM) [83]

Each administrative domain will inherit catalogues and hierarchies of user roles, data sets and user locations from their ancestor administrative domains. Then these hierarchies will be defined to meet the special needs of the specific domain. By exploiting the inheritance in the hierarchies it is possible to reduce the huge amount of data that needs to be defined, and make it easier to manage rights in all domains.

6.7 SRBAC

SRBAC (Spatial Role-Based Access Control) [84] is basically a RBAC model [75] with a location control extension, as shown in figure 23. The location control used in SRBAC is assigning permissions to a role limited by the location in which the user is situated. A user can therefore have different permissions for two or more locations, which is called a dynamic role. The SRBAC model [84] consists of five basic components: *Users*, *Roles*, *Permissions*, *Sessions*, and *Locations*. *Users* are the units that can establish a connection with the system resources to perform activities. *Roles* are a set of permissions to access system resources. *Permissions* are the approvals to perform operations on one or more RBAC objects. *Sessions* are a symbolic expression of a user's session.

Locations are a symbolic expression of where the user is. SRBAC use a concept called *logical location domains*. This is a method to reflect an organizational location infrastructure and organizational security policy. The SRBAC controls a whole domain which consists of many partitions where a partition is normalized set of locations. The UA (user assignment) represent a user to a role. The PA (permission assignment) represents the permissions based on roles and location.

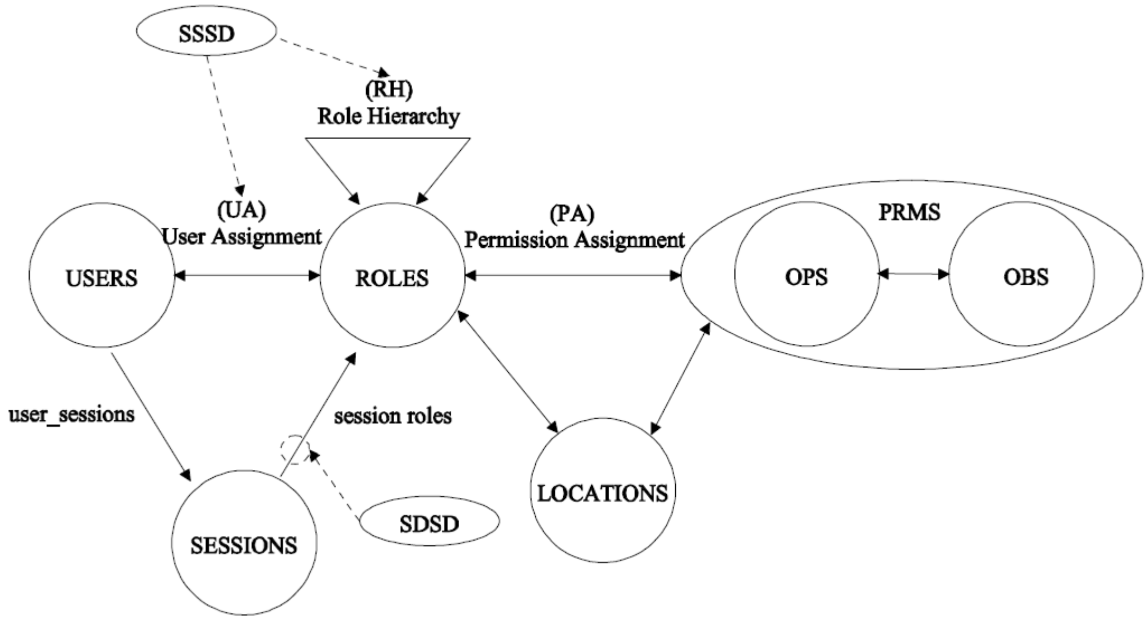


Figure 23: SRBAC model [84]

SRBAC utilizes a location dependant role hierarchy similar to standard RBAC [84], but with the location element. A role r_i inherits all permissions from role r_j in location L if all permissions of r_j in location L are permissions of r_i in location L and if L is a normalized set of locations (a partition). Two roles with the same permissions can be mutually exclusive for one location, but the user can have authorization for both roles in another location. The model is thus defined as both *Spatial Static Separation of Duty* (SSSD) relation and *Spatial Dynamic Separation of Duty* (SDSD) relation [84].

SSSD relations enforce constraints on the assignment of users to roles regarding their location [84]. If a user is assigned to a role with special permissions on one location, the user cannot be assigned to another role in the same location if the roles are in conflict with the each other.

SDSD relations enforce constraints on the permissions assigned to roles that are activated of a user's session [84]. It allows users to be assigned to several roles when activated in separate sessions for specified locations, if the roles are not in conflict with each other.

7 OUR SOLUTION

7.1 OVERVIEW

In this chapter we will present our proposed solution to protect privacy in a mobile biomedical information collection service. Figure 24 show an overview of the system. We suggest using the ZigBee standard for communication between the sensor attached to the patient and the PDA. ZigBee has built-in support for our recommended cryptographic algorithm AES. We recommend the use of AES encryption with a key size of 128 bits to ensure the integrity and confidentiality of the transmitted recordings. The PDA will analyze the recorded data and transmit an excerpt to the local EHR located at the attending physician's office (which most often is the RGP, as mentioned in chapter 2.1) using the GPRS standard for mobile data service. Transmitted excerpts will be sent using message packages conforming to the ebXML message standard. ebXML is also to be used for all messages sent internally in the National Health Network and for information transport to and from external users like general practitioners and mobile health care services like ambulance personnel and community nurses. Several different message types will be used and the various defined ebXML message structures will be maintained and distributed by a central registry and repository located in the national health network. The content of the ebXML messages will be encrypted using the AES cryptographic algorithm with a key size of minimum 128 bits. We propose key management using a PKI system with digital certificates issued by a central certificate authority located within NHN. These digital certificates will be used to generate and distribute session keys for the AES encryption/decryption scheme used to protect the message content. All messages will be signed using the digital certificates.

Access rights to the medical databases will be controlled using a role based access control system. We propose an implementation of a location control in the RBAC server to limit the access of medical information to those who actually need access, i.e. qualified medical personnel in the right locations.

To improve security and privacy protection in the system, medical personnel will be required to identify themselves using a smartcard with a personal certificate to access the most sensitive patient information on the EHR.

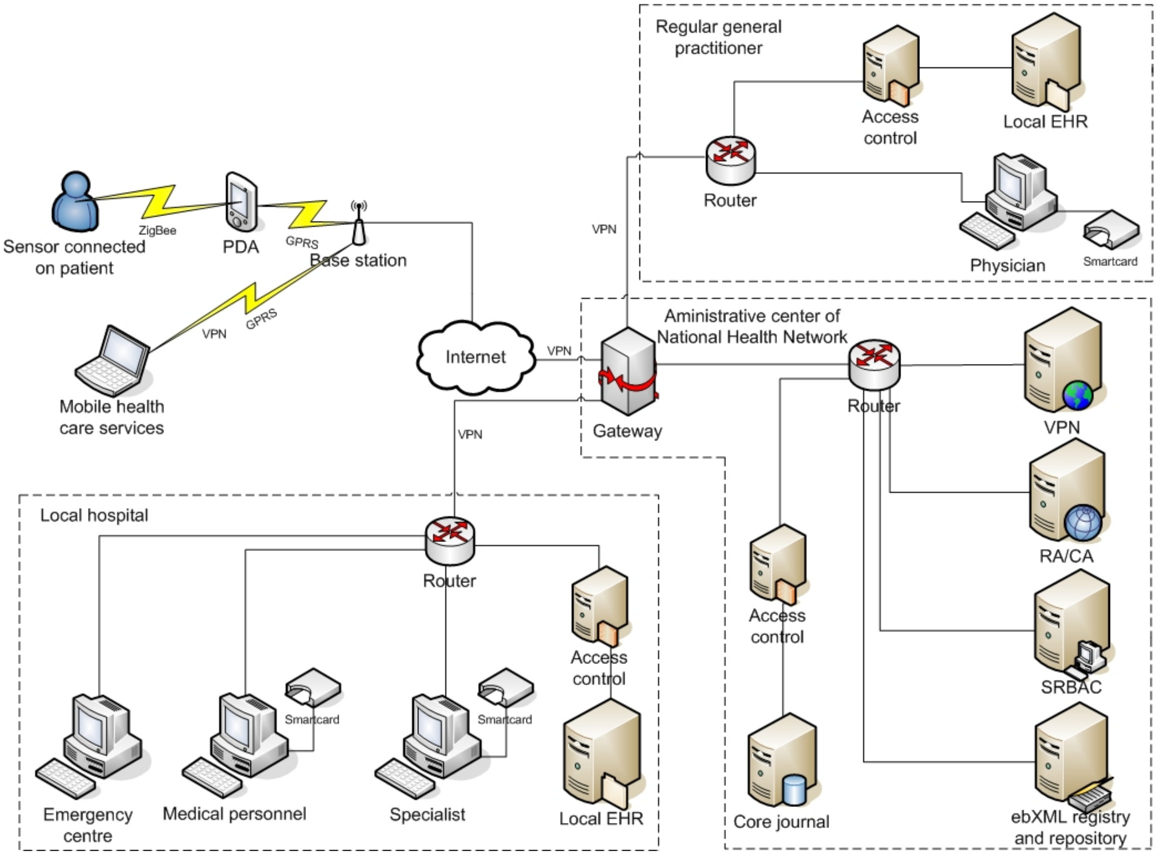


Figure 24: Our solution

7.2 SHORT RANGE WIRELESS COMMUNICATION

7.2.1 Topology

We are suggesting the use of ZigBee in a star topology (figure 25) for the short range wireless communication channel. The PDA is a full function device (FFD), has the responsibility as a network coordinator, and it may talk to any other devices. The sensors are reduced function devices (RFD), and can only talk to the network coordinator (PDA). It is easy to implement star topology and the ways RFD’s and FFD’s are handled make this a very power efficient topology.

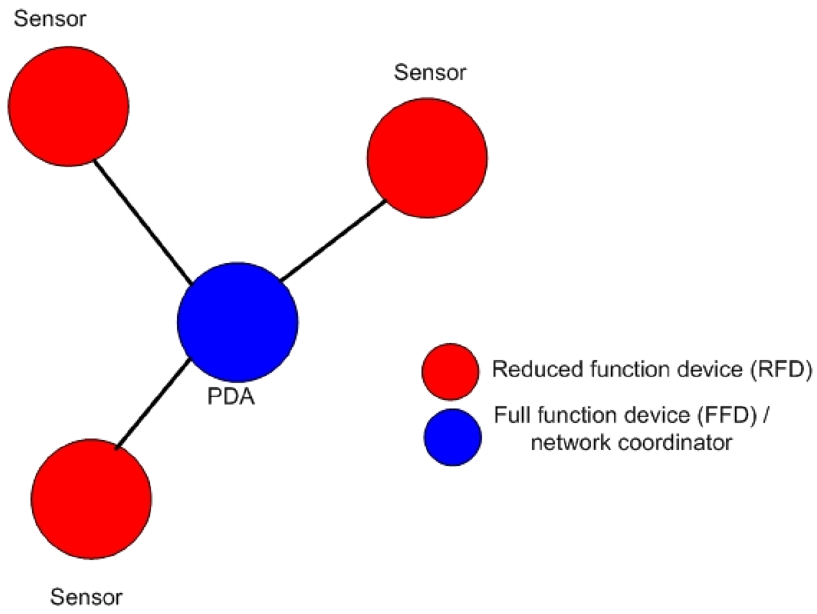

Sensor
Sensor
PDA
Sensor
Reduced function device (RFD)
Full function device (FFD) / network coordinator

Figure 25: ZigBee star topology

The sensor has a built in ZigBee transmitter with a range of up to 10 meters. The ZigBee standard comes with support for the security chosen for this transmission, AES. Even though the data rate is limited to a maximum theoretical bandwidth of 250kbit/s, this is sufficient for our use. The sensor will transmit the measured data continuously.

7.2.2 Setup

Figure 26 shows the initial setup process of the sensor. The sensor has a button which synchronizes communication with the PDA. When a patient is at the attending physician (AP) for attaching the sensor, the AP will press the button on the sensor to initiate the setup sequence with the PDA. The PDA is the coordinator device and acts as a trust centre that is responsible for accepting new devices into the network and distributes keys. Every sensor will have a sensor ID which is a unique identification for that particular sensor, like a MAC address. This ID is used when setting up the sensor and the PDA and exchanging the link key. When the synchronization button is pressed the sensor will transmits its sensor ID to the PDA and ask the PDA to start the setup process. The PDA will display a message with the sensor ID asking the AP if the sensor can be accepted. If the AP confirms, the PDA and sensor will negotiate a link key using a symmetrical key-key exchange (SKKE) handshake. This link key is usually used for the duration of the sensors lifetime, but can be refreshed if needed. The link key will authenticate the sensor to the PDA and the PDA will only process data received from sensors that have had this manual setup process. Messages from other ZigBee devices will not be accepted. The initial setup phase can be vulnerable to attacks unless it is done in a secure environment like the doctors office.

A single PDA can be used to process data from several different sensors attached to the same patient. The link key is unique to the PDA-sensor pair and is used to identify and authenticate the device in the network, guaranteeing that the PDA will only accept data sent from authenticated sensors.

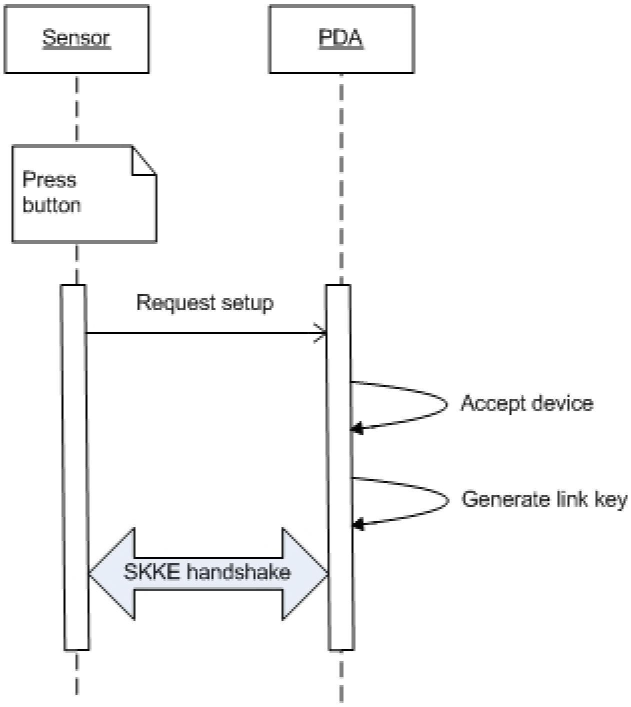


Figure 26: Sensor setup process

7.2.3 Security

Message freshness is ensured by the freshness counter maintained by ZigBee devices for both incoming and outgoing messages. These counters are reset if link keys are updated. To ensure message integrity and protect the messages from eavesdropping we propose the use of the AES cryptographic algorithm with 128 bits key length. The example ZigBee chip mentioned in chapter 4 is built to support this encryption in a very effective way, and this enables us to have high security on even this low energy unit. A key size of 128 bits will be highly secure for several years to come. The sensors get a device level authentication (chapter 4.1.2.4) by the link key used for the transmissions. This prevents inside and outside attacks. The use of strong encryption of the packets, and not using any private information about the patient in the packets ensure that the privacy of the patient is protected.

7.3 ELECTRONIC MESSAGING

7.3.1 National Health Network

The core in our scenario is the administrative centre of the National Health Network. The NHN will bed a centre where the CA, RBAC, the ebXML registry, VPN server, and the Core Journal are located. The core journal is a central database that contains a complete medical record for all patients. This core journal will be updated with information located in local EHR databases. The benefit of a core journal is the possibility of a single patient journal containing all medical information about each patient.

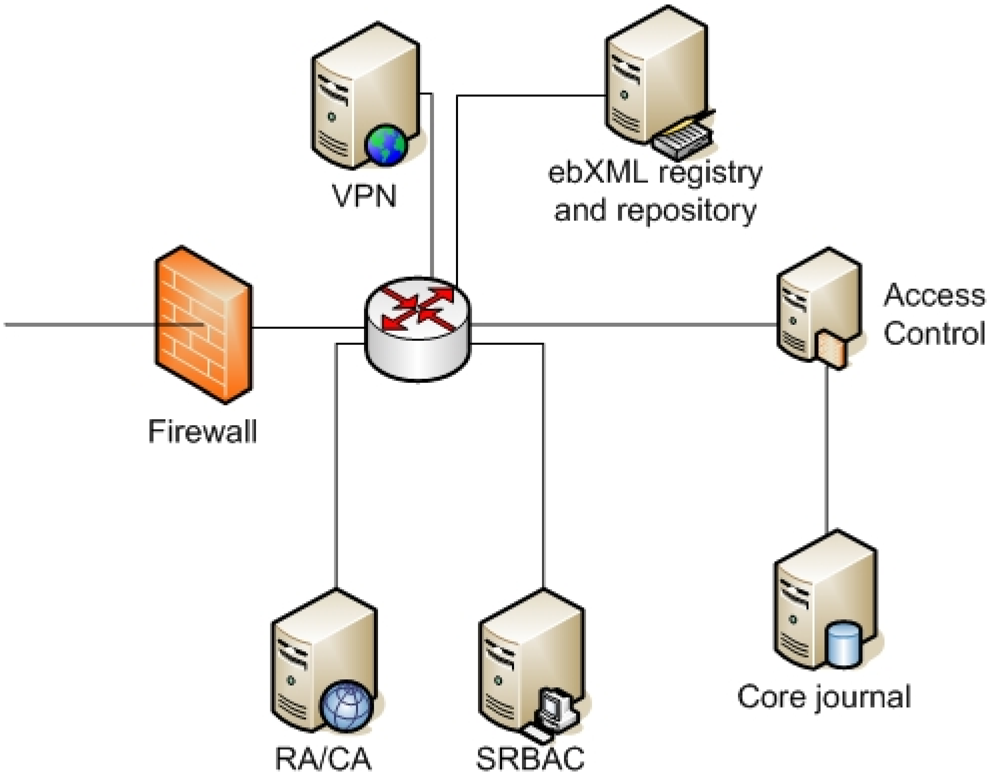


Figure 27: Overview of the core parts of National Health Network

The CA server distributes the certificates to users. We suggest having the CA server as part of the NHN, but this server can also be administered by a trusted third party that supplies the NHN with all digital certificates needed. All computers will have a digital certificate that identifies them to a specific location, and all users get a smartcard with a personal digital certificate, which will be used as personal identification. Not all actions require a personal certificate, but some actions will. For example when a RGP grants a specialist access to a patient journal the RGP will need to use his smartcard to verify his identity, as well as the specialist.

Administration of users and their roles will be done by the RBAC server. The RBAC server contains all the roles available and which permissions the different roles have. All users connected to the national health network will be given one or more roles, and there has to be routines to update roles when needed and to remove them when a user no longer should have them. Local access control units will do the permission checks when users attempt to access local services. Each access control unit will contain the access matrices regarding all information stored in the respective domains/locations. These access control units will be updated by the RBAC server when changes are made to roles that are used on the access control units.

The ebXML registry and repository is a database administering document type definitions (DTD) for the various message types used in the network. The server provides services for adding and updating DTDs, and services for accessing this information for outside parties who want to exchange messages conforming to the ebXML messages used in the network.

Access to servers in the NHN requires a secure connection. We suggest the use of a virtual private network, VPN. Technologies like IPsec, SSL and PPTP can be used to encrypt this secure network. We propose the use of a central VPN server, where the users automatically establish a secure connection when they log on the network, identifying themselves using a smart card containing a digital certificate and a password or pin code. Using both a smart card and a pin code/password will provide a very strong authentication. The ebXML standard uses secure messages, but can be sent over the secure network because the standard is independent of the connection technologies. All medical personnel will use VPN when accessing remote resources, including community nurses that are using GPRS to communicate with the EHR.

The recorded information from the sensor will be stored at a local EHR, often located at a regular general practitioners office or in a hospital. An access control unit will administer access to the database based on user roles and locations. The different users in the office, like secretary, nurse and RGP will have different permissions to the EHR. The information in the local database will regularly be synchronized with the core journal. The core journal will log all high level access and changes to the medical journal, i.e. operations where the personal smartcard is needed.

7.3.2 ebXML

We propose the use of the ebXML message standard on the messages used to transport information. The ebXML message standard is independent of underlying transport protocols, and provides a message structure than can be adapted to all our needs. Each device in the network needs an ebXML client application to do packaging and preparation of the ebXML messages. The content of the ebXML message envelopes is encrypted using a 128 bit AES encryption. The message envelopes can contain any form of binary data. The ebXML standard defines reliable delivery of messages with rules for persistence, retries, error messages, and acknowledgements. The message will have a sequence number to avoid that re-sent messages can be accepted when they already have been accepted if a “received” message failed.

7.3.3 Long range wireless communication

We suggest the use of the GPRS standard as transportation protocol for the long range wireless transmission connecting the PDA to the Internet. Since the PDA only transmits periodically the GPRS bandwidth is sufficient for the message transportation we require. The PDA will analyze the data, package an excerpt of the data in an ebXML envelope, and use a normal GPRS compact flash card to transmit it to the EHR.

The setup process of the PDA in the AP’s office includes several elements; digital certificate for the PDA, adding a sensor, patient ID stored on the

PDA, and a unique ID generated by the EHR to identify the messages sent from the PDA. When the PDA is initially set up the AP will store the name, address and phone number of the patient, so this information can be included in an emergency message if needed. A digital certificate will be loaded into the PDA while it is in its cradle connected to the AP's computer. This certificate is used to sign the ebXML messages to authenticate them to the EHR so it will accept the message. The digital certificate is also used to negotiate a session key to use for the AES encryption of the message content. The session key will be regularly updated. The AP will go through the sensor setup process described in chapter 7.2.2 for each sensor he attaches to the patient.

The PDA will receive a unique temporary ID from the local EHR used to identify the patient. This ID is generated by the EHR and will be used when the PDA sends messages to the EHR. We use this ID to protect the patient's identity during the wireless transfer of the sensor recordings. The PDA will analyze the received recordings from the sensor and package an excerpt in an ebXML envelope and transmit it to the EHR. The message containing the excerpt will be digitally signed using the digital certificate, and will also contain the temp ID, and the PDA ID, which may be the MAC address. The ID will be linked to the correct patient and the sensor ID number. The EHR will add the received excerpts to the correct patient's journal.

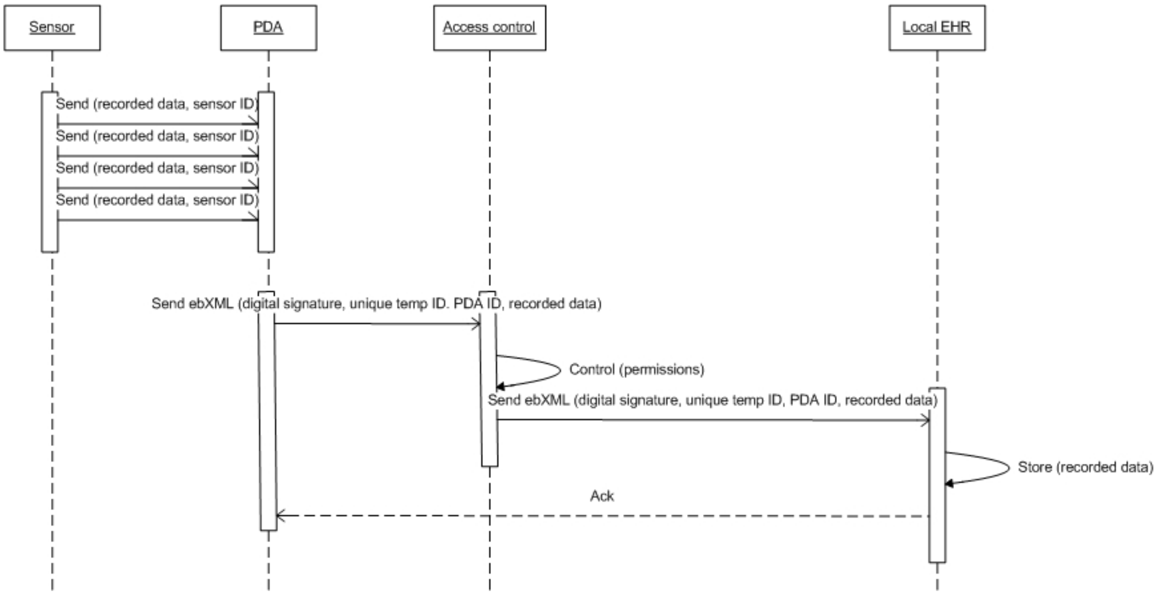

Sensor
PDA
Access control
Local EHR
Send (recorded data, sensor ID)
Send (recorded data, sensor ID)
Send (recorded data, sensor ID)
Send (recorded data, sensor ID)
Send ebXML (digital signature, unique temp ID. PDA ID, recorded data)
Control (permissions)
Send ebXML (digital signature, unique temp ID, PDA ID, recorded data)
Store (recorded data)
Ack

Figure 28: Sequence diagram sensor – EHR

If for some reasons the GPRS can not contact the EHR, the data will be stored on a flash card in the PDA, and sent at first opportunity. If the flash card is 1GB, and the sensor sends data at 50 KB/s, the PDA can store over 5.5 hours of continuously data. Only excerpts of the data will be stored, enabling the device to store data for a long time if needed. An overview of the transmission is shown on figure 29.

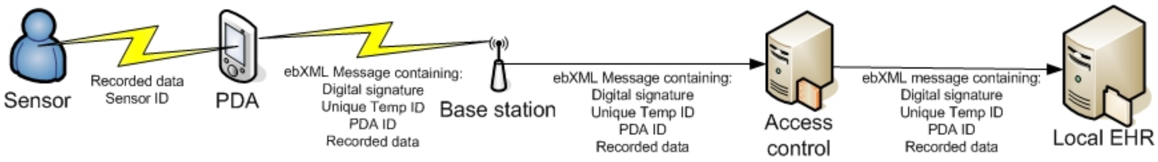


Figure 29: Overview of the transmission from the sensor to the EHR

7.3.4 Security

A secure network is dependant on secure key handling and correct identification and authorization of users. We propose the use of a PKI framework with digital certificates to maintain and distribute secure keys to all users connected to the health network. The PKI framework will distribute digital certificates to all computers, and all personnel will have smart cards with a personal digital certificate. These digital certificates can be obtained, updated and revoked by a central certificate authority. We suggest that the CA should be located in the national health network, but these services can also be supplied by a trusted third party. We suggest using the international X.509 digital certificate standard, but other digital certificates can also be used, as long as they meet the requirements of the particular system in which it is to be implemented.

There are two different digital certificates in this system; one is a personal certificate stored on a smartcard for the specific user, and the other will be a certificate stored on each computer. The personal certificate on the smartcard will contain the user's identity. The smartcard will be used to authenticate the user in the network. Certificates for computers will contain information about the ID, location and administrative domain of the computer. All digital certificates will in addition contain to the public key, validity period and the digital signature of the issuer. To give some protection against theft of these personal smartcards, we suggest that the user is asked for a PIN-code or password when activating the smartcard.

All messages are encrypted using 128 bit AES encryption. 128 bit session keys will be negotiated with the use of the public key included in the digital certificates. These session keys are unique to the two participants and will be used to encrypt the content of ebXML messages transmitted between them. New session keys will be negotiated for every new session. The encrypted messages are protected from eaves dropping and the unique link key ensures that the message can only be read by the intended receiver. All messages will be signed using the digital certificates to ensure non-repudiation. The use of personal information in messages should be limited, but the strong security will protect the content.

7.4 PRIVACY PROTECTION USING SRBAC

7.4.1 SRBAC elements

We propose a solution based on RBAC with location control. All users will be given access to information and resources based on their role and location. We will define users, roles, locations, operations, objects and permissions and propose as examples a limited number of roles, locations, operations, and objects to make the description simpler and more understandable. Users can have one or more roles, and will also have a location that combined with their role will give them access to the correct information in the correct patient journals.

Figure 30 shows how the SRBAC model [84] can be adapted to our scenario. We have suggested some values for each element. The users are the persons that are accessing the network. Roles are the job description for the different users. Loc describes the different locations of the users. Operations are the different functions a user is allowed to do. Objects consist of different patient information. The permission element consists of possible combinations of operations and objects.

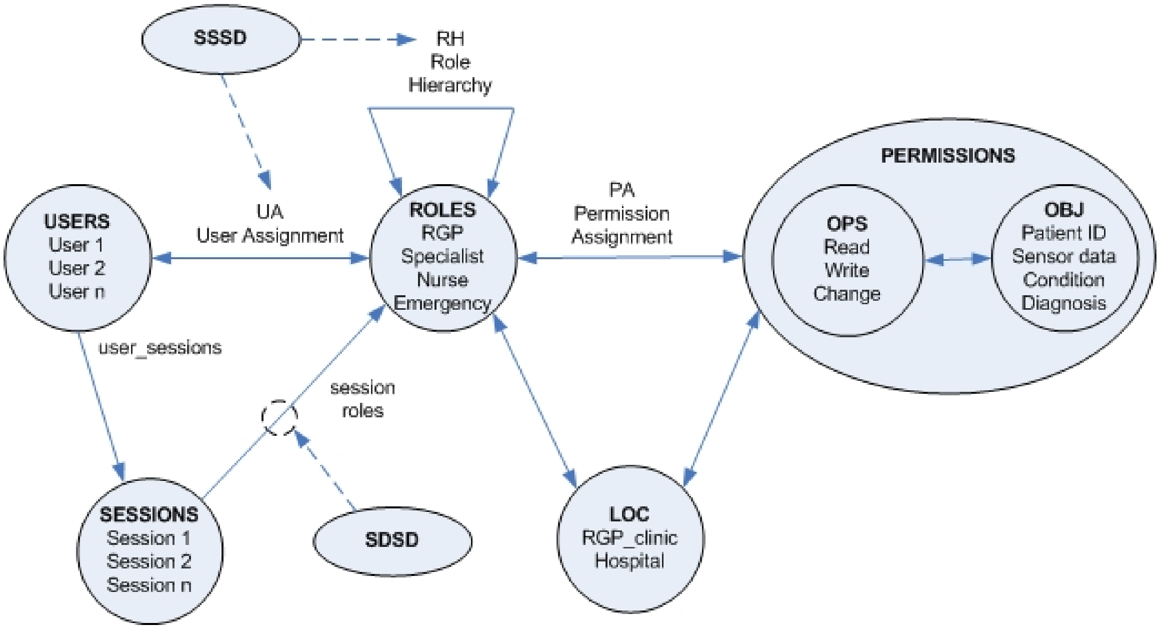


Figure 30: SRBAC model adapted to our solution

7.4.1.1 Users

We have several different users in the scenario described in chapter 2. The users are medical staffs in hospitals and medical offices that are to be accessing the Network. They can be regular general practitioners, emergency centre personnel, doctors, specialists, and nurses.

7.4.1.2 Roles

We have defined a few example roles to help describe the solution we propose. In a real implementation there will be more roles. Some users may hold more than one role at a time, and some roles are mutually exclusive. For example a doctor can be both an attending physician and a regular general practitioner at the same time, but he cannot be attending physician and patient at the same time. For simplicity sake we have given every specialist the role "Specialist", but it should be divided into a more specific job description, i.e. the field that the specialist has as its specialty, e.g. cardiology specialist. Table 3 shows a listing of the roles we propose.

Table 3: Roles

Role	**Description**
Regular General Practitioner	The regular general practitioner role is held by regular practitioner who is appointed as a patient's regular doctor. He has full rights to the patient's medical journal, and can grant access rights to personnel who need it to perform medical treatment.
Attending Physician	An attending physician role is held by the doctor who has main responsibility for the current medical treatment of the patient. The regular general practitioner can also have the role attending physician to the same patients that he is RGP for and other for patients who for various reasons is under his medical treatment.
Specialist	The specialist is a physician with more expertise in its field than most general practitioners, and will sometimes be asked for a second opinion based on the measured readings from the sensor due to his knowledge. He will not need to know the patients personal information, only the data collected and other medical information needed to make a diagnoses. That means the specialist will have a lower clearance level than the RGP.
Nurse	Nurses will only need access to basic information like e.g.

	allergies, what medication they use and what special care they need, and will only have medium level of clearance. Community nurse will hold the nurse role, but she will be located to an external location.
Emergency Centre Personnel	Emergency centre personnel are the people working in the emergency centre. They have no access rights to medical journals, but can grant access to personnel that need it to perform medical treatment, like ambulance personnel and emergency room staff.
PDA	The PDA role is exclusively for PDA. When the sensor and PDA are set up at the attending physician, the PDA is linked with a particular patient. When the PDA is sending recorded data, it has the permission to write the data in the EHR.

7.4.1.3 Locations

While the previous sections are examples that can be implemented into a RBAC model, this section uses the Location element from the SRBAC model. A location LOC is a normalized set of locations L = {l_1,l_2,…,l_k} that is a partition of the entire domain area Z. In our scenario the domain Z can either be a RGP clinic or a hospital, L1-L7 is the partitions of a domain, and l_1-l_8 are a selection of locations.

We have chosen a limited number of locations. Locations can be small or large, ranging from a medical district down to a single workstation. Table 4 shows the domains Z, table 5 the selected partitions, and table 6 shows the selected locations.

Table 4: The domains

DOMAINS Z	**Description**
Z_{RGP}	The RGP clinic
$Z_{Hospital}$	The hospital

Table 5: The partitions

Partitions	**Description**
L1	RGP_office
L2	GP_office
L3	Medical_secretary
L4	Cardiology_department

L5	Other_specialists_department
L6	Medical_staff_department
L7	Emergency_centre

Table 6: The locations

Locations	**Description**
l_1	RGP_workstation
l_2	GP_workstation
l_3	Medical_secretary
l_4	Nurse_workstation
l_5	Cardiologist
l_6	Other_specialists_workstation
l_7	Public_health_nurse_workstation
l_8	Emergency_room
l_9	General_medical_staff_room

We propose an example on how a domain can be built regarding the partitions and locations based on tables 4-6.

Z_{RPG} = L1+L2+L3

L1 = $\{l_1\}$

L2 = $\{l_2\}$

L3 = $\{l_3, l_4\}$

$Z_{Hospital}$ = L2+L3+L4+L5+L6

L2 = $\{l_2\}$

L3 = $\{l_3, l_4\}$

L4 = $\{l_3, l_4, l_5\}$

L5 = $\{l_3, l_4, l_6\}$

L6 = $\{l_2, l_3, l_4, l_{7,} l_9\}$

L7 = $\{l_2, l_3, l_8\}$

7.4.1.4 Operations

The operations are the different commands a user can perform on an object. The different operations we propose are *read*, *write* and *change*. The read operation allows the user to look at the information on the EHR. The write operation allows the user to write and create new information on the EHR. The change operation allows the user to change the existing information.

7.4.1.5 Objects

We have given a few selected object examples with description in table 7. This is a small example and a real medical record contains several additional objects. We have selected a few to suit our scenario and show the intent behind the objects.

Table 7: Objects

Objects	**Description**
Patient identification	Patient Identification is values that uniquely identify a single patient, like name, address, and national identity number. This is sensitive information and access on this level is very limited.
Sensor data	Sensor Data are all recordings transmitted by the wireless sensor, and will only be accessible for appointed physicians.
Medical decisions	This is the decisions made by different medical staffs
Diagnoses	This is the diagnoses made by different medical staffs
Special diagnoses	Special Diagnosis is given highest level, and is used to keep extra sensitive medical information, for example a HIV diagnosis.
Patient number	The patient number is a global identification of the patient, created randomly by the EHR. It is not related to national security number or any other personal information.

7.4.1.6 Permissions and roles

The permission element is a combination of operations and object. An example of a permission can be *read access on the sensor data*. Another example can be *write access on diagnoses*. Every role will have a number of permissions based on its location. An example on permissions of the RGP role will be write access on all the objects mentioned in table 7, if the patient is located at the EHR at the RPG clinic.

Based on the personal data act the patient can decide whom he wants to grant privileges to information in his medical journal. If medical personnel need access to a patient's medical journal, the permissions will be given by the RGP or attending physician with the consent from the patient. In case of emergency, the emergency centre staff can grant special permissions to emergency personnel, based on the assumption that the patient would consent. A detailed example is given in chapter 7.5.2.

7.4.2 Separation of duty

To maintain privacy, the accessibility and limitations are a very important element. The locations are linked with roles to make a location/role pair that is used to grant doctors and nurses access to patients in their location and restrict them from accessing patient files belonging to patients residing in other locations.

As an example, a particular user can have both the roles *specialist* (SP) and *AP* (attending physician). When he's on a hospital, he may have access from the locations l_2, l_6, and l_9, i.e. the GP_workstation, specialist_workstation and general_medical_staff_room respectively. As mentioned in chapter 6.7, SRBAC uses two elements called SSSD (Spatial Static Separation of Duty) and SDSD (Spatial Dynamic Separation of Duty) as shown in figure 30. In this case the SSSD will enforce constraint on the location l_6, because it is exclusively for the specialist role (marked by the ellipse), and the AP role is not allowed to access the EHR from that location. To solve this, the user starts a new session with the role *specialist* only. The SDSD will control which locations the specialist role are allowed to enter for each session.

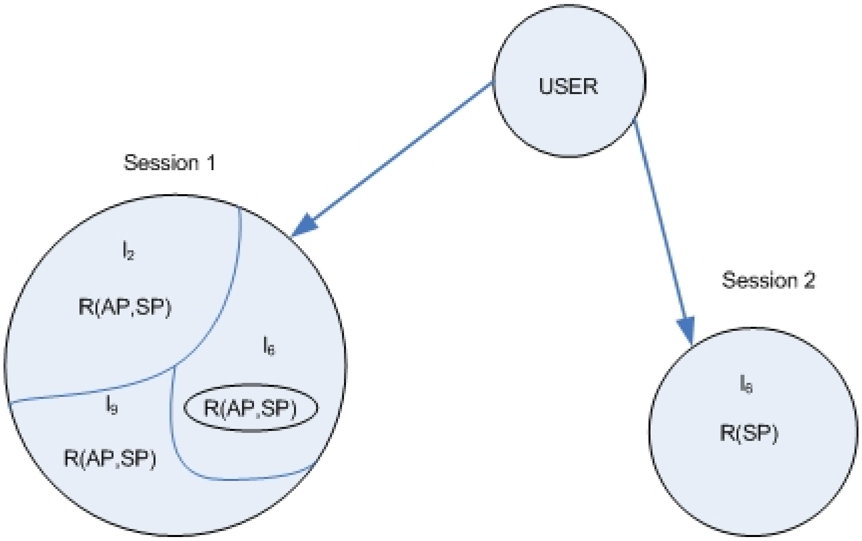


Figure 31: The SSSD and SDSD relations

It is also possible to perform a separation of duty such that a user may never have both the role *attending_physician* (AP) and *patient* (P). That way it is impossible for a physician to write his own receipts.

7.5 SITUATIONAL EVENTS

7.5.1 AP contacts specialist

If the AP need help to interpret the recorded results, he may want to contact a specialist. The AP will have to grant the specialist permissions to the selected patient's medical journal. This is done manually for each patient. Figure 32 shows an overview of the parts involved.

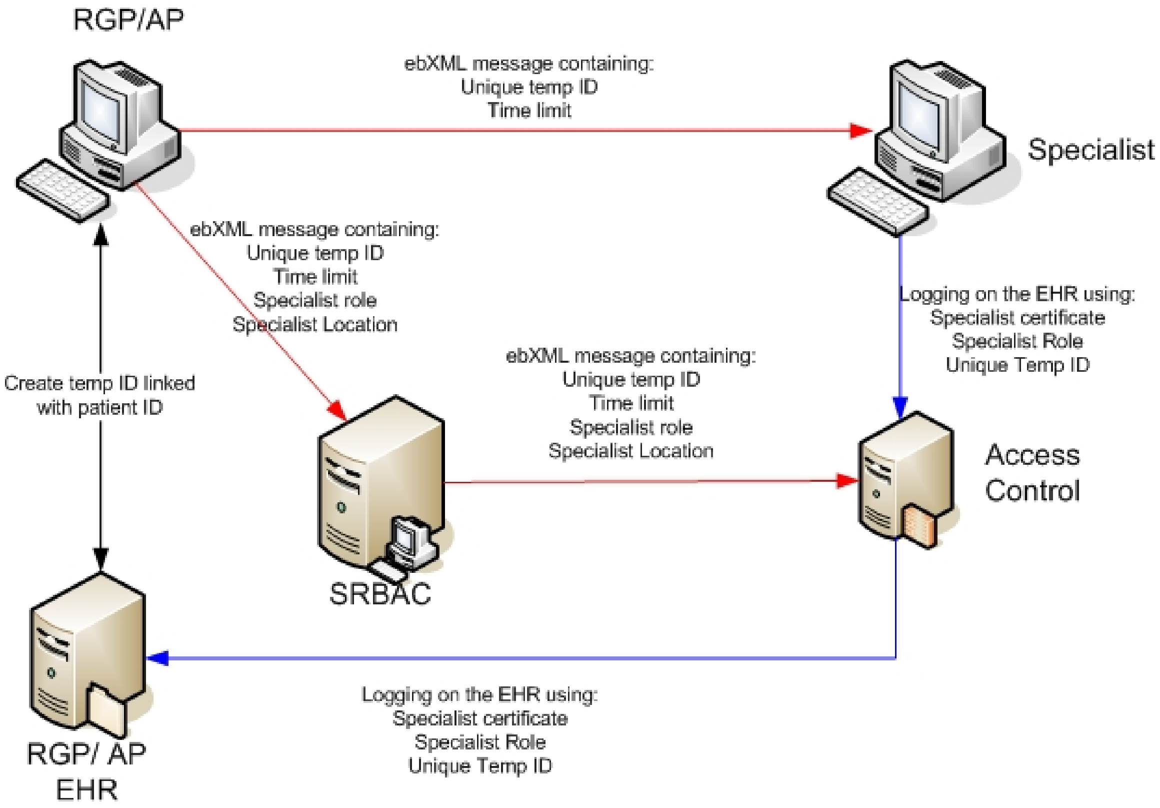


Figure 32: A graphical overview when an AP contacts a specialist

The specialist will be assigned permissions based on two factors; his role as specialist and his location. When the AP grants the specialist access, the location of the specialist will be added to the list of locations allowed to access the patient's journal. The specialist role will only get a temporary access right to a limited number of objects on the specific patient. The temporary access rights are limited to only include permissions to medical information; the specialist will never have permission to access private information about the patient, like name, address, national identity number or birthday. To prevent the specialist of accumulating access to an increasing number of patients, the access rights given to the specialist are temporary with a predefined time to live. We propose a lifetime of 168 hours, or 1 week, for the temporary access rights, as this should grant the specialist sufficient time to review the patients journal. The access rights will be automatically revoked when they expire.

For privacy reasons the EHR generates a unique temporary identifier the selected specialist can use to access the selected patient journal without him knowing any personal information about the patient. The identifier will be used as a pointer to the correct patient journal when the specialist wants to access it. With the use of a unique identifier we can grant the specialist access to a patient without giving him access to personal information and this maintain the patient's privacy.

Figure 33 shows a sequence diagram describing the process when an AP asks for a second opinion from a specialist, and thus granting him temporary permissions. The AP asks the EHR to generate a unique identifier linked with the patient ID. EHR generates this ID and returns the temporary unique ID to the AP. This temporary ID can have a permanent lifetime of 1 week, and if the specialist need more time to look at the patient data, the AP will have to do this process once more. The AP will then update the SRBAC server with a temporary permission for the specialist. The update message contains the unique temp ID, a time limit set by the AP, the specialist role, and the specialist location. The SRBAC server will then update the access control unit with the same information. The AP will also send the unique temp ID and the time limit to the specialist. When the specialist are logging in to the AP's local EHR, he will have to identify himself with his computers certificate, his personal smartcard and the unique temp ID he got from the AP. If the specialist's identifier is valid and matches a patient journal in the EHR, he will be granted access to the patient journal for the time period decided by the AP.

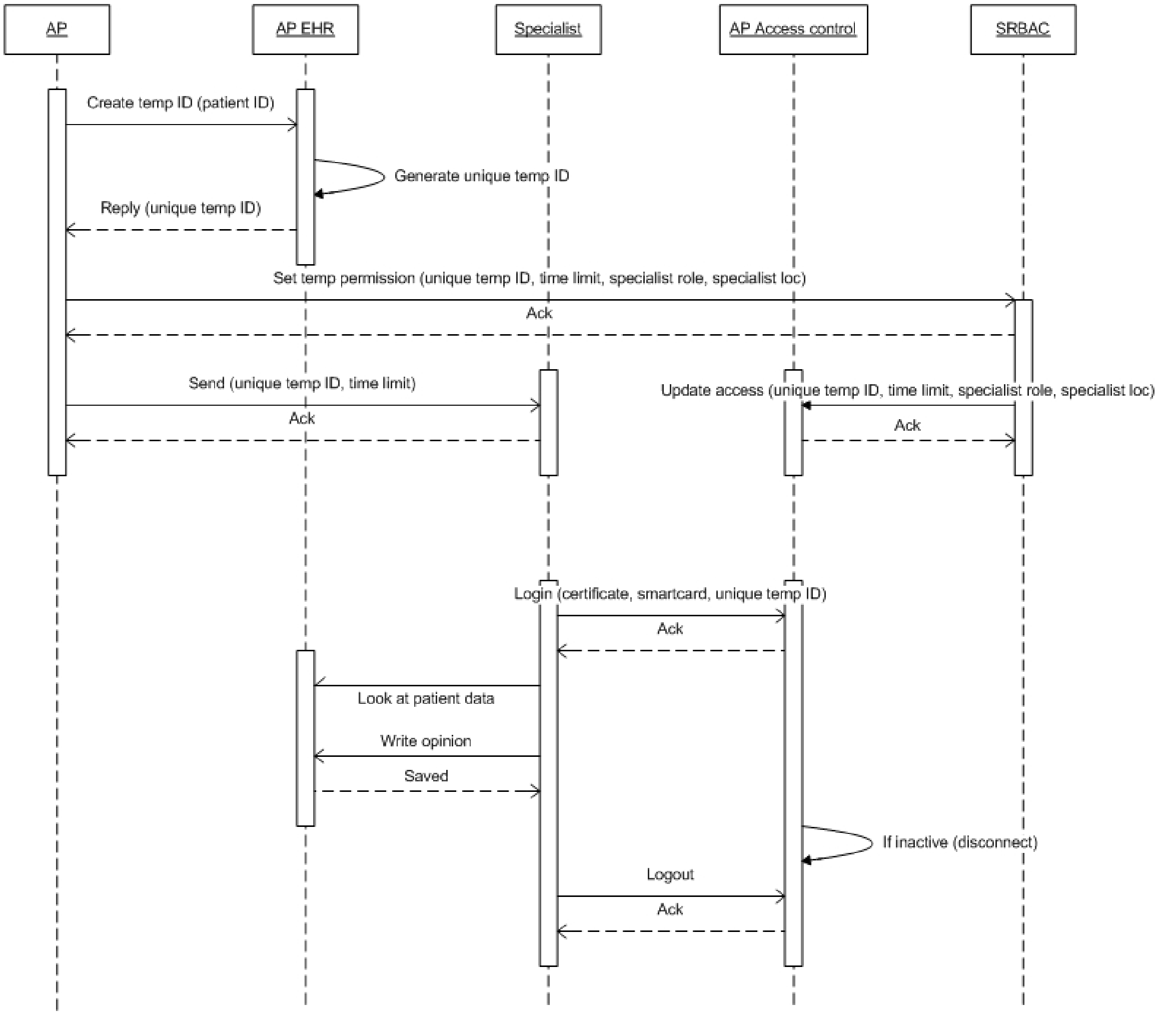

AP
AP EHR
Specialist
AP Access control
SRBAC
Create temp ID (patient ID)
Generate unique temp ID
Reply (unique temp ID)
Set temp permission (unique temp ID, time limit, specialist role, specialist loc)
Ack
Send (unique temp ID, time limit)
Update access (unique temp ID, time limit, specialist role, specialist loc)
Ack
Ack
Login (certificate, smartcard, unique temp ID)
Ack
Look at patient data
Write opinion
Saved
If inactive (disconnect)
Logout
Ack

Figure 33: Sequence diagram showing an AP contacting a specialist.

7.5.2 Emergency message

The RBAC system we propose can handle emergency messages. Whenever an emergency event is detected by the PDA, it will send an emergency message to the emergency centre with the name, address and phone number of the patient. The patient's private information will be stored on the PDA, and typed in by the AP. This information will be used exclusively for emergency messages. When the emergency centre receive the emergency message, they will try to contact the patient, or send an ambulance if the patient doesn't answer. Unless the emergency message is confirmed to be false, it will grant the emergency centre personnel access rights to the patient’s journal. This will give the emergency centre permission to grant temporary permissions to other medical personnel that needs it. Examples of such personnel can be ambulance or emergency room doctors and nurses.

8 DISCUSSION

8.1 LAWS AND LEGISLATIONS

The laws and legislations presented in chapter 3 impose a few restrictions on our solution. The Norwegian Data Inspectorate has announced that transport of personal information outside of the attending physicians control must be encrypted using DES 128 (3DES) equivalent or better. We propose the use of the stronger AES algorithm. The AES encryption is both more secure and more effective than the older 3DES, and is more suited to be used in a mobile wireless medical environment.

Based on the Personal Health Data Filing System Act the Norwegian Data Inspectorate has concluded that access to medical information can only be granted to personnel within a hierarchical organization context. In our solution we give access to a specialist outside the hierarchical organization context of the AP. Based on The Personal Data Act the patient can decide how he wants to be protected and to whom he wants to grant privileges to information in his medical journal. This can be used to argue that the AP can grant access to personnel outside the hierarchical organization context if medical treatment is dependant on it and the patient consents. In case of an emergency, the emergency personnel may grant themselves necessary permissions. We assume that in an emergency the patient would consent to giving the medical personnel these permissions, because in this situation the need for emergency treatment is more important than the patient’s privacy.

8.2 SECURITY AND PRIVACY IN THE SHORT RANGE WIRELESS COMMUNICATION

We propose the use of AES encryption between the sensor and the PDA. This encryption is proved to be very strong and will remain secure for several years to come. AES is also both more effective and more secure than the 3DES encryption required by the Norwegian Data Inspectorate. The sensor has very limited processing capacity and the use of hashing functions to sign messages could have solved the integrity and authentication issues. Hashing functions does not provide the security required by the Norwegian Data Inspectorate. The requirements from the Data Inspectorate can be argued not to be applied on this short range transmission, but as long as better solutions like AES are available and practical we disregarded the use of hashing functions.

A privacy issue is that the patient can be tracked using the ID of the sensor. The patient is using the sensor everywhere he goes; if eavesdroppers can find the sensor ID they can use this to track the movements of the patient. Both the recorded information and the sensor ID are encrypted and thus protected from eavesdropping. This ensures that the patient cannot be identified based on the ID of the sensor and prevents attacks where an attacker wants to track the movements of the patient.

AES encryption can be implemented on all of the 3 most relevant transmission technologies; ZigBee, Bluetooth and RF-radio. We suggest using ZigBee because the ZigBee standard comes with native support for AES on the network layer, and that it is possible to get ZigBee chips with AES coprocessors to make the encrypting more effective. ZigBee is designed to be low cost and power efficient. Bluetooth and RF-radio needs to do the AES encryption in the application layer and this requires more processing power on the sensor, which leads to a higher energy consumption. AES encryption using 128 bit key length is very secure and solves several security issues like integrity and confidentiality. Using a link key we can authenticate the sensor to the PDA and guarantee that accepted transmissions are form manually accepted sensors.

8.3 MESSAGE SECURITY

8.3.1 Mobile telecommunication

An important factor when developing our solution was to keep it independent of transport protocols. Different countries will have better coverage for different technologies, and it is important to select the technology that gives the best result for the end user. In our solution we suggest using GPRS. GPRS offer the necessary properties for security, data rate, availability, and has high coverage. GSM has way too low data rate and is not suitable for our scenario. Other technologies like EDGE and UMTS can also be used. These new technologies do not function as intended due to low coverage and variable data rate. It took 10 years for GPRS to become the leading mobile communication standard, and it is assumed it will take just as long for these new technologies [31]. However, when they have the coverage to allow the patient to move freely as he likes and does not limit him to certain areas, these technologies may be used without hesitation because of the transport layer independent design of the ebXML messages.

8.3.2 Message handling

We propose the ebXML standard as common message standard for our solution. The international ebXML standard can be adapted to any kind of content and security level. It is also independent of lower layer transport protocols. This makes it very well suited to be used in an environment where a combination of wireless and wired communication is used. The ebXML message standard can also use encryption methods selected by the users, in our case AES. The standard has a built-in system for reliable delivery of messages, with rules for persistence, retries, error handling and acknowledgments. This makes the standard suited for use in a medical environment where reliability and security is very important.

8.3.3 Encryption

The most important issues when choosing an encryption standard for the transmission are provable security strength, processing speed, and versatility. The Norwegian Data Inspectorate requires the use of 3DES or better. The 3DES encryption has not yet been successfully attacked, but AES encryption is stronger due to better design and also the possibility for longer key lengths. AES will be secure for many years to come and is around 6 times faster than 3DES in software implementations, making it a better choice. AES can be implemented in many ways, including encrypting the content of our electronic messages. AES is an international standard, and if any successful attacks should be developed it will be known and necessary countermeasure can be implemented.

8.3.4 Signatures and keys

We propose the use of digital certificates to prove identity, sign electronic messages and distribute encryption keys. Digital certificates can be used to sign messages and ensure non-repudiation. When a medical journal is updated it is very important that the update is correct and that changes can be tracked. The best way to authenticate users is to combine smart cards containing a personal digital certificate with the use of a pin code or password. The public key in the digital certificates is also used for a secure negotiation of symmetric session keys used for the encryption of messages. This provides a simpler and more secure way of distributing such keys than having to use a trusted third party as intermediary.

8.4 PRIVACY PROTECTION

The RBAC model is a thoroughly examined, very well-known model to maintain privacy, and suits very well for scenarios with clear job descriptions like a medical environment. Users are not assigned permissions directly, but acquire them through their role. To keep the privacy and integrity, RBAC use a concept called Least Privilege. This means that a user is not given more rights than necessary to perform a job. It also utilize a role hierarchy, so a role r_i inherits all permissions from role r_j if all permissions of r_j are permissions of r_i.

There are several different propositions on a RBAC model with location control. Two such propositions are SRBAC and DIMEDAC. We have adapted SRBAC to our scenario, but it is possible to use DIMEDAC, though some modifications are needed. The RBAC model itself is very well tested and gives a high degree of privacy when implemented and used correctly. With a location control it can perform more specific tasks and still maintains the privacy.

The main advantage of using the SRBAC model in our scenario is the possibilities to let the users (i.e. medical staff) have several roles with different permissions based on their location. This way it is possible to set the necessary constraints on the users, so they have as little permissions as possible to do their job. In addition to their roles, when performing crucial operations on the patient journal (EHR) the users have to use a personal smartcard to get access. Whenever someone accesses the EHR, the session is logged.

As it is in the Norwegian Health Network today, information about a patient is spread over several databases and getting access to needed information can be hard. Our proposal is a local EHR in each medical office, be it a RPG clinic or a hospital. To maintain privacy only medical personnel involved in the medical care are allowed to access the medical journal. The exception is when an AP is asking for a second opinion from other medical personnel at other locations. In addition to these local EHR's, we propose a core journal located at the NHN. This core journal contains all the information about a patient, and is constantly updated by the local EHR's when they have made changes on a patient record.

The main threat to privacy is the access on patient data from unauthorized users within an organization, in our case the medical staff. Many medical employees are browsing the patient journal to other co-workers or even famous people [85]. This is illegal, and to prevent this, we propose the SRBAC model using a location control in addition to the concept *least privilege.* If today's network had the location control, the mentioned example would never have happened. We feel confident to have a solution that maintains the privacy of the sensitive patient data.

9 CONCLUSIONS AND FURTHER WORK

9.1 CONCLUSIONS

In this thesis we have proposed a suggestion on how existing technologies can be used to maintain privacy protection in a mobile health care environment. The issue of privacy protection in this type of scenario is very little addressed in literature, and we hope our work can contribute to this. In order to protect the privacy we have to ensure the security.

In every part of our scenario we are using 128-bit AES encryption. This is a better algorithm that delivers much higher security than the minimum requirement from the Norwegian Data Inspectorate, 128-bit 3DES. The use of AES guarantees a high security for message transfers throughout the network. The use of encryption ensures the integrity and confidentiality.

We suggest a key management scheme using PKI with digital certificates. A central PKI distributes certificates used to guarantee secure identification and authentication of the users. The digital certificates are also used to negotiate symmetric keys to be used for the AES encryption, and to digitally sign messages to ensure non-repudiation.

ebXML is a international standard for electronic message exchange. The use of one common standard simplifies the communication between the participants. The advantages for selecting ebXML are good adaptability, independence of underlying transport protocols, and it is possible to select the wanted security protocols.

We propose the use of RBAC with location control to maintain privacy. RBAC is well suited to administrate access control in a medical environment. The added location control makes it possible to restrict access to groups of users sharing the same role. This can be used to protect the patient’s private information from users who are not directly involved in the medical care of the patient.

We have shown that using the security and privacy technologies mentioned above it is possible to protect privacy in a mobile biomedical information collection service.

9.2 FURTHER WORK

This report only presents guidelines for privacy protection in a mobile biomedical information collection service. In order to make a complete working implementation of these guidelines several tasks has to be completed. A more detailed description of users, roles, locations and messages must be formulated.

The users and roles described in our solution are only some examples. A wireless mobile biomedical information collection service has several users not included in our scenario. Roles and users must be defined based on the needs of the health care system. Roles for all users connected to the national health network must be created and the permissions these roles are given must be defined. The health network consists of several domains, all of who have many partitions. These must be defined and users must be assigned to their correct location.

We have only given a brief description of a few of the ebXML messages to be used. ebXML messages have to be defined according to all of the messages used in the system today, and new messages that are needed but not used today must be defined. These message structure definitions must be made available to all service providers connected to the health network.

10 REFERENCES

[1] Malan, D. et al (2004) “CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care”

[2] Shnayder, V. et al. (2005) “Sensor Networks for Medical Care”

[3] Perrig, A. et al (2001) “SPINS: Security Protocols for Sensor Networks”

[4] Fensli, R., E. Gunnarson, and T. Gundersen (2005) "A Wearable ECG-recording System for Continuous Arrhythmia Monitoring in a Wireless Tele-Home-Care Situation," presented at The 18th IEEE International Symposium on Computer-Based Medical Systems, Dublin, Ireland

[5] Norsk Helsenett http://www.norsk-helsenett.no (online May 24, 2006)

[6] Widding, D. (May 2006) *Personal Communication*

[7] Fensli R, Gunnarson E. “Mobile Monitoring of Vital Parameters within the Electronic Health record - Medical, Technological and Legal aspects”. In: Tromsø Telemedicine and eHealth Conference - TTeC2004; 2004 21.-23. June 2004; Tromsø, Norway; 2004. p. 46

[8] Helse- og omsorgsdepartementet, “LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)”, http://www.lovdata.no/all/hl-20010518-024.html (current Jun. 10, 2005)

[9] Helse- og omsorgsdepartementet, ”LOV 1999-07-02 nr 63: Lov om pasientrettigheter (pasientrettighetsloven)”, http://www.lovdata.no/all/hl-19990702-063.html (current Dec. 21, 2005)

[10] Datatilsynet, “Act of 14 April 2000 No. 31 relating to the processing of personal data” http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf (current Apr. 14, 2000)

[11] Norwegian Data Inspectorate (2003) “Vedtak om pålegg til helse Bergen HF”

[12] Norwegian Data Inspectorate http://www.datatilsynet.no/ (online May 24, 2006)

[13] Bluetooth.com, the official Bluetooth Web site, http://www.bluetooth.com (online May 24, 2006)

[14] Bluetooth SIG (2004) “Specification of the Bluetooth System”

[15] Wikipedia.org “SAFER” http://en.wikipedia.org/wiki/SAFER (current Apr. 21, 2006)

[16] Wikipedia.org “E0 (cipher)” http://en.wikipedia.org/wiki/E0_%28cipher%29 (current Apr. 24, 2006)

[17] Shaked, Y. and A. Wool (2005) “Cracking the Bluetooth PIN”
http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html (current May 2, 2005)

[18] Lu Y., W. Meier, and S. Vaudenay (2005) “The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption" Crypto'05, Santa Barbara.

[19] CABA “Standards and protocols” http://www.caba.org/standard/zigbee.html (current Jan. 18, 2006)

[20] ZigBee Alliance “Our Mission” http://www.zigbee.org/en/about/ (online May 25, 2006)

[21] Freesoft.org “OSI Seven-Layer Model” http://www.freesoft.org/CIE/Topics/15.htm (online.May 26, 2006)

[22] ZigBee Alliance (2004) “ZigBee Specification v1.0”

[23] IEEE Computer Society (2003) “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)”

[24] Callaway, E. (2003) “Low Power Consumption Features of the IEEE 802.15.4/ZigBee LR-WPAN Standard”, Florida Communication Research Lab

[25] ZigBee Alliance (2005) “ZigBee Security specification overview”

[26] Øyen, G.E. (2006) “ZigBee and IEEE 802.15.4: A brief introduction”

[27] Kinney, P. (2003) “ZigBee Technology: Wireless Control that Simply Works”, Kinney Consulting LLC, Chair of IEEE 802.15.4 Task Group, Secretary of ZigBee BoD, Chair of ZigBee Building Automation Profile WG

[28] ChipCon “CC2510 Product Information” http://www.chipcon.com/index.cfm?kat_id=2&subkat_id=12&dok_id=258 (online May 24, 2006)

[29] C-GUYS http://www.c-guysusa.com/ (online May 24, 2006)

[30] GSA “GSM/3G Stats” http://www.gsacom.com/news/statistics.php4 (current May 15, 2006)

[31] Schiller, J. (2003) *Mobile Communications, second edition*, Addison-Wesley, pages 93-156

[32] Wikipedia.org “GSM” http://en.wikipedia.org/wiki/GSM

[33] Wikipedia.org “GPRS” http://en.wikipedia.org/wiki/GPRS (current May 24, 2006)

[34] Andersen P. B. og R. Johnsen “Mobiltelefon - Ikke bare prat” in (Ed.) Kunnskapsforlagets Årbok 2000 http://fag.grm.hia.no/ragnarj/mobile_syst/tradlos_komm.pdf

[35] European Telecommunications Standards Institute http://www.etsi.org/ (online May 25, 2006)

[36] Wikipedia.org “2.75G” http://en.wikipedia.org/wiki/2.75G (current Mar. 23, 2006)

[37] Wikipedia.org “EDGE” http://en.wikipedia.org/wiki/EDGE (current May 24, 2006)

[38] Meskauskas, P. ”Customised Applications for Mobile Enhanced Logic (CAMEL)”

[39] Telenor Dekningskart http://telenormobil.no/dekninginnland/index.do (online May 25, 2006)

http://www.telenor.no/bedrift/produkter/mobil/merom_umts_edge.html

[40] Wikipedia.org “UMTS” http://en.wikipedia.org/wiki/UMTS (current May 23, 2006)

[41] UMTS Forum “What is UMTS?” http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/What+is+UMTS_index (online May 25, 2006)

[42] Wikipedia.org “Cryptographic Hash Function” http://en.wikipedia.org/wiki/Cryptographic_hash_function (current Apr. 25, 2006)

[43] Mao, W. (2004) Modern Cryptography Theory & Practice, Bristol, Prentice Hall

[44] Rivest, R. (1992), MIT laboratory for Computer Science and RSA Data security, inc. April 1992.

[45] Answers.com “MD5” http://www.answers.com/topic/md5#after_ad1 (online May 25, 2006)

[46] Wikipedia.org “SHA Hash functions” http://en.wikipedia.org/wiki/SHA (current May 6, 2006)

[47] Schneier, B. (2005) “New Cryptanalytic Results Against SHA-1” http://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html (current Aug. 17, 2005)

[48] Wikipedia.org “Triple DES” http://en.wikipedia.org/wiki/3DES (current May 9, 2006)

[49] Bishop, M. (2003) *Computer Security Art and Science*, Addison-Wesley

[50] Wikipedia.org “Advanced Encryption Standard” http://en.wikipedia.org/wiki/Advanced_Encryption_Standard (current May 24, 2006)

[51] National Institute of Standards and Technology “Advanced Encryption Standard (AES) Questions and Answers” http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html (current Jan. 28, 2002)

[52] Federal Information Processing Standards Publications (2001) “Announcing the ADVANCED ENCRYPTION STANDARD (AES)” *Federal Information Processing Standards Publication 197*

[53] CNSS (2003) “CNSS Policy No. 15, Fact Sheet No. 1
National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information”

[54] Børthus, B and Tomas, E. (2005) ”Public Key Infrastructure for Windows Server 2003”

[55] National Institute of Standards and Technology (1995) “Secure Hash Standard” http://www.itl.nist.gov/fipspubs/fip180-1.htm (online May 25, 2006)

[56] Wikipedia.org “Public Key Infrastructure” (current May 26, 2006)

[57] Wikipedia.org “Smart Card” http://en.wikipedia.org/wiki/Smart_card (current May 24, 2006)

[58] Hong Kong University of Science & Technology (1998) "Guide to Smart Card Technology"

[59] Sosial- og helsedepartementet (2004) "S@mspill 2007- Elektronisk samarbeid i helse- og sosialsektoren"

[60] Kompetansesenter for IT i helse- og sosialsektoren AS "Najonale oppgaver" http://www.kith.no/templates/kith_WebPage____495.aspx (online May 25, 2006)

[61] Wikipedia.org "Electronic Data Interchange" http://en.wikipedia.org/wiki/Electronic_Data_Interchange (current May 22, 2006)

[62] UNECE "United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport" http://www.unece.org/trade/untdid/welcome.htm (current Feb. 15, 2006)

[63] Rosettanet http://www.rosettanet.org (online May 25, 2006)

[64] Kotok A. and D.R.R. Webber (2002) *ebXML: the new global standard for doing business over the internet*, Indianapolis, IND: New Riders Publishing

[65] OASIS ebXML Collaboration Protocol Profile and Agreement Technical Committee (2002) "Collaboration-Protocol Profile and Agreement Specification Version 2.0"

[66] OASIS ebXML Messaging Services Technical Committee (2002) "Message Service Specification Version 2.0"

[67] OASIS/ebXML Registry Technical Committee (2001) "OASIS/ebXML Registry Information Model v2.0"

[68] OASIS/ebXML Registry Technical Committee (2001) "OASIS/ebXML Registry Services Specification v2.0"

[69] UN/CEFACT (2003) "Core Components Technical Specification v2.01"

[70] OASIS (2004) "UK National Health Service NPfIT Uses ebXML Messaging"

[71] Kotok A. (2003) "Centers for Disease Control and Prevention, Public Health Information Network Messaging System (PHINMS)"

[72] VPN Consortium (2006) "VPN Technologies: Definitions and Requirements" http://www.vpnc.org/vpn-technologies.html

[73] Wikipedia.org "Virtual private network" http://en.wikipedia.org/wiki/Virtual_Private_Network (current May 25, 2006)

[74] Westin, A. (1967) "*Privacy and Freedom*", New York, 1967

[75] [Ferraiolo, D. and Richard K., (1992) "*Role Based Access Control*", 15th National Computer Security Conference.

[76] S. Osborn (1997), "Mandatory Access Control and Role-Based Access Control Revisit", Department of Computer Science, The University of Western Ontario

[77] ATIS Committee T1A1 "Discretionary Access Control (DAC), Telecom Glossary 2K http://www.atis.org/tg2k/_discretionary_access_control.html (online May 25, 2006)

[78] W.Boebert and R.Kain. "A Practical Alternative to Hierarchical Integrity Policies" Proc. 8th National Computer Security Conference, October 1985.

[78] H.A. Smith (2001) "A Context-Based Access Control Model for HIPAA Privacy and Security Compliance" http://www.sans.org/rr/whitepapers/legal/44.php

[79] Chandramouli R. (2001) "A Framework for Multiple Authorization Types in a Healthcare Application System"

[80] Sandhu R. et al (1996) "Role-Based Access Control Models", IEEE Computer, Volume 29 Issue 2, pp. 38–47

[81] He Q. (2003) "Privacy Enforcement with an Extended Role-Based Access Control Model" http://www4.ncsu.edu/~qhe2/publications/csc890report_final.pdf

[82] Castano S. et al (1994) "Database security", Addison Wesley publishing company

[83] "*Defining Access Control Mechanisms for Privacy Protection in Distributed Medical Databases*", Mavridis et al (1999) http://infolab.gen.auth.gr/Phd/mavridis/WUIPP99.pdf

[84] Hansen F, Oleshchuk V. "Security Model for Wireless Environments Based on Spatial Role-Based Access Control" Conference on Information Security and Cryptology, Higher Education Press 2005; 129-138.

[85] Aftenposten.no ”Ansatte snoker i pasientjournaler”, May 5th 2004, http://www.aftenposten.no/nyheter/iriks/article787554.ece

[86] Crawford, M.H. et Al.(1999)“ACC/AHA Guidelines for Ambulatory Electrocardiography: Executive summary and Recommendations” American College of Cardiology