# Securing Mobile Healthcare Systems Based on Information Classification: DITIS Case Study

Eliana Stavrou[1], Andreas Pitsillides[1]

[1] Department of Computer Science, University of Cyprus
P.O. Box 20537 CY1678, Nicosia, Cyprus

**Abstract.** Healthcare applications require special attention regarding security issues since healthcare is associated with mission critical services that are connected with the well being of life. Security raises special considerations when mobility is introduced in the healthcare environment. This research work proposes a security framework for mobile healthcare systems based on information classification into security levels. By categorizing the information used in mobile healthcare systems and linking it with the security objectives and security technologies, we aim in balancing the trade-off between security complexity and performance. Furthermore, this paper discusses a number of issues that are raised in the healthcare environment: privacy, confidentiality, integrity, legal and ethical considerations.

## 1 Introduction

The introduction of mobile services into our every day work has changed the way people interact with each other, process information and complete mission critical tasks. Within the framework of mobile services, the healthcare sector has evolved in such a way meeting the needs of its patients for an enhanced quality of care. A number of mobile healthcare applications exists today taking advantage of modern information technology in information systems and supplementing traditional delivery of healthcare services. Benefits from this trend include among others, improved communication among the healthcare professionals, instant access to medical information, and effective management of people (such as healthcare professionals and patients) and information, all these leading to the number one priority of healthcare sector for improved quality of care and patient satisfaction.

Healthcare applications require special attention regarding security issues since healthcare is associated with mission critical services that are connected with the well being of life. However, mobile devices raise extra security considerations since mobility encompasses other dangers such as physical threats and compromization of sensitive information stored on mobile devices. In addition, limitations of mobile devices (limited battery life, computational power) often affect the security technologies adopted. Therefore, it is essential to use security solutions in an effective way so that healthcare services can be provided without been affected.

Stavrou E. and Pitsillides A. (2006).
Securing Mobile Healthcare Systems Based on Information Classification: DITIS Case Study.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 67-79

This research work proposes a security framework for mobile healthcare systems based on information classification into security levels. By categorizing information used in the healthcare application and by linking it with the security objectives and security technologies we aim in balancing the trade-off between security complexity and performance. The proposed security solutions are further categorized based on the security objective they serve.

Furthermore, this paper discusses a number of issues that are raised within the mobile healthcare environment: privacy, confidentiality, integrity, legal and ethical considerations. Nowadays, there are various mobile healthcare applications that are in use, many of which are initiated in a research project context. WARD IN HAND (IST-1999-10479) allows the management of key clinical information while providing decision support to mobile medical staff of a hospital ward, MOBIDEV (IST-2000-26402) promises to provide mobile users with secure access to the Hospital Information System in and outside the hospital, using web interfaces based on Bluetooth technology and GPRS/UMTS networks and also improve user friendliness via voice commands, DOCMEM (IST-2000-25318) and MOMEDA (HC 4015) aim to offer web access to electronic patients records (EMR) via multimedia terminal and possibilities of remote consultation, SMARTIE (IST-2000- 25429) aims to develop web tools for multi-platform EMR access and support for medical error prevention, MTM (IST-1999-11100) provides via a local wireless network multimedia medical support to the mobile hospital personnel. These projects are based on a variety of technologies (e.g., GSM, GPRS or local wireless networks) and face the mobile health care problem from a variety of angles. Although all healthcare applications have implemented some kind of security, none is concerned in adequate detail with the security challenges that are raised in the mobile environment.

This work is made in the context of DITIS case study, a mobile telemedicine application and is organized as follows. Section 2 discusses related work. Section 3 briefly describes the case study. Section 4 presents the security framework based on the information classification. Section 5 constitutes conclusions.

## 2 Related Work

A number of guides [1], [2], [3], [4] exists today providing information on how to classify confidential information for a variety of sectors like the government and the healthcare sector. Through out our research, no security framework has been detected to be focused on information classification and which is applied on mobile healthcare systems. However, healthcare security frameworks exist that do not take into consideration information classification. Markovic et al. [5] overview modern security systems which are used in medical electronic business systems and mobile healthcare systems. Bourka et al. [6] describe and assess the integration of Public Key Infrastructure security mechanisms (such as strong authentication and encryption) in an electronic referral and prescription application. Spinellis et al. [7] proposed a secure framework for web-based telemedical applications defining among others the relationship between security services and security concepts and technologies. Misra et al. [8] address the security challenges raised by mobile communication and discuss

the wired equivalent security showing how this concept can be applied to achieve end-to-end security in a mobile healthcare environment.

## 3 Case Study

The healthcare application and its infrastructure considered for this research are used to derive the main information and services that could be used in other mobile healthcare applications and be included into information classification, the security objectives and considerations identified and the security technologies implemented within the environment under consideration.

### 3.1 Environment

DITIS [9], [10] (in Greek it stands for Networked Collaboration for Home healthcare) is an Internet-based Group collaboration system with fixed and GSM/GPRS mobile connectivity.

DITIS was initiated in 1999, supporting the activities of the home healthcare service of the Cyprus Association of Cancer Patients and Friends (PASYKAF). DITIS supports homecare by offering wireless healthcare services for chronic illnesses with emphasis on prevention, assessment and diagnosis. The main service is the dynamic creation, management and co-ordination of *Virtual Collaborative Healthcare Teams* for the continuous treatment of a patient at home, independently of physical location of the team's members, or the patient. For each patient a flexible (dynamic) virtual medical team is provided, made up from visiting homecare nurses, doctors, and other healthcare professionals, responsible for each case that may not be physically located at the same time at a particular patient. The team has easy and timely access to the unified Electronic Medical Record database to retrieve information about a patient i.e. the current medical treatment and modify it as needed, as well as a range of collaboration tools and services. Currently, the main mobile device used within DITIS application is Sony Ericsson P900 mobile phone.

### 3.2 Stakeholders

Currently, DITIS application is used by the following categories of people:

Healthcare professionals (i.e. oncologists, cardiologists)
Nurses
Therapists (i.e. physiotherapists, social workers)
Secretarial personnel

All people aforementioned are working for the welfare of the patients.

### 3.3 Services

The main services that are provided through DITIS application are the following:

Demographics
- Medical history

Symptoms registry
Diagnosis
Treatment
Medication
Virtual Team registry
Statistics
Appointments

## 4 Security Framework

In this section, a classification of information into security levels is proposed based on the data and services that could be used in a mobile healthcare application, followed up by the identification of the security objectives and considerations raised within such an environment. Furthermore, appropriate security technologies are categorization under each objective. Finally, an association between the categorized information, the security objectives and security technologies is made, aiming in balancing the trade-off between security complexity and performance. In this way, implementing a complex and flat security architecture that will degrade the performance of the provided services, is been prevented. Security technologies must be used in a smart and efficient way in order to balance security complexity and performance.

### 4.1 Information Classification

According to the Council of Europe Recommendation R(97)5 on the Protection of Medical Data "*Appropriate technical and organizational measures shall be taken to protect personal data - processed in accordance with this recommendation - against accidental or illegal destruction, accidental loss, as well as against unauthorized access, alteration, communication or any other form of processing. Such measures shall ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks*."

It is obvious that the medical data is placed on the center of all efforts towards security. As stated earlier, a number of guides [1], [2], [3], [4] provides guidance on how to classify confidential information.

The proposed healthcare security framework defines a four level classification:

Public level. Information is categorized in the public level if it is intended to be used by any interested party. This level includes: educational material, press releases, annual reports, and statistics. Security mechanisms are not needed for this level.

Internal Use Only level. Although this information is intended to be used internally, compromization will not impact the organization. Internal Use Only information involves demographics, internal project reports, appointments and the virtual team assigned to each patient. Security is required but kept at minimum levels.

Confidential level. This category involves patients' medical records that are accessed by appropriate personnel on a need-to-know basis. Medical records include, among others, information on medical history, symptoms, diagnosis, treatment and medication. Security at this category must be highly defined.

Highly confidential level. This level involves medical records of special content such as information related to physical abuse, HIV status, and abortions. Furthermore, it includes medical records of recognized people (such as the president of a country) that their wok position is considered critical.

### 4.2 Security Objectives

Based on DITIS profile and taking into consideration the fact that DITIS is a mobile telemedicine application, the security objectives that are defined using the OCTAVE (Operationally Critical Threat, Asset and Evaluation) technique [11] are the following:

- Confidentiality

Confidentiality ensures that sensitive information is kept secret and is available only to those who are authorized to access it. Since information is related to sensitive personal information such as medical records, Data Protection Law [12], [13] restrictions should be followed. Furthermore, the network architecture and sensitive configurations must be kept secret from people without the need to know.

Confidentiality objective is more complex to maintain when sensitive data is stored on handheld devices since a device can be lost. Furthermore, mobile communication uses the airwave that is open to adversaries that could eavesdrop on the communication and steal sensitive data.

In DITIS, the healthcare professionals are greatly concerned with the medical confidentiality. As mentioned earlier, a variety of job roles are involved in DITIS, raising considerations for people that are not bound by the medical confidentiality (such as a secretary), since these people can compromise sensitive information. People involved in DITIS require that appropriate penalties are created so that if someone is found compromising confidentiality then she/he must be considered liable.

Loss of confidentiality can cause great damage to the reputation of a certain patient that may embarrass him and affect his life as he could even loose his job. For this reason, and with respect to the privacy and confidentiality objectives, the healthcare team is obligated to inform the patients that they use their personal information in order to provide their services. Patients must give their written consent in order to store and process their personal data; in this way the healthcare team is legally covered in a case of a lawsuit.

- Integrity

Integrity protects systems and information from unexpected modifications. Since a healthcare system relies on the integrity of the information to function with accurate outcomes, integrity objective is a top-level requirement. Therefore, there is urgent need to make sure that information is traveling from one end to the other without being intercepted and modified in the process. Medical records must be kept accurate and be modified only by authorized personnel. System configurations must be up to date and modified by authorized members of the development team to preserve the stability of the system.

The healthcare team considers unacceptable situations where medical information is altered in any way. The success of DITIS system is mainly depended from the team's satisfaction that must trust it 100% in order to use it for their everyday work. After all, at the end of the day the healthcare team will first take the blame if they provide services based on inaccurate data and cause damage.

- Availability

Information and systems should be accessible at any requested time. Due to the nature and criticality of the healthcare sector, medical records and systems must be available on a 24/7 basis to nurse patients quickly and effectively at any time needed. Loss of availability can cause severe damage especially for online service-oriented systems that depend on information to function; in the case of healthcare systems the damage may cause even death. DITIS healthcare team made it clear that since they are dependent on the system to offer their services, they expect uninterrupted flow of operation at all times.

Furthermore, availability problems may arise due to battery constrains. Without a lightweight security solution, the battery of handheld devices may be absorbed quickly resulting in loss of availability at the point of care.

- Authentication & Authorization

Authentication and Authorization are two related concepts. Authentication provides a way to proof identify of a user and authorization determines whether an authenticated user has the credentials to carry out a certain activity. Healthcare and development team members should be assigned special credentials to access the system and information stored on them. Proper security education should be provided to prevent people from exchanging passwords or performing other actions that could endanger the safety of people, information and systems.

These objectives are directly related with information classification. Low sensitivity levels may need simple authentication methods where highly sensitive levels could require a combination of techniques.

- Logical Access Control

Access control is essential for any system that handles sensitive information since it implements appropriate mechanisms to protect the system and resources against

unauthorized access. As mentioned earlier, mobile healthcare services raise extra considerations since they support the continuity of life. Therefore, healthcare information must be accessed on a need-to-know basis. Since a mobile healthcare application requires a fixed infrastructure to function that hosts a number of servers such as web and database servers, appropriate configurations must be made to provide access to data only to the designated personnel.

The most valuable asset of any healthcare application is the medical records that hold specific medical data about a patient i.e. health condition, medication treatment. This information is hosted and can be retrieved from the database server(s). Therefore, in order to maintain the security of the systems and information, different logical access control mechanisms should be provided to safeguard different levels of sensitivity. For example first level access control should be implemented for information shared between the healthcare team while second (or more) access controls should be applied for information designated for a group of users such as nurses, social workers, and physiotherapists.

- Accountability

Actions taken by legitimate users can be tracked down. By doing so, a user is accountable for his actions. Mechanisms should be in place to protect people from been accused for something they did not do. In addition to this, appropriate legislation must be in place to legally cover people when they performed well their responsibilities.

DITIS healthcare team considers this requirement to be one of the most basic challenges they have to face in their work. For example, the nurses need to be sure that the system identifies doctor X as the person who changed the medical treatment of patient Y. Nurses are responsible only for the provided treatment, in accordance with the prescribed protocol, but they are not responsible for its selection.

- Physical security

Since the study is focused on mobile healthcare applications, physical security of the mobile devices is a critical objective that must be achieved in order to protect sensitive information that is stored locally on the devices. Mobile devices can be easily misplaced or lost. Therefore, appropriate techniques must be applied to maintain security even though a mobile device is stolen.

### 4.3 Security Technologies Classification

As stated earlier, this section briefly discusses appropriate security technologies that should be included in a security framework and support the previous defined objectives. These technologies are also implemented within DITIS environment, expect if indicated otherwise.

### 4.3.1 Integrity & Confidentially

There are many places where the data may be intercepted; for example at the client side, when synchronizing data or at the server side. In order to retain the integrity and confidentiality of the data it is a necessity to implement end-to-end encryption between the mobile device and the fixed infrastructure or implement encryption on the device to encrypt stored data that need protection.

- Public Key Infrastructure (PKI)

PKI [14] makes use of the technology known as public key cryptography. Public key cryptography uses a pair of keys to encrypt and decrypt messages, a public key and a private key. The public key is widely distributed in digital certificates whereas the private key is held secretly by its owner. Messages are protected from adversaries by encrypting them with the public key of the recipient. Only the recipient can decrypt the message by using his / her private key, thus retaining the privacy of the message.

- Virtual Private Networks (VPN)

A VPN [15] allows a user to send data between two remote devices across a public network as he was using a point-to-point private link. Information sent over a VPN connection is kept private by using a tunneling protocol and appropriate security procedures. Data is encrypted and encapsulated with a header containing routing information that is used to find its destination. In this way, even if the packets are intercepted, the attacker cannot read it or modify it without the changes be seen by the recipient.

### 4.3.2 Availability

In many cases, medical professionals like nurses may visit patients who are located away from a fully equipped hospital and use their mobile device to connect with the hospital's database and retrieve information about the patient. This communication must be retained at all times so that nurses can respond immediately to emergencies.

- Fail safe plan

In sensitive areas like the healthcare sector, the implementation and operation of healthcare applications must be performed in a well-designed environment. The main idea is to be precautious and have a fail safe plan implemented so that if anything happens (due to physical threats like fires or a security violation) with the primary infrastructure, a secondary infrastructure will take over until the problem is solved; this means that equipment must be redundant so that operation will continuously be supported. This plan may introduce overhead in managing the two infrastructures but it is a cost that needs to be taken since the benefit to be gained is more important.

- Backups

In order to support a fail safe plan, it is necessary to maintain appropriate backups of the critical data hosted on systems. Data to be backuped may include medical records, security configurations and any other data that is considered to be critical for operation and must be accessible in a 24 / 7 basis. Data must be stored on removable media or other redundant equipment and be well protected (i.e. locked down) since it could be used immediately if a system crashes and goes down.

### 4.3.3 Authentication & Authorization

Authentication mechanisms incorporate one or more of the following elements:

Something the user has, like a digital certificate or a token.
Something the user knows, like a password.
A physical attribute, like a fingerprint.

The three pillars of authentication, as they are often called, can be used separately or combined for even stronger authentication.

- Password

Mobile device users must be able to authenticate themselves to the mobile device by providing a Personal Identification Number - PIN (i.e. for mobile phones), or a password (i.e. for PDAs). Attention is needed when choosing weak PINs or passwords since they could easily be compromised and give access to an adversary that would masquerade as the legitimate user. At the most basic level, organizations should require the selection of strong passwords that would be difficult to guess.

- Digital certificate

A user's digital certificate can be required (code-specific) to either be authenticated to a mobile device or to the healthcare application in order to be able to access it and use the available services.

- Smart cards

Smart cards are hardware devices similar to credit cards. They however provide additional functionality. A smart card has a memory chip and a mini-processor attached to it. An amount of information can be stored in a smart card and used for various purposes. For instance, a smart card can be used to hold a user's private key or medical record and contact information. A smart card can have many usages. For example, a user may use his smart card for authentication purposes in order to gain access to a building, an X-Ray machine etc. Additionally, a smart card can be used to digitally sign a transaction or a document; for example, it can be used from a doctor to sign changes made to a patient's record. Currently, DITIS does not support smart card usage; it is planned as a future task.

- Biometric

Biometric [16] user authentication can be accomplished using unique characteristics i.e. face, voice, fingerprint, and retinal. Mobile devices can be configured to use fingerprint and voice biometric authentication to give access to the application in use; these authentication methods use more compact devices that are suitable for the mobility aspect of mobile devices. Currently, DITIS does not use biometrics as an authentication mean.

### 4.3.4 Accountability

- History

As mentioned earlier, a mobile healthcare application is supported by a fixed infrastructure, where a variety of systems host sensitive data like the patients' medical records. Since it is important to record a number of events like who accessed certain information, who made a change and where, when a modification happened etc, it is essential to implement history tables on the database level.

The database server that hosts the data must be configured appropriately so that history tables are created. The history tables will contain all the recorded events so that a user action can be tracked down if necessary. For an enhanced level of security, the history tables must only be accessed by the administrator of the systems or other designated personnel; in addition to this, the tables must be encrypted so that noone who has access to the database server will be able to read and modify the tables.

- Digital signature

The digital signature is created within the PKI framework and has the same purpose as a handwritten signature. When a user digitally signs an electronic document (email, spreadsheet, text file etc.) he provides a mean to the recipient to authenticate him as the writer of the document. In addition, by receiving a digitally signed document a user can verify that it has not been altered in any way since the writer created it. In the case an adversary changes the message, the PKI mechanism informs the user about the situation.

By using digital signatures in a healthcare application, we achieve non-repudiating actions. For example, a doctor changing the medical treatment of a patient cannot later deny his action. However, it is important to educate the users about issues like the importance of protecting the private key; if someone else compromises the key then he would be able to sign documents on behalf of the user owning the key.

Furthermore, it is essential to make a background research and find out if the local legislation supports the operation of digital signatures [17] and whether such evidence is accepted by a court of law.

- Confidentiality documents

Although the healthcare team must be convinced for the transparency of how the application is functioning, they also have responsibilities against the patients and against the organization offering the healthcare services [18].

Medical personnel accessing medical information have a responsibility to maintain the privacy of the data. After all, a patient's reputation may be damaged if his medical condition is publicized, for example he could loose his job.

In addition to the medical personnel, the development personnel of the healthcare application may has access to confidential documents. Therefore, it is critical to create confidentiality and code of ethics documents that must be signed by both medical and development personnel. By signing these documents, all personnel recognize the importance of keeping information confidential and also the responsibilities they have towards the organization. These documents should adhere to local and national data protection laws.

To retain the accountability objective, it is important to bind the patients as well. The patients must sign an appropriate form, acknowledging and permitting the storage and processing of their personal and medical information for providing an enhanced quality of care. In this way, the healthcare team is legally covered in a case of a lawsuit.

- Auditing

Auditing is used to check systems if they fulfil the appropriate security requirements and security policies. In addition to this, any action against the security policies is recorded for further investigation. In this way, people's action can be tracked down.

### 4.3.5 Logical Access Control

Role separation must be implemented to provide increased database security. Since the healthcare sector involves a number of medical professionals i.e. nurses, oncologists, physiotherapists, there is the need to distinguish the rights and permissions of each professional. Before deploying the application, it is essential to perform a detailed analysis in order to design access rights for each group of users. According to the organization, all appropriate user roles must be identified and their responsibilities must be documented in order to define their permissions. Based on the permissions defined, each group of users will have an appropriate view of the data stored on the database server.

### 4.3.6 Physical Security

Physical security controls [19] are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

According to NIST Handbook, "The controls over physical access to the elements of a system can include controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points".

In the case of mobile devices, there is an increased risk of theft and physical damage. Therefore, appropriate mechanisms should be developed so that after a number of unsuccessful attempts to be authenticated, all sensitive information stored on the device is locked or even destroyed.

### 4.4 Information Classification, Security Objectives and Technologies

Table 1 indicates the relationship between the classification of information, the security objectives and technologies discussed in the previous section. All these, formulate a security framework that could be adopted in a mobile healthcare environment.

**Table 1.** Information classification, security objectives and technologies association.

| OBJECTIVES | TECHNOLOGIES | CLASSIFICATION | | | |
|---|---|---|---|---|---|
| | | Public Level | Internal Use Only | Confidential Level | Highly Confidential |
| I&C | Encryption (PKI,VPN) | NO | YES | YES | YES |
| Availability | Fail Safe Plan | NO | YES | YES | YES |
| | Backups | YES (2 a month) | YES (2 a week) | YES (3 times/day) | YES (every hour) |
| A&A | Password | NO | YES | YES | YES |
| | PKI | NO | NO | YES | YES |
| | Smart Card | NO | NO | NO | YES |
| | Biometrics | NO | NO | NO | YES |
| Accountability | History | NO | NO | YES | YES |
| | Digital Signatures | NO | NO | YES | YES |
| | Confidentiality docs | NO | YES | YES | YES |
| | Auditing | NO | NO | YES | YES |
| Logical Access | Role Separation | NO | YES | YES | YES |
| Physical Access | Physical Security | YES | YES | YES | YES |

I&C = Integrity & Confidentiality, A&A = Authentication & Authorization

## 5 Conclusions

Mobile healthcare applications have revolutionized the healthcare sector. However, new challenges are raised regarding privacy, confidentiality, integrity and legal issues. All these are necessary to be addressed in a comprehensive security framework where security technologies will complement one another. By categorizing information used in the healthcare application and by linking it with the security objectives and security technologies we aim in balancing the trade-off between security complexity and performance. The target of all these efforts is to develop mobile healthcare applications for improved quality of care.

## Acknowledgements

This work is supported by the Cyprus Research Promotion Foundation under the SKINIKO project.

## References


1. Boran, S. (2003), IT Security Cookbook, Chapter 4: Information Classification
2. CSTB - Computer Science and Telecommunications Board Commission on Physical Sciences, Committee on Maintaining Privacy and Security in Health Care application (1997), For the Record: Protecting Electronic Health Information, National Academy Press, pg. 94-96
3. ISO17799 Security Standard, Section 5: Asset Classification and Control
4. Krutz, R. et al. (2001), The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, Wiley, pg. 5-10
5. Markovic, M., Savic, Z. and Kovacevic, B. (2004), Secure mobile health systems: Principles and solutions, Book Chapter in M-Health: Emerging Mobile Health Systems, Kluwer Academic/Plenum Publishers
6. Bourka, A., Kaliontzoglou, A., Polemi, D., Georgoulas, A. and Sklavos, P. (2003) PKI-based security of electronic healthcare documents, SSGRR 2003 International Conference on Advances in Infrastructure for Electronic Business, Science, Education, Medicine, and Mobile Technologies.
7. Spinellis, D., Gritzalis, S., Iliadis, J., Gritzalis, D., and Katsikas, S. (1999) Trusted third party services for deploying secure telemedical applications over the WWW, *Computers and Security*, 18(7):627–639
8. Misra, S., Wickramasinghe, N., and Goldberg, S., (2003) Security Challenge in a mobile healthcare setting http://www.itacontario.com/policy/wireless/WES-v4-conf.pdf
9. Pitsillides, A., Pitsillides, B., Samaras, G., Dikaiakos, M., Christodoulou, E., Andeou, P. and Georgiades, D. (2005) DITIS: A Collaborative Virtual Medical Team for the Home Healthcare of Cancer Patients, Book Chapter in M-Health: Emerging Mobile Health, Kluwer Academic/Plenum Publishers.
10. Pitsillides, B., Pitsillides, A., Samaras G. and Nicolaou, M. (2004) DITIS: Virtual collaborative teams for improved home healthcare, Book Chapter in 'Virtual Teams: Concepts and Applications', ICFAI University Press.
11. Alberts C, Dorofee A. “Managing Information Security Risks: The OCTAVE approach”, Addison Wesley Publisher 2002
12. European Union Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
13. Council of Europe (1997), Recommendation R(97)5, On the Protection of Medical Data
14. Digital Signature Trust, PKI basics: Digital Signatures and Public Key Infrastructure http://www.digsigtrust.com/support/pki_basics.html
15. Microsoft, (2000) Virtual Private Networking in Windows 2000 http://www.microsoft.com/windows2000/docs/VPNoverview.doc
16. Reid, P. (2003) Biometrics for Network Security, Prentice Hall
17. European Union Directive 1999/93/EC on e-Signatures
18. NHS Code of Practice (2003) Confidentiality http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf
19. NIST Handbook (1996): An Introduction to Computer Security, Chapter 15: Physical and Environmental Security