# Security in Medical Telediagnosis

J.-B. Aupet, E. Garcia, H. Guyennet, J.-C. Lapayre, and D. Martins

LIFC - EA 4269, Université de Franche-Comté,
16, Rte de Gray - 25030 BESANCON Cedex, France

**Abstract.** Telemedicine is the process by which electronic, visual and audio communications are used to support practitioners at remote sites with diagnosis and consultation procedures, such as remote clinical examinations and medical image transfers. Telemedicine is legally regulated by laws and constraints regarding the access of data contained in Personal Medical Files. These requirements are given by international entities such as IHE. They often specify the required functionalities to meet requirements of information exchange in the medical field. These functionalities are presented in this paper and outline some technical examples for their implementation in each level: authentication, communication, data storage, tracking and patient identification.

**Keywords :** Authentication, Biometric, Cryptography, Medical Software, Medical Data, Remote Telesurgery, Secured data, Secured Network, Telediagnosis, Telemedicine, Tracking.

## 1 Introduction

Over the past 10 years, the concept of working remotely (teleworking) has been in rapid development. This phenomenon is due in large part to the parallel growth in high performance networks and processors, but also due to the improvement of security in these systems. Teleworking is used in various ways such as distant learning, remote maintenance and even telemedicine. The CARTOON (Collaborative Architecture Distributed Algorithm Optimization and Network) Group at the LIFC (Franche-Comté Computer Science Lab. in France) has acquired a good experience on collaboration management for medical e-diagnosis. The TeNeCi project(Collaborative Teleneurology, 2006) and the Decopreme project (Precocious Collaborative Screening of Melanomas, 2007) are parts of INTERREGIII program in collaboration with Swiss partners (Vaud University Hospital at Lausanne, and EPFL Lausanne).

Telemedicine is generally used in a non-acute setting for patient monitoring or education and has only recently been introduced into emergency care. Telemedicine can be defined as the use of telecommunication technologies to provide medical information and services. It is the process by which electronic, visual and audio communications are used to support practitioners at remote sites with diagnosis and consultation procedures, such as remote clinical examinations and medical image transfers.

For this kind of application, graphic interface and additional tools must facilitate actors capacity to disregard distance and time in order to reconstitute a virtual examination room. Software and network architecture have to be optimal to improve interactivity and fault tolerance. Our aim is to obtain a secure environment to exchange medical data, diagnoses and opinions.

This chapter is composed of four sections after this introduction. In section two, we present the security requirements for telemedicine and telediagnosis. Section three exposes methods of authentication such as cryptography with certificates or SSO modalities and other solutions. Section four presents a secured medical data storage then in the next section a state of art in secured data transfer. Finally the last section describes a new secured telemedicine software which shows solutions to implement security in this kind of application.

***Definition of Telemedicine and Telediagnosis.***
It is interesting at the beginning of this chapter to define the context of our study. ((SET 2009), (ISfTeH 2009)).

The rapid progress in telecommunications in recent years has allowed the practice of telemedicine to grow. Telemedicine means "*practice of medicine remotely by means of telecommunication*". It is multifaceted:

***Telesurveillance.***
For example, the tools to supervise patients at home using internet or GPRS. The EPI-MEDICS project and the UR-SAFE project try to propose solutions for remote monitoring of patients. The idea is to give to the patient a mobile device that can retrieve and transmit data such as blood pressure or heartbeat (Mailhes 2003), (Gouaux 2002).

***Telesurgery.***
In September 2001 the first telesurgery was realized by Professor Jacques Marescaux (Marescaux 2001), (Marescaux 2002) specialist in digestive surgery. He operated from New York a patient who was at the Strasbourg hospital. Another form of telesurgery is teleassistance for operating gesture and remote handling. In this domain, another projects make it possible to share patient's medical records in real time for in-depth analysis and enhanced preparation of optimum surgical strategies : for example Argonaute3D (Le Mer 2004).

***Teleconsultation.***
Teleconsultation is used in different fields of medicine (such as neurology (Garcia 2005) , psychiatry (Worth 2003), or dermatology for precocious collaborative screening of melanomas (Elmarzouqi 2007), ...). It is a possibility to allow a practitioner a distant help (Mlabs 2009) with a Multimedia Conferencing System for example), by a senior practitioner for example. This collaboration between practitioners is not new, it has existed for a long time, but the means were different: in general, information exchange was done by phone. For example, on Figure 1 a patient arrives to the hospital and is admitted to the emergency service (a): different data are collected (electroencephalography, cerebral scan...).

Now it is possible, in real time, to have a distant help with a practitioner (b) or with a staff of practitioners (c).

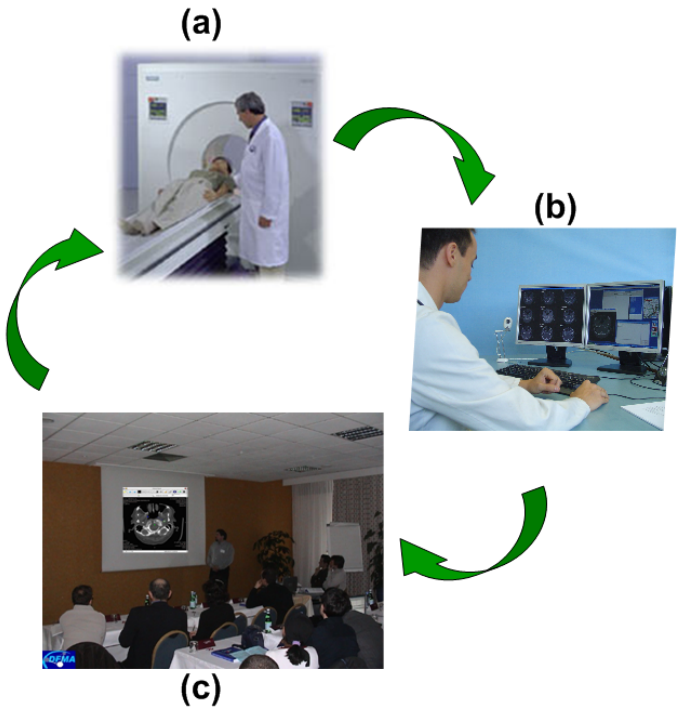


**Fig. 1.** Telediagnosis example: (a)Emergency, (b)Remote Practitioner, (c) Telestaff

***Teleexpertise.***
The idea is now to allow remote expertise. Many projects are developed for the tele-use of echography (figure 2): the OTELO project (*mObile Tele-Echography using an ultra Light rObot) (OTELO 2004), the ESTELE project (*Expert System for Tele Echography), the ARTIS project 2 or the TERESA project in (Vieyres 2003). These projects propose a solution to make an echography remotely: for example TERESA is a tele-echography project that proposes a solution to bring astronauts and remotely located patients on ground quality ultrasound examinations despite the lack of a specialist at the location of the medical act.

***Remote Vocational Training.***
During a practitioner's career, it is necessary that the knowledge is put up to date regularly: medicine evolves. Vocational training is not necessarily given

in hospitals and it is very interesting to minimize the business trips of senior practitioners: the remote teaching is one of the solutions.

***E–health Network.***
These networks are developed to encourage access to the medical attentions, coordination, continuity or interdisciplinary of care, notably of those that are specific to some populations, pathologies or sanitary activities. They assure an adapted care to the needs of the patient: from the education to health and prevention to the diagnosis. They can contribute to the actions of public health.

In all of these telemedicine domains the security is an important point. Access is remote by the networks and computer systems. And therefore problems of security appear: connection to the system, securization and transfer of data.

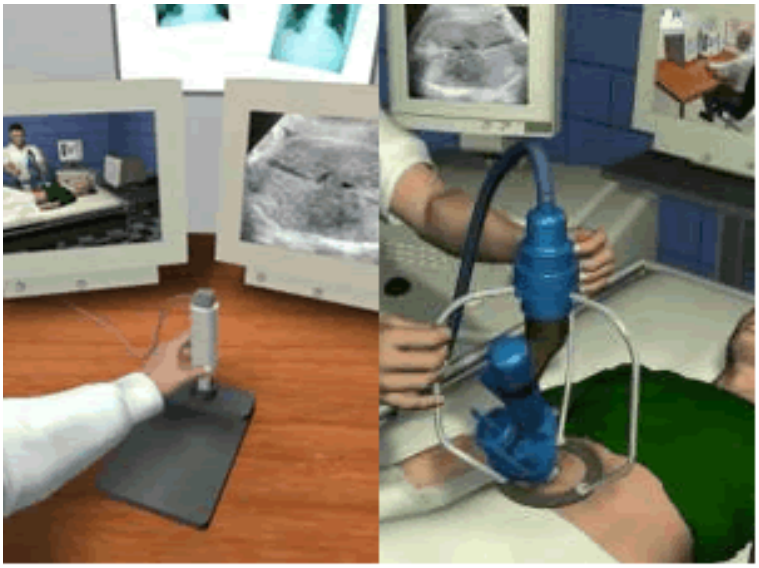

**Fig. 2.** ARTIS project: Remote Tele Echography

## 2 Security Requirements for Telemedicine and Telediagnosis

Many technologies are now available to secure electronic information in all domains. Telemedicine has its own rules depending on the country in which they applied.

We can find different directives in the laws of the different countries; we can also find requirements given by international entities such as IHE. They

often specify the functionalities to meet requirements of information exchange in the medical field. Some countries also require a certification of the telemedicine applications to allow their deployment.

These functionalities are presented in this paper and outline some technical examples for their implementation. Among these features, we can find:

***The authentication.***

The first requirement concerns the methods of authentication. The aim is to ensure that a user is allowed to enter the system and manipulate confidential data. It also requires the ability to verify if a specific user (e.g. a physician) can access the data of a particular patient according to the rules applied in the country. A patient for example can choose his doctor and ask to be allowed to have access to only part of the file.

In addition, the node (computer) used by the user also needs to be authenticated in different applications, for example, for applications that need to connect to high security systems, such as PACS (Picture Archiving and Communication Systems). In this case, only identified stations are allowed to send and retrieve data from the system. Even if the user is authenticated and authorized, he can't perform transfer with these systems without being on allowed nodes. Indeed, a great number of medical systems are in shared access, and the identity of the computer is more important than the identity of the user. The physical access to these systems is often controlled.

Authentication of users and nodes can be managed by many technologies, including login/password, card, RFID card, biometrics... It is frequently recommended to use certificates in most cases based on X509 to encrypt communication.

As the authentication becomes more and more required, a health information system composed of several applications makes it heavy for the user to launch. Indeed, he will have to authenticate several times, with several means, therefore, it is recommended to use a unique mean of authentication (based on a RFID, on a login/password with a LDAP repository...) with a policy avoiding multiple authentications. It can be a RFID which automatically authenticates the user when he launches an application, or an SSO system (Single Sign On) asking the login/password once and using it for each application.

***The data security.***

All data has to be secured when stored and during communications. Two means can be used: the use of a VPN and data encryption. The second one may be used to avoid the installation of a VPN technology. Encryption provides security for information while in transit. Different technologies can be used for encryption: DES, 3DES, AES... A common way to transfer data is to use SSL or TSL connections. Medical systems can also have to meet integrity control requirement. In this case the use of digital signature is recommended. This allows the system to check the identity of the sender and ensure that data has not been modified by another user. Anonymization must also be respected. There exist cases where the identity of a patient must be automatically deleted by the system like the

use of medical data for scientific or teaching use. Generally, images belong to the hospital, and if a user wants to send them to someone out of the hospital, telemedicine system has to support this functionality.

The requirements have to be met without making it too heavy to deploy and use telemedicine applications (they have to be compliant with common security functionalities such as proxies and firewall).

***The tracking.***
Medical applications need to offer audit trail tools that track all exchanges of medical data. IHE ATNA specifies a standard way to log these events. Reliable Syslog (RFC 3195) is the recommended transport protocol for audit messages. Events and audit trail messages are based on IETF, DICOM, HL7 and ASTM standards. For example, one must log successful connections, as well as successful and failed transfers... Such a system must allow the administrator to verify who has used the system and who has accessed a patient file...

Another issue here is the recording of actions during a work session. Let us take the example of a collaborative diagnosis. All or part of the actions could be recorded. In such cases, the telemedicine application has to provide the functionalities to keep a guaranteed information such as: who has performed this action... These records could be used for teaching, knowledge management, as well as for responsibility research.

***Other specific requirements.***
**Patient Identification:** Many countries do not have a unique patient ID for different sites, thus another important requirement for a telemedicine system is to ensure that a patient is highly identified (on one site or on different sites in case of transfer) in the system to avoid any error. PIX standard is often used for such a feature.

**Storage:** Storage is also a large issue in data security. Two aspects must be taken into account:

- to protect data from intrusion: this is made by encryption of data and by putting the data on protected servers
- to protect data from loss: this is ensured by using replicated servers with backup functions and using a specific life cycle of data (recent data is stored on server hard disks, and then stored on other type of supports according to their age).

**Bandwidth:** Some countries have a separated network for the health system. To deploy an application on such a network, a certification could be required. Software is tested for security issues but also for bandwidth consumption and avoids deploying an application that could break down the network. It is a feature to take into account to obtain this type of certification.

## 3 Methods of Authentication

Telemedicine is legally regulated by laws and constraints regarding the access of data contained in Personal Medical Files. Telemedicine systems must formerly respect these obligations. Patients could have access to their personal files, know what information it contains, who has entered the information and have the ability to rectify or delete saved information. To ensure these requirements, the system must implement strong and sure authentication methods and traceability mechanisms.

Authentication is the process of determining whether someone or something is, using a method approved by the asked information provider (application, database, internet server...). Authorization rights were also managed by the authentication scheme. With the increase of data transmission on computer networks, the rate of sensible data transmitted is becoming important. So the authentication is required ensure the identity of each actor on the system. This concept has been studied since the early days of computing (Lamport 1981), networking (Needham 1978) and distributed system (Lampson 1992).

In Telemedicine softwares, patient's files should be accessible only for allowed practitioners and only with patient agreement. When the user (or machine) has been authenticated, secured data can be exchanged and the access to the allowed services according to the granted rights will be authorized. There exists different methods of authentication but each has advantages and inconveniences.

The authentication process is a compromise between the measure of risk and the computing time to authenticate, but also depend on the computing possibilities of the terminal, for example, mobile networks (MacDonald 2008), PDA, 3G Smartphone. For high risk systems such as applications and information exchanges, an authentication that accurately confirms the user's digital identity is chosen. For a low risk application, where the confirmation of the digital identity is not as important from a risk perspective, a method that is more prompt is chosen. Authentication methods differ by using something the user knows such as password (Lamport 1981), something the user has such as security token (Schwiderski-Grosche 2006) or directly a part of the user itself, biometrical properties (Tuyls 2004), (Bernecker 2006), (Ruud 2001). These methods will be enumerated and we will show how to use and combine them to make sure that no one can usurp a protected identity.

### 3.1 Authentication Possibilities

***Password Authentication.***

This is the commonly used authentication method, but is also the least secure. Password authentication verifies the identity of the user with user id and password, in order to login. The security level is set by password management including configuration of password length, type of characters used and password duration. The ability to easily crack passwords has resulted in high levels of identity theft. The risk of using passwords has resulted in deploying a layered security

strategy. Password authentication method is used only for low risk applications and other forms of authentication are required for higher risk applications.

***Lightweight Directory Access Protocol (LDAP) Authentication.***
Most enterprises use Lightweight Directory Access Protocol (LDAP) directories to handle the centralized authentication. LDAP directories, such as Active Directory, Sun One Directory, Novel e-Directory and other vendors, provide a low cost way of doing fast identity look-ups and authentication as compared to traditional databases. Today it is common to use virtual LDAP directories to quickly integrate the identity and authentication information contained in one or more databases and/or other LDAP directories. The use of these directories is a critical piece of the identity infrastructure that leads to integrating access control.

***PKI Authentication.***
Public key infrastructure (PKI) authentication, is another way of doing identity authentication. An identity is given a digital certificate by a Certificate Authority (CA). Then presented during the authentication process to verify an identity versus his own key. The level of authentication trust varies for digital certificates depending on the level of identity verification done during the identity registration process as well as the digital certificate revocation process. Digital certificates are becoming more important to authentication and verification of an identity in single sign on systems, document management systems and in web services.

***Security Token Authentication.***
Security token authentication, such as RSA secureID tokens, are used to make authentication of an identity. During the login process, or if required by a single sign on system for a higher risk application, the user is required to enter in the numbers appearing on the token screen along with their id (Figure 3). Since the numbers change randomly to the user viewing the screen (but is understood by the central authentication server), there is a higher degree of trust associated with this form of authentication. Unfortunately, operating costs for security authentication tokens are higher than the use of password and id since they have to be physically issued, replaced and recovered.

***Smart Card Authentication.***
Smart cards are another form of authentication token. Often they contain a digital certificate as well as additional identity attribute information. Information can be stored in an RFID or Mifare no-contact chip or in a microchip or magnetic stripe systems (Figure 4). Smart card authentication is becoming wide spread. The same smart cards used in an authentication process are now commonly used for access control mechanisms to enter physical facilities, buildings, floors and rooms. This type of card is commonly used in medical infrastructures

**Fig. 3.** Token Generator


**Fig. 4.** Smart Card

to secure rooms and authenticate users, therefore it can be used to authenticate users on the information system.

***Network Authentication.***
Network authentication is the process of granting a user (or node) the ability to authenticate a network as well as their authorization. Almost all network authentication systems are now LDAP based, including Microsoft 2000, Linux, Solaris, AIX and HPUX. Many mainframe authentication systems such as RACF are now LDAP enabled. Network authentication is commonly assured by password, but most enterprises replace or add to this system another authentication modality.

***Biometric Authentication.***
Biometric authentication is the process of taking a "piece of you", digitizing it to formerly authenticate the user on the system, then he can access his personal directory or database. Typical types of biometric authentications include digital finger prints, hand scans, retina scans, digital signature scans or vein scans (figure 5). All these technics are available and can be used for authentication. They can compared with several criteria such as False Accept Rate and False Reject Rate (table 1) and the Equal Error Rate that is a result of both as shown (figure 6). Biometrics are commonly used as part of an array of authentication methods used in information systems.

### 3.2 SSO Modalities

Single Sign On (SSO) is the ability of a user to enter the same id and password to logon to multiple applications within an information system. As passwords are the least secure authentication mechanism, single sign on has now become known as reduced sign on (RSO) since more than one type of authentication mechanism is used according to risk models. Single sign on can also take place between enterprises using federated authentication. For example, a business partner's employee may successfully log on to their system. When they click on a link to your application, the business partner's single sign on system will provide a security assertion token to your information system using a protocol like SAML,

**Fig. 5.** Vein Scanner

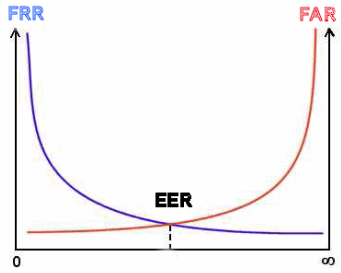


**Fig. 6.** Equal Error Rate obtention

| Part | Finger | Voice | Iris | Face | Vein |
|---|---|---|---|---|---|
| Type | Physical | Behavioral | Physical | Physical | Physical |
| Method | Active | Active | Active | Passive | Active |
| Equal Error Rate | 2 - 3,3% | $< 1\%$ | 4,1 - 4,6% | 4,1% | 1% |
| Failure to Enroll | 4% | 2% | 7% | 1% | 0.02% |
| Nominal False Accept Rate | 2.5% | $< 1\%$ | 6% | 4% | 0.0001% |
| Nominal False Reject Rate | 0.1% | $< 1\%$ | 0.001% | 10% | 0.1% |
| Liveness Aware | Possible | Yes | Possible | Possible | Yes |
| System Cost | Average | Low | Very High | High | High |

**Table 1.** Comparative table of biometrical methods

Liberty Alliance, WS Federation or Shibboleth. Your company's SSO software receives the token, checks it, and then allows the business partner's employee to access your business application without having to sign on.

For example, in a company using SSO server, users log on with their id and password, gaining them access to low risk information and multiple applications such as the business portal. However, when the user tries to access higher risk applications and information, like a payroll system, the single sign on server requires them to use a stronger form of authentication. This may include digital certificates, security tokens, smart cards, biometrics or combinations thereof.

Single Sign On benefits are:

- Ability to enforce uniform authentication and/or authorization policies across the information system.
- End to end user audit sessions to improve security reporting and auditing.
- Removes application developers from having to understand and implement identity security in their applications.
- Usually results in significant password help desk cost savings.

Since the internet is stateless, this means that the single sign on software must check every request by the user's browser to see if there is an authentication policy pertaining to the resource or application the user is trying to access. In

a medium to large company or medical center, this means that every time the user clicks on a different URL, there is traffic between the user's browser, the web or application servers and the security server. This traffic can become large and cumbersome from a performance perspective. Therefore, most modern single sign on systems use LDAP (Lightweight Directory Access Protocol) directories to store the authentication and authorization policies. The LDAP directories are made for high performance lookups thus addressing the high traffic load. Further, the LDAP directories are often the source for the single sign on system to authenticate against. Single sign on systems in medium to large information systems can become a single point of failure if not properly designed. If the single sign on system goes down but the applications remain up, no user can access any resource or application protected by the SSO system. Many companies have experienced this painful condition resulting in productivity loss. Therefore, it is essential that your single sign on system have a good and well tested failover and disaster recovery design.

Finally, single sign on systems requires good identity data governance. Security features being offered by the single sign on system is only as good as the underlying identity data. Thus it is critical that all identity data have good, quick business processes that pick up on any change to the identity such as new identity creation, identity termination or role changes. Without this, SSO systems are vulnerable to creating security holes.

## 4 Secured Data Storage

As the population of the world is growing quickly, and as new medical diagnostic technologies are developed, the traditional archival system produces several major problems in accommodating the increased demand. Consequently, more and more physical space will become necessary to store medical files, and it will become increasingly less efficient and more difficult to access and retrieve a particular medical file (Zhang 2005). In recent years, there has been an evolution of technology access and storage, and especially with increased legal obligations.

Two categories of staff have access to patient data: administrative staff, and nursing staff. Their ways to access archived data are radically different. The nursing staff is a population which is very difficult to secure manner access: open access to workstation, shared access by several people, with the imperatives of access speed incompatible with strong authentication techniques. In addition this medical data storing can be entrusted to companies outside the hospital that will also secure. All this information is new wealth for institutional care but it must be always available and reliable.

With the rapid development of computer and network technologies, it is possible to share and access to data on grid storage devices. In (Zhang 2005), a web-based medical information archive system enables storage, maintenance, sharing, updating, and retrieval of medical data based on the existing Internet facilities.

### 4.1 DICOM standard

Digital Imaging and Communications in Medicine (DICOM) (Pianykh 2008) is a standard conceived over 20 years ago for storing and transmitting medical data. This standard enables different DICOM modality such as scanners, MRI, PET, to communicate over a TCP/IP network and then exchange and store medical data into a picture archiving and communication system (PACS). The DICOM C-STORE service is used to send data to a file server (e.g. PACS). However, there is no guarantee that the data has been archived. For this reason, the Storage Commitment was introduced in addition to storage services to ensure that data received on archiving has been taken into account. It explicitly takes the responsibility of good data archiving. For example, a single workstation can implement a reception service tomography images in order to display them and then delete them after use. Another example is a scanner which produces series of medical images. Once produced, these images are sent to a server for archiving. After sending data, the scanner asks for a storage commitment. If the commitment succeeds, the scanner can delete data from its memory. Nowadays, more and more DICOM devices offer this service confirmation archiving, although this storage commitment is purely an administrative problem. Indeed, anyone can log in (username and password) on a storage device and delete some medical data.

DICOM applications offer strategies to try to tackle this problem such as lockers or no-delete flag but none of them really solve the problem.

### 4.2 Security requirements for medical data storage

All medical data are considered as sensitive to preserve patient privacy. To read the content of an image, a user needs to be authorized both to access the file and the encryption key. Data anonymization prevents the exposure of most sensitive data to unauthorized users. Several services are required to secure the storage of medical data (Montagnat 2008):

***File access control.***
Control access is most often used to assure a higher degree of security of server. This technique allows connecting any given port of the server and accept particular services and reject suspicious request for access. In the future, medical image access will use digital videos, smart phones and increasingly lighter mobile systems, consumers expect the same level of mobility from digital medicine.

***File anonymization.***
The patient data are confidential and should not be open to the general public. DICOM anonymization software keeps a list of 18 major confidential attribute types (Name, Social security numbers, account numbers) and removes them from DICOM files.

***File encryption.***
Encryption is the process of changing the format of the data to protect its content. Storing the data in encrypted form considerably reduces the risk of disclosure. The encrypting medical files before emailing them is a great way to ensure that identity thieves and others do not have access to those sensitive records. The DICOM standard permits to encrypt the data to verify the data origin and the data integrity.

***Secure access to data.***
Data should be locally stored but also faraway on a remote server. For example in teleriadiology, the images made in one location can be interpreted and read in a completely different one. The only way to transmit images faster implies better networks and the use of lossy image compression. In the case of application email, direct connection to an email server from a remote DICOM application may be rejected for security reasons or overflow mailbox quotas.

### 4.3 Distributed storage of medical data

Distributed architecture allows users from different organizations to share storage capacity and data. However distributed systems improve the number of users, the number of networks and the number of the storage devices. Because of the cross institution nature of distributed application communications, distributed storage has specific security needs. Network security is a hard-to-define paradigm in that its definition varies with the different organizations which implement it. Security is defined by the policies that implement the services offered to protect the data. Since all medical data are stored on electronic devices, it is important to establish a host-based authentication approach. In (Montagnat 2008) authors propose software architecture to implement a medical data management. This system provide access to medical sources for Grid services and users while taking into account the constraints related to clinical practice. In (Seitz 2005) authors present grids as architecture for medical image processing and health-care networks. The goal is to create a scheme that allows the storage and access to encrypted data on grid storage devices.

## 5 Secured Data Transfer

Telemedecine's applications need a secure data transfer in a network. This transfer has to ensure four requirements.

***Data Confidentiality.***
The network has to ensure that transmitted data is confidential and respects the confidentiality's rule for a patient. An external person of the network should not be able to read the information exchanged. To secure data, the exchange in the network is to be encrypted by using a private key secret that only intended receiver's posses.

***Data Integrity.***
Data in the network should not be altered by the communication. We have to ensure that nobody can enter in the network and modify data. Consequences could be the death of the patient. This is why the data integrity is probably the most important thing in the security of a telemedecine's application.

***Data Freshness.***
In medical area, the freshness of data is very important. By freshness, we mean that data is recent or not. If we do not pay attention on the freshness of data, an attacker could replay old data. For example, someone can resend critical information about a patient (such as an old decline in insulin) to mislead the nurses, therefore they give insulin to a patient, who does not need, leading to disastrous consequences.

***Availability.***
Data should always be available. It is vital that information can be transmitted without interruptions. We have to ensure that data cannot be stopped. In telemedecine's applications, every second is important and data has to be receiving in time.

In the following parts, vulnerabilities of data transfer in telemedecine's networks will be shown, such as wired networks, wireless networks and more specifically in mobile ad-hoc networks (MANET) and wireless sensor networks. Then solutions for the attacks in the different networks are presented, which can be used to secure data transfer in telemedecine's networks.

### 5.1 Vulnerabilities of telemedecine's networks

**Attacks in wired networks.**

Wired networks are obviously the most secure networks. However, Internet is often used in telemedecine to transfer data from one hospital to another. It is known that the Internet is not the most secure network. It is very important in telemedecine to have a security policy against these attacks and to know these vulnerabilities. Here is a short list of current attacks in wired networks.

***Packet sniffing.***
If data is not encrypted, packet sending on the network or in Internet can be sniffed. Then an attacker can rebuild the entire data and read data information. This attack is a passive attack, but the data confidentiality is broken, and the attacker could know private information of patients.

***Denial of service attack.***
This is one of the most known active attacks. The aim is to saturate by different ways a computer or a server. In telemedecine this kind of attack endangers the availability of the network. For example, a doctor who uses a telemedecine's

application to operate a patient with a real time server. The server sends and receives video information. If an attacker makes a denial of service attack against this server, the doctor could not finish the operation.

***Man in the middle.***
The attack of the man in the middle consists of an active eavesdropping in which the attacker makes independent connections with the victims (such as two persons communicating in two different hospitals) and relays messages between them. They believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. With this attack, an attacker can listen, modify or delete data.

***Replay attack.***
An attacker uses a sniffer to catch packets sent by a computer. Even he cannot read data, he can masquerade the network by replaying this data in the network later. The data will be compromised.

**Attacks in wireless networks.**

Telemedecine's applications use wireless networks more and more. Wireless offers more mobility and possibilities. A wireless telemedecine's application can be used for a field hospital in a war or catastrophic area. However a wireless network is less secure than a wired network, because the medium is wave. This medium allows the possibility for other specific attacks. Obviously in wireless networks, the same attacks are found as in wired network. Here are next the two specific attacks of wireless network.

***Eavesdropping.***
This passive attack consists of listening to the network to intercept information on the network. This attack is easy, if data is not encrypted and the medium is radio wave. Since this attack does not modify the data, it is difficult to detect it. It attacks directly the confidentiality of data sent by the network. An attacker could read data of patients. Even if the data is encrypted, the network can be eavesdropped, if the network uses a crypted protocol easy to break. For example the wired equivalent privacy (WEP) protocol, which is used in some hospitals, can be easily uncrypted in less than 10 minutes with a basic laptop.

***Radio jamming.***
An attacker sends radio waves at the same frequency that it used by wireless networks. The network cannot communicate if the transport medium is flooded by radio interferences and availability of the network is broken.

**Attacks in MANETS.**

Mobile ad-hoc network (MANETs) is a specific wireless sensor network. An example of MANET in telemedecine is a network with a PDA for each doctor, who communicate together and send information to one or more computers. In MANET, each computer or mobile host (PDA, sensor, etc...), called nodes, communicate with their neighboring nodes and not directly with the base or sink. In a wireless network, hosts communicate directly with a base station, which sends data to the Internet or sends information to another computer. But in MANET, a node, which will communicate information to the base station or a specific node, has to find the lower path to the receiver and send data to its neighbors. The neighbors will then send data to their neighbors and finally data will be received by the base station or the receiver. The particularity of this kind of network creates the possibilities of other specific attacks.

***Black Hole Attack.***

The black hole attack consists at first the insertion of a malicious node in the network (Karlof 2003) (laptop, sensor, pda, etc..). This malicious node, will change routing tables, in several ways, to force a maximum of neighboring nodes to send data to it. After that, like a real black hole in space, all recovered data will never be sent back by the malicious node.

***Selective Forwarding (Grey hole attack).***

This is a variant of the black hole attack (Karlof 2003). Like in the black hole attack, an attacker will insert a malicious node in the network and this node will change the routing to capture data around it. Unlike the black hole, the attack of selective forwarding relays information. For example, the malicious node will relay all information concerning the routing and it will not relay data, which is critical. That is why, this kind of attack is more difficult to detect than the black hole attack. If the malicious node works normally, it cannot easily be detected.

***Slowdown.***

An attacker can use some malicious nodes to slowdown the network. It can use a selective forwarding attack to do it. This slowdown may be crucial if the network sends critical information of a patient. The information will be slowed and the patient could die.

***Wormhole.***

This attack needs to insert in the network at least two malicious nodes (Hu 2006). These nodes are connected by a powerful connection such as a wired liaison or a powerful wireless signal. This attack wrongs the other nodes of the network by the distance between the two bad nodes, and proposes a quicker route. Generally the routing protocols search the route with the shortest number of hops. In a wormhole attack, the two malicious nodes propose to achieve a distant position with an unique hop. This possibility will wrong other nodes on the real distances that separate the two malicious nodes. The nodes will choose this shortest route for sending their data, and thus send their information to the malicious nodes. The attacker can then catch some information of the network.

***Sinkhole.***
A malicious node will attack the data directly, which circulate near the sink or base station, as the sink is the point at which there is the maximum of data on the entire network (Karlof 2003). To do this attack, the malicious node will offer the quickest route to reach the sink, using a powerful connection. Nodes, near the malicious node, will send data for the sink to it. All information, which is sent from these nodes to the sink, may be captured by the attacker.

***Sybil attack.***
A Sybil attack (Newsome 2004) is a malicious sensor which is masquerading as multiples sensors. It will modify the routing table, which will be wrong.

**Attacks in WSNs.**

Wireless sensor networks or WSNs are specific MANETs. They can be used by example in telemedecine with one or more patient wearing sensors to know their health status such as the CODE BLUE project (Malan 2004). The specificities of WSNs are a low power of calculation and a limited energy. These two differences are used by attackers to endanger the network.

***Sleep deprivation torture.***
An attacker sends many messages or asks calculations to a sensor. The aim is to prevent the sensor to sleep to consume his energy until the sensor becomes out of order. This active attack prevents a sensor to sleep in different ways (Stajano 1999). If the sensor cannot sleep, it will consume its battery and be out of order. In telemedecine, if a sensor is out of order, patient data is no longer read, and the network will not receive vital information.

***Flooding.***
An attacker will use one or many malicious nodes or something else with a powerful signal, sending some messages regularly some messages into the network, flooding it. This is an active attack such as denial of service and the consumption of the energy of nodes in the network.

***Infinite loops.***
An attacker can use two or more malicious nodes to send infinitely packets on the network. As these messages will be endlessly sent by the network like a ping-pong game, sensors will consume their energy and the network will saturate.

***Pace maker.***
Pace maker is a specific sensor which uses electrical impulses to steady the beating of the heart. The pacemaker can be controlled by an external device to change the frequency of beats, however the connection is not secured. In (Halperin 2008), they show that it is possible to make an attack to derange the pacemaker. This attack shows us the problem of data transfer in a sensor without security and consequences.

### 5.2 To secure data transfer in telemedecine network

**Secure wired networks.**

Solutions of security for a telemedecine application in wired networks are not different from solutions existing in other applications that need security. The most important thing is to encrypt data. We have to use existing protocols to do it, such as Secure Sockets Layers (SSL) or Secure Shell (SSH). Both use public key infrastructure and ensure considerably data transfer, principally the data confidentiality and data integrity. The aim is to create a virtual private network (VPN) to secure data transfer. To counter denial of service attacks in telemedecine's application, which use a server for communication, it can be better to have two or more servers. If a server is attacked by denial of service attacks, the other servers can take over and ensure the availability of the network. For data freshness in data transfer, a telemedicine's application has to insert time information in encrypted packets. This time information should be encrypted too, to counter the replay attack. However, some other solutions are given by possibilities of trust computing and the trust computing group, by using a trusted platform module in the computer of the network (Abendroth 2006) to increase the security of the network.

**Secure wireless networks.**

Wireless networks can use the same solutions as wired network to secure telemedecine's application, but they need also to secure data transfer with radio waves. The principal point is to not use WEP. WEP uses the RC4 algorithm with a secret key of 40 or 128 bits. This key is too short, and it is too easy to find it for an attacker. WIFI Protected Access or WPA must be used, as it uses the TKIP algorithm or Temporary Key Integrity Protocol. The TKIP randomly generates a key and changes it many times by second. Moreover WPA uses a authentication server RADIUS for identify users and define access rights in the network. With this solution, it is harder for an attacker to eavesdrop or to enter in a wireless telemedecine's network.

**Secure MANETS.**

In MANETs, WPA2 is principally used, which is a version of WPA supporting MANET, to secure data transfer with radio wave. To counter wormhole attacks some solutions are proposed such as a packet leash protocol (Hu 2003), the SECTOR mechanism (Čapkun 2003) or using directional antennas. The fact to use directional antennas limits the available listen area, for an attacker. Moreover (Seung 2001) presents a security-aware ad hoc routing protocol (SAR), a solution against black hole attacks. Other specific solutions are discussed in (Hu 2004).

**Secure WSNs.**

The specificities of WSN are a low power of calculation and of limited energy, which require to find specific security's solution for WSNs (Martins 2008). For example in WSN, we cannot use public key infrastructure, because a sensor cannot do calculations of this security's solution (Piotrowski 2006). We can only use symmetric secret key to encrypt information. This encryption is easy to break. This is actually why security in WSNs is a big way of research. Other secure solutions need to be found, however there are two popular secure protocols, SPINS (Perrig 2002) and TinySEC (Karlof 2004), which can be used to secure a telemedecine application.

***SPINS.***
is a protocol based on two blocks of security SNEP and $\mu$TESLA indent SNEP uses two security mechanisms. The first is to encrypt to ensure the confidentiality of data and the second is to use a code authenticity of messages MAC (Message Authentication Code) to ensure authentication and data integrity between two entities.
$\mu$TESLA uses a symmetrical authentication linked to an asymmetrical method where the symmetrical keys are disclosed over time.

***TinySEC.***
is a security package integrated in the operating system TinyOS.(TinyOS 2009) The aim of this link layer is to detect unauthorized packets while they are injected for the first time into the network, to prevent their spread in the network that would generated by communications, a loss of energy. TinySEC establishes authentication mechanisms (with the use of MAC key), encryption of information and protection against duplication of information.
For authentication and encryption TinySEC uses a building cipher block channels with CBC-MAC to create and verify the key MAC. This method is particularly suitable for sensor networks because it does not require a large memory.

Outside these two protocols, the scientific community has proposed other solutions to secure a WSN. (Deng 2005) give a solution to prevent the capture of information in wireless sensor networks by the data partitioning. The aim is to divide the information into several parts. For example a message is divided into 3 packets which are going to follow 3 different routes. If someone want to read the information, he needs to have all the parts.

Another solution proposed by (Zhu 2004), (Ganeriwal 2004) and also by (Oleshchuk 2007), is to use the mechanisms of trust and reputation that can be found in peer to peer networks, community networks or even market websites like Ebay . In this kind of network as in wireless sensor networks, it is hard, to know what node can be a malicious node, because the number of nodes is large. To detect and protect the integrity of the network, each node of the network will monitor its neighboring nodes and their actions over time. Depending on actions taken by its neighboring nodes, a node will increase a level of trust of these nodes, based on its reputation. When a node does not carry out a request, its level of trust will fall. If this node always sends data correctly, its level of trust

will increase. With the help of these levels of trust, a node will then choose the most secure route for sending data. Instead of going through the fastest route (number of hops or geographical distance), the node will choose to send its data via nodes with the highest level of trust (the safest route).

## 6 Presentation of Secured Telemedicine Software

We will present the Servastic project. The aim of this software is to provide practitioners several means of assistance to take the right decisions on complex medical cases. Two tools are available:

1. a module providing image treatment functions: we can send a sequence of images to be analyzed, these functions will return results for a diagnosis assistance. (figure 7) (Covalia 2009).
2. a module providing communication tools to allow a doctor to interact with an expert on complex cases.

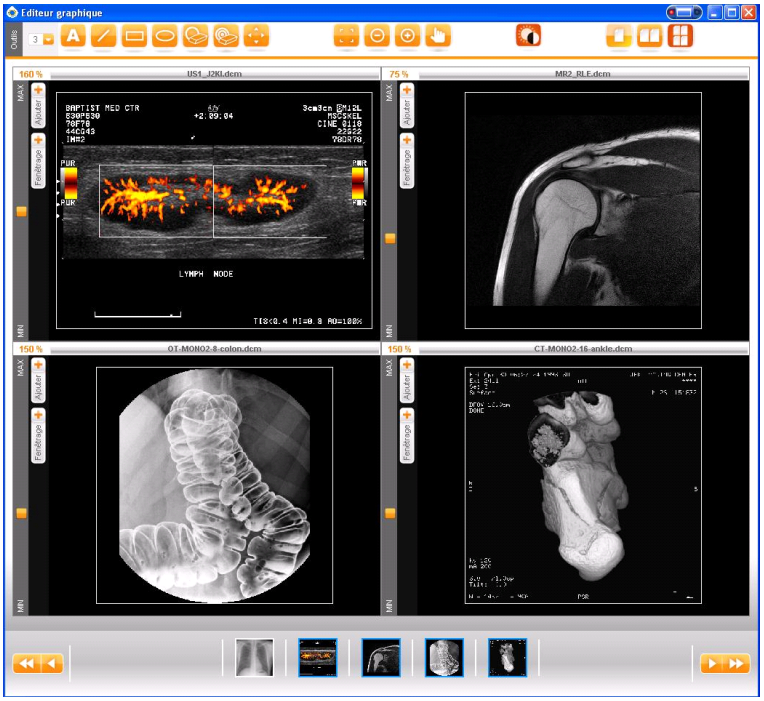


**Fig. 7.** Secured Telemedicine Software

One of the essential keys of medical imaging evolution is the transition from a qualitative analysis performed by a specialist looking at images, to a quantitative analysis providing precise statistics on these images. This kind of technique

is very useful for neuro-degenerative diseases (Alzheimer). At an early stage, anatomic changes not visible by a human can be detected by a computer with a mathematic comparison with reference images (quantitative analysis). This allows the practitioners to save time on diseases diagnosis.

The architecture of the service is presented on figure 8. The aim is to provide centralized computational services on a server. These services have to be accessible from anywhere to allowed users. A main issue is to allow these users to handle complex calculations without having particular software on their computer.

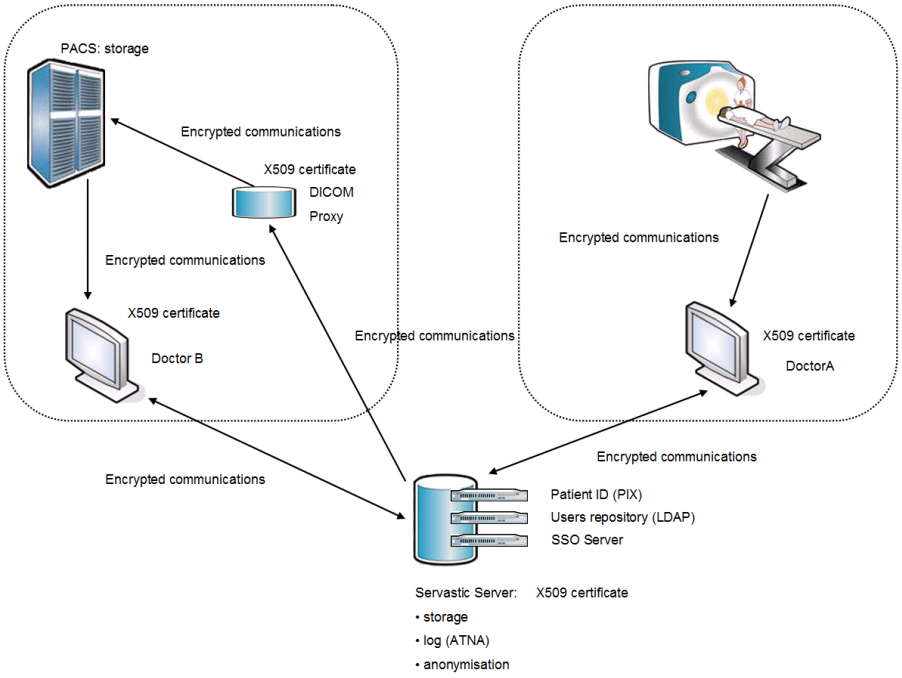


**Fig. 8.** Software Functionalities

In this case, we use several security technologies. We have a LDAP repository and a SSO server to authenticate allowed users. Each connection and calculation is logged on the server. Encryption and X509 certificate are used to ensure a secured communication (SSL connections), and an anonymization stage is performed on DICOM files (patient ID are removed from the DICOM file, we can keep a mapping with he PIX service if we wish to reuse the data).

The second module allows practitioners to interact on medical data using the network. In this case, we also use authentication, encryption of communication and stored data, anonymization using the PIX service. We have to use a node authentication when a practitioner wishes to insert data sent by a colleague in his own PACS. It can be useful if the expert wants to use its usual interpretation

station to manipulate images; in this case the images have to be put in the local PACS. As previously stated, a PACS accepts only communications with authenticated nodes. This operation is quite heavy, since we have to work with hospitals IT services to update the list of authorized nodes. We use a DICOM proxy to make it possible to send medical data from one site to the PACS of another site. For this kind of operation, the link with the patient ID service is essential. Indeed, a patient with an ID "A" in one site can have an ID "B" on the other site. It could be worse if a patient with an ID "A" already exists on the second site. We see clearly here that we have to meet the requirements of patient identification to provide a secured environment.

## 7 Conclusion

In this chapter we defined telemedicine and the different areas affected. These types of remote medical applications need a management of information security. As the population of the world is growing quickly, more and more physical space will become necessary to store medical data. In addition, patient data are confidential and should not be open to the public. Several services are required to secure the storage of data: file access control, file anonymization, file encryption and secured data access. These security features are now available with several different technologies. Medical field is in advance in standardization for data exchanges (DICOM...). Recommendations begin to appear for security management, with IHE or national security referentials.

The aim of the next years will be to guarantee a high security without making a complex use, deployment and interoperability of telemedicine applications. Security of data transfer and data storage in telemedecine's applications is very important for the development of telemedecine's applications to be aware of the risk that information could be altered if bad solutions are used to secure data. A telemedecine's application must have a strong policy to ensure that information of a patient could not be read, modify or delete.

## 8 Acknowledgement

The authors thank:
- the European Community (by the projects TeNeCi, and Decopreme), which allowed a part of the financing of this work,
- as well as the French ministry of Research and the French ministry of industry which allowed financial aids for the creation of the new startup Covalia Interactive.

## References


(Abendroth 2006) Joerg Abendroth and Jean-Marc Seigneur, Deploying the trusted platform module (TPM) to increased fairness and trust in P2P file sharing servents. *ISP'06: Proceedings of the 5th WSEAS International Conference on Information Security and Privacy (2006)*, 202–207.

(AuthWorld 2008)AuthenticationWorld.com : The business of authentication, *http://www.authenticationworld.com/*

(Bernecker 2006) Otto Bernecker, Biometrics security: An end user perspective. Giesecke and Devrient GmbH, Germany, *Information security technical report 11 (2006)*, 111-118.

(Čapkun 2003) Srdjan Čapkun and Levente Buttyán and Jean-Pierre Hubaux, SECTOR: secure tracking of node encounters in multi-hop wireless networks. *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (2003)*, 21–32.

(Deng 2005) Jing Deng and Richard Han and Shivakant Mishra, Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks. *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (2005)*, 113–126.

(Elmarzouqi 2007) Elmarzouqi, N.,Garcia,E., Lapayre, J.-C. and Humbert, P., Use of ACCM Model for teledermatology implementation. *DFMA'07, 3rd int. Conference on Distributed Framework for Multimedia Applications (July 2007)*, Paris, France, pages 84–89.

(Ganeriwal 2004) Saurabh Ganeriwal and Mani B. Srivastava, Reputation-based framework for high integrity sensor networks. *SASN (2004)*, 66–77.

(Garcia 2005) Garcia, E., Guyennet, H., Lapayre, J.-C. and Moulin, T., Adaptive Teleapplication for Remote Neurology Diagnosis. *International Journal of Telemedicine and e-Health (2005)*, 11: 6, 692–701.

(Gouaux 2002) Gouaux, F., Ambient Intelligence and Pervasive Systems for the Monitoring of Citizens at Cardiac Risk: New Solutions from The EPI-MEDICS Project. *Computers in Cardiology (2002)*, 29: 289–292.

(Halperin 2008) Daniel Halperin and Thomas S. Heydt-Benjamin and Benjamin Ransford and Shane S. Clark and Benessa Defend and Will Morgan and Kevin Fu and Tadayoshi Kohno and William H. Maisel, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. *SP '08: Proceedings of the 2008 IEEE Symposium on Security and Privacy (2008)*, 129–142.

(Hu 2003) Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. *INFOCOM (2003)*.

(Hu 2004) Yih-Chun Hu and Adrian Perrig, A Survey of Secure Wireless Ad Hoc Routing. *IEEE Security and Privacy (2004)*, 28–39.

(Hu 2006) Yih-Chun Hu and Adrian Perrig and David B. Johnson, Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications (2006)*, 370–380.

(Karlof 2003) Chris Karlof and David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks (2003)*, 293–315.

(Karlof 2004) Chris Karlof and Naveen Sastry and David Wagner, TinySec: a link layer security architecture for wireless sensor networks. *SenSys, ACM (2004)*, 162–175.

(Lamport 1981) Leslie Lamport, Password Authentication with Insecure Communication. *Communications of the ACM, Volume 24, Number 11 (November 1981)*.

(Lampson 1992) BUTLER LAMPSON, MARTiN ABADI, MICHAEL BURROWS,and EDWARD WOBBER, Authentication in Distributed Systems:Theory and Practice. *ACM Transactions on Computer Systems, Vol. 10, No. 4, (November 1992)*, 265–310.

(Le Mer 2004) P. Le Mer, L. Soler, D. Pavy, A. Bernard, J. Moreau, D. Mutter, J. Marescaux., Argonaute 3D: A real-time cooperative medical planning software on DSL network. *MMVR12, 12th Annual Medicine Meets Virtual Reality Conference, Newport Beach, California, january (2004).*

(MacDonald 2008) John A. MacDonald Authentication & key agreement for off-portal mobile applications. *information security technical report 13 (2008)*, 127-135.

(Mailhes 2003) Corinne Mailhes, Francis Castani, Stphane Henrion, Louis Lareng, Albert Alonso., The URSAFE telemedicine project: improving health care of the elderly. *MIE, Saint Malo, France, European Federation for Medical Informatics, (mai 2003).*

(Malan 2004) David Malan and Thaddeus Fulford-Jones and Matt Welsh and Steve Moulton, CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care. *International Workshop on Wearable and Implantable Body Sensor Networks (2004).*

(Marescaux 2001) Marescaux, J., Leroy, J., Gagner, M., Rubino, F., Mutter, D., Vix, M., Butner, S.E., Smith, M.K., Transatlantic Robot-Assisted Telesurgery. *Nature (2001)*, 413: 379–380.

(Marescaux 2002) Marescaux, J., Leroy, J., Rubino, F., Vix, M., Simone, M., Mutter, D., Transcontinental Robot Assisted Remote Telesurgery: Feasibility and Potential Applications. *Ann Surg (2002)*, 235: 487–92.

(Martins 2008) David Martins and Herve Guyennet, Etat de l'art - Securite dans les reseaux de capteurs sans fil. *Conference SAR-SSI (2008).*

(Montagnat 2008) Johan Montagnat and all, A Secure Grid Medical Data Manager Interfaced to the gLite Middleware. *Journal of Grid Computing (March 2008)*, (6)1 45–59.

(Needham 1978) Roger M. Needham and Michael D. Schroeder, Using Encryption for Authentication in Large Networks of Computers. *Xerox Palo Alto Research, Communications the ACM, Volume 21, Number 12(December 1978).*

(Newsome 2004) J. Newsome and E. Shi and D. Song and A. Perrig, The Sybil attack in sensor networks: analysis & defenses. *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium (2004)*, 259–268.

(Oleshchuk 2007) Vladimir Oleshchuk and Vladimir Zadorozhny, Trust-Aware Query Processing in Data Intensive Sensor Networks. *SENSORCOMM '07: Proceedings of the 2007 International Conference on Sensor Technologies and Applications (2007)*, 176–180.

(OTELO 2004) OTELO clinical and technical validation (2004). *Reference D35_WP7_2004_10_1_A (2004).*

(Perrig 2002) Adrian Perrig and Robert Szewczyk and J. D. Tygar and Victor Wen and David E. Culler, SPINS: Security Protocols for Sensor Networks. *Wireless Networks (2002)*, 521–534.

(Pianykh 2008) Oleg S. Pianykh, Digital Imaging and Communications in Medicine (DICOM). *, Springer (2008)*,377 pages.

(Piotrowski 2006) Krzysztof Piotrowski and Peter Langendoerfer and Steffen Peter, How public key cryptography influences wireless sensor node lifetime. *SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks (2006)*, 169–176.

(Ruud 2001) Ruud M. Bolle., Jonathan H. Connell, Nalini K. Ratha, Biometric perils and patches. *Pattern Recognition 35 (2002)*, 2727-2738.

(Stajano 1999) Frank Stajano and Ross J. Anderson, The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. *Security Protocols Workshop (1999)*, 172–194.

(Seitz 2005) Seitz, L., Pierson, J.-M., and Brunie, L., Encrypted storage of medical data on a grid. *Journal of Methods of Information in Medicine (Jan 2005)*, 198–202.

(Seung 2001) Seung Yi and Prasad Naldurg and Robin Kravets, Security-aware ad hoc routing for wireless networks. *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing (2001)*, 299–302.

(Schwiderski-Grosche 2006) Schwiderski-Grosche, S., Security: An end user perspective. Information Security Group, Royal Holloway, University of London, Egham, Surrey TW200EX, United Kingdom, *information securitytechnical report 11(2006)*, 109-110.

(Tuyls 2004) Pim Tuyls and Jasper Goseling, Capacity and Examples of Template-Protecting Biometric Authentication Systems. *BioAW 2004, LNCS 3087,Springer-Verlag Berlin Heidelberg (2004)*, 158-170.

(Vieyres 2004) P. Vieyres, G. Poisson, F.Courrges, O. Merigeaux et P. Arbeille, The TERESA project : from space research to ground tele-echography *Industrial robot : an international journal, Vol 30, n1, (2003)*, 77–82.

(Worth 2003) Jonathan L. Worth, M.D., and Theodore A. Stern, M.D., Benefits of an Outpatient Psychiatric TeleConsultation Unit: Results of a 1-Year Pilot. *Primary Care Companion J Clin Psychiatry (2003)*, 5: 80-84.

(Zhang 2005) Zhongfei Zhang, Ruofei Zhang, Jian Yao, Guangbiao Pu, Knudson, P.E., Weinstock, R.S. Krol, A. Medical data on demand with WebmiaEngineering. *IEEE Medicine and Biology Magazine, Volume 24, Issue 3, (May-June 2005)*, 117–122.

(Zhu 2004) H. Zhu, F. Bao, R. H. Deng and K. Kim, Computing of trust in wireless networks. *Proceedings of 60th IEEE Vehicular Technology Conference, Los Angeles, California (2004).*

**Web and Software**

(Covalia 2009) Covalia Interactive is the Covotem producer
*http://www.covalia.com/*

(ISfTeH 2009) International Society for Telemedicine and eHealth
*http://www.isft.net/*

(Mlabs 2009) Multimedia Conferencing System producer
*http://www.mlabs.com/*

(SET 2009) European Society of Telemedecine
*http://www.societetelemed.eu/*

(TinyOS 2009)TinyOS: an open-source operating system designed for wireless embedded sensor networks.
*http://www.tinyos.net/*

## Resources

### A. Key Books

Oleg S. Pianykh, Digital Imaging and Communications in Medicine standard (DICOM). *Springer (2008).*

B.S Chowdhry and Faisal Abro, Telemedecine Modernization and Expansion of Health Care Systems. *Mehran Info Tech Consultants (2003).*

### B. Key Survey/Review Articles

Otto Bernecker, Biometrics security: An end user perspective. Giesecke and Devrient GmbH, Germany, *Information security technical report 11 (2006)*, 111-118.

Butler Lampson, Martin Abadi, Michael Burrows and Edward Wobber, Authentication in Distributed Systems:Theory and Practice. *ACM Transactions on Computer Systems, Vol. 10, No. 4, (November 1992)*, 265–310.

David Martins and Herve Guyennet, Etat de l'art - Securite dans les reseaux de capteurs sans fil. *Conference SAR-SSI (2008).*

Yih-Chun Hu and Adrian Perrig, A Survey of Secure Wireless Ad Hoc Routing. *IEEE Security and Privacy (2004), 28–39.*

### C. Key Journals

Journal of Methods of Information in Medicine *(Schattauer).*

International Journal of Telemedicine and Applications *(Hindawi Publishing Corporation).*

International Journal of Telemedicine and e-Health *(Mary Ann Liebert, Inc. publishers).*

IEEE Security and Privacy *(IEEE).*

IEEE Medicine and Biology Magazine *(IEEE).*

### D. Key International Conferences/Workshops

CSCWD - International Conference on Computer Supported Cooperative Work in Design.

DFMA - International Conference on Distributed Frameworks for Multimedia Applications.

E-MEDISYS - E-Medical Systems International Conference.

MMVR - Medicine Meets Virtual Reality Conference.

SECURECOMM - International Conference on Security and Privacy in Communication Networks.