# ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
## ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ


# POLICIES IN THE HEALTH CARE TO SUPPORT PUBLIC KEY INFRASTRUCTURE


**Μάριος Πιερή**

Επιβλέπων Καθηγητής
Ανδρέας Πιτσιλλίδης



Η Ατομική αυτή Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Master Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Ιούνιος 2003

**ABSTRACT**

**ABSTRACT**

In this thesis, an approach for securing health information transactions over the public Internet or private networks is investigated. This is commonly proposed to assist in secure transactions. The approach is based on developing custom policies that will help health organizations in developing an effective strategy for exploiting the public and private internet-based networks to improve quality of care. At the same time this approach is designed to help preserve patient privacy, patient data confidentiality, and human safety.

The requirements for designing the policies for the implementation of a complete Public Key Infrastructure (PKI) system [9, 22, and 29] that would cover the health care sector of Cyprus are analysed, including potential risks. The first policy is the certificate policy (CP), which defines the set of rules for the operation and management practice of certification authorities (CAs) issuing qualified certificates. The second policy proposed is the certificate practice statement (CPS), which outlines the technical, procedural and personnel policies and practices of a particular CA. Both of them comply with the "Internet X.509 V3 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [5].

As a result of the adoption of the proposed policies the Hippocrates CA was implemented, the goal of which is the coverage of the Pancyprian health care sector. Hippocrates CA is still at an experimental stage however, and its first users will be the Bank of Cyprus Oncology Centre (BOCOC) and the Cyprus Association of Cancer Patients and Friends (PASYKAF).

# Chapter 1

## Introduction

### 1.0 Introduction

Today healthcare is among the most personal services rendered in our society [58], yet to deliver this care, a large number of personnel must have access to intimate patient information. Sharing this information improves the quality and efficiency not only of health care, research, and public health surveillance, but also in many cases, the patient's general outcome. Patients must however, be willing to reveal personal information. In return, the healthcare provider must guarantee that patient confidentiality is established and.

Maintaining confidentiality is becoming very difficult. Information systems' technology allows instant retrieval of medical information and a widening access to a greater number of people. This however has its risks, as the confidentiality of patient information may be compromised. There is a need to find a safe way of exchanging such confidential information without having unauthorized people viewing it. One of the most popular ways of accomplishing this is by implementing a public key infrastructure (PKI) [29].

The aim and contribution of this thesis is the investigation, design, and preparation of the policies needed for implementing a PKI system in the healthcare sector [10, 13]. These policies were designed by the author of this dissertation based on the standards and legislations given by the European Community Directives [10, 16] and several Request For Comments (RFCs) (RFC2459/2527/2510) [1, 2, 5] also analysing any potential risks for the health care sector. In addition to providing the opportunity of achieving trust between users, implementing the PKI system enables the exchanging of records among health care professionals. Communication security over public (Internet) and private networks can also be achieved. Such an infrastructure does not currently exist in Cyprus, not only because of the unwillingness of health care officials to exchange patient information among themselves but, also due to the lack of confidence these professionals have in such a system. This thesis proposes the policies which should be followed for a PKI system to be used for Cyprus's Health

Care system. This PKI is going to be designed in such a way that will make it easy to convince Health care professionals and other prospect users to trust the system since the transaction of patient information will be secure and the final outcome will most certainly be more beneficial to the patient. This is because of the fast, efficient and secure method of transmitting and exchanging patient information.

The Cyprus health care sector, including organizations, hospitals, and private doctors, do not use any electronic message system to convey patient information between them today. The use of email to exchange patient information, records, etc is a long way from being a common practice. Communication between different hospitals and doctors regarding the health of their patients is also far from becoming a common practice.

This thesis will present the policies written as a result of the implementation of the PKI system, which are needed both for (a) establishment of trust among those in a health care PKI system and (b) for ensuring that all users participating in such a system, show full confidence in it. All the people involved must adopt a new way of thinking for such a system to succeed. For example, health care professionals must understand that exchanging patient information may result in better healthcare given to the patient. Patients should also understand that the sharing of their information would not result in any harm to them.

The thesis also analyzes the risks associated with the adoption of such a system in the health care sector and presents the methods proposed for implementing a PKI in a health care organization. It is also intended to be read by health care administrators who are concerned with the security of patient information transmitted and received online by their organizations. It will provide all the policy guidelines and background information that is essential in any comprehensive PKI implementation, and finally, it will briefly describe the components of a functional PKI [37, 48] and the options available for obtaining or creating these components.

### 1.1 Objectives of the thesis

The undertaking and motivation of this thesis was (a) the need to achieve a safe and secure transmission of medical records among health care professionals and (b) the

need to guarantee communication security over public (Internet) and private networks, and thus maintain the patient confidence in the healthcare professional at the maximum. At the same time it aims to prevent or deter any access to unauthorized users, and discourage and detect any inappropriate use of health data. This security feature must be able to verify the identity of people and computers with authorized access on a timely basis in order to provide security management across the network and help improve authentication, data integrity [37], and privacy [9]. This thesis also intends on addressing both the organizational policy and technology needed to understand and manage security risks.

### 1.2 The need of PKI in the health care sector

Personal information contained in medical records is reviewed, not only by physicians and nurses, but also by professionals in many clinical and administrative support areas of health care organizations.

Healthcare executives must follow the laws governing release of information. While the healthcare organization owns the health record, the information in that record remains the patient's personal property. Releases cannot be made without proper authorization. Healthcare executives must determine whether patients, or their legal representatives, consented to the release of information. No exceptions to patient confidentiality are allowed and the rights of individual patients must be protected. Therefore privacy, confidentiality, and data integrity must be assured during the transmission of clinical information, to qualified recipients.

Although patient information, consultations, and medical prescriptions between doctors in remote locations, organizations or different hospitals could be done via the internet, unauthorized interception and tampering by intruders, exposes any exchange of information to potential risks. As a result, hospitals or health care organizations are often exposed to financial and legal liability. The development of a private PKI system is expected to protect the health care organization from such liabilities.

In general, health care organizations and health care professionals should be capable of knowing exactly who is accessing their data and who requests it. PKI technology offers these capabilities through strong authentication [29].

Health care technology is improving dramatically and costs a lot more, while at the same time most governments have to face increased spending for the treatment of an ageing population [58]. These challenges will be impossible to meet without the deployment [35] of a robust solution. A potential solution to this problem lies in PKI technology [13, 35], which provides authentication, non-repudiation, data integrity, confidentiality, easy usage, and controlled accessibility to information. This is a solution proven for protecting electronic messages transmitted over unsecured paths. PKI should therefore be considered "a must" for the proper authentication of users in exchanging messages among the health care industry. The importance of the PKI technology lies in its ability to manage secure, reliable and trustworthy key pairs. PKI satisfies all requirements for data confidentiality, user authentication, access control, data integrity, and support for non-repudiation [13].

Health care is a major business sector. PKI technology is posed to help hospitals deal with a double challenge: to improve the quality and accessibility of health care for all the citizens, whilst constraining overall costs [58].
PKI assists in making the above possible by providing a way of identifying and trusting another internet user[1], through the use of digital identification called digital certificate [29, 50]. Through its trust framework, it enables security across networks, by employing synchronous methods of remote user identification and establishing correct methods which replace, and possibly improve the written signature [30].

### 1.3 Overview

This thesis concentrates on methods that are needed to protect the confidentiality and integrity of electronic information over unsecured networks, as detailed in Chapter 2. The analysis of the risks [27, 28] that need to be taken into account prior to the implementation and the design of any policies is presented in Chapter 3. This thesis also addresses the complex legislations and standards that apply in the European Union. A section that contains these legislations and standards, as they apply to Cyprus's environment is included in Chapter 4. Chapter 5 discusses similar work done in other places of the world and explains the differences with the Hippocrates – PKI System. A review of the main policies that a CA requires in order to be operational, as well as significant differences from the proposed policies are provided

[1] A user can be a person, a computer, or some other electronic entity.

in Chapter 6. The complete set of all the proposed policies is included in Appendix A. The above mentioned chapters cover the plans, procedures, and technical measures that make such a system unique in the Cypriot health care sector. The Certificate Practice Statement (CPS) for the specific Certificate Authority (CA) running at the BOCOC is given as an example of the implementation of these policies in Chapter 7. Finally, Chapter 8 gives the conclusions and views for the particular technology trend.

# Chapter 2

## Introduction to PKI

### 2.0 Introduction

Nowadays the Internet is the preferable technology that companies and individuals use to complete thousands of online transactions [25, 58] or to exchange important information and data, i.e. patient data. For example two doctors discussing patient information over the Internet. However, security suffers, since the Internet does not have the inherent security controls in place to secure all traffic passing through it against unauthorized access because it was not designed with security in mind. Therefore, individuals and organizations that want to take advantage of their benefits, must also consider the steps necessary to secure their private transactions over a public or semi-public medium of transmission [25].

While Intranets and Extranets are becoming more widely deployed, new security challenges have emerged concerning the protection of organizations and individuals from unexpected visitors and interceptions to their networks, and also to protect their sensitive information from being misused or even stolen. Firewall systems, Intrusion detection systems and other access control technologies are today a must within an organization; however these technologies leave many security issues unstressed. The issues are authentication, data integrity and non-repudiation.

Establishing trust between people and companies is today the main issue for an organization that uses the Internet to do business. Organizations today are requested to do business with people they have never met before. The success of such business affects the complete organization image and the organization reputation. Public key infrastructure can help organizations build trust into their network systems and has the potential to make Internet transactions as secure as face-to-face transactions.

### 2.1 Internet Security Issues

Normal operation of systems in many cases is affected by unexpected conditions, so called threats [41], which need to be addressed in a comprehensive security approach prior to the adoption of any appropriate solution. To achieve that, a spherical knowledge on the dangers that threaten the normal operation of the systems is needed.

To start with, all communications over the Internet use the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP allows information to be sent from one computer to another through a variety of intermediate routers, computers and separate networks, before it reaches its destination. Thus a third party may alter any information sent when it interferes with communications in the following ways:

- **Unauthorized disclosure:** When patient information is transmitted between doctors', "in the clear," hackers can intercept the transmissions and obtain patients' sensitive information.
- **Unauthorized action:** A competitor or disgruntled customer can alter a Web site so that it refuses service to potential clients or cause malfunctions within the Web site. For example a Web Site that is being used to offer information to a patient may be altered, resulting in all of its services being declined to its visitors.
- **Eavesdropping:** The private content of a transaction, if unprotected, can be intercepted en route over the Internet. For example, someone could learn about a patient's situation, record a sensitive conversation, or intercept classified information.
- **Data alteration:** The content of a transaction cannot only be intercepted, but also altered en route, either maliciously or accidentally. User names, patient ID numbers, patient demographics, and patient treatments sent "in the clear" are all vulnerable to such alterations. For example, someone could alter a pharmacy order or change a doctor's prescription.

Other security threats or attacks that may affect the normal operation of a system are:

**Spoofing:** Is the kind of attack during which the perpetrator appears to be someone else either by using its IP or its address. Spoofing relies on trust relationships between machines within the trusted network. For example, in the health care sector a hacker can pretend to be the doctor that gives fake advices to patients. Another example of spoofing appears to be the creation of illegitimate sites, i.e. health care sites, which appear to be published by established organizations or hospitals.
**Smurf Attack:** In this attack, the attacker sends an IP ping (or "echo my message back to me") request to a receiving site. The packet specifies that it be broadcasted to

a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. The result will be lots of replies flooding back to the innocent, spoofed host.

**Denial of Service Attacks:** Is the disruption of service and the loss of availability. On the Internet, a denial of service (DoS) attack is an incident during which a user or organization is deprived of the services of a resource they would normally expect to have. Such attacks are designed to bring down services and machines and do not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money. Health care services are critical for the patient health and patient confidentiality; as a result such disruptions may have impact not only to the normal operation of the health care sector but may also lead to the loss of patient trust.

**Viruses:** Nowadays, one of the biggest threat that computer users face, are viruses. A virus is a program that usually propagates to the computer via the Internet, email (as an attachment), downloads, or via contaminated files that are contained on infected floppy discs or CD's. As some of the viruses can enable the email sending procedure automatically it will be very degrading for the health care professional to appear to have sent an email to one of his/her patients propagating a virus or even sending meaningless emails. Viruses can also cause data corruption as well as accessing passwords or other patient information.

**Syn Attack:** This attack is initiated during the initiation of Transport Control Program (TCP) between a client and a server in a network. During this communication, an attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This results in an unauthorized increase of traffic and a delayed response to different services. For example if the pharmacists tries to access a prescription, the increased amount of traffic will cause a delay in the viewing of the prescription.

### 2.2 Definition of Public Key Infrastructure

Public Key infrastructure (PKI) [29] is the technology that builds trust over unsecured public networks. With PKI, users can securely and privately exchange data, i.e. a

health care provider sends personal health information (e.g. a hematology test result) to another health care provider securely, in the knowledge that only the intended recipient will be able to read the information, or can even proceed to an exchange of money in return for service provided. PKI enables these by providing a way of identifying and trusting another Internet user, through the use of digital identification called digital certificate [29, 50]. This digital certificate is like a driver's license or a passport. It contains the Internet user's name and some other credentials[2].

A digital certificate can also be used to verify a digital signature, which can be attached to e-mail messages or other types of electronic messages. This signature is created using Public Key Cryptography [22].

### 2.2.1 Public Key Cryptography

PKIs are built upon a security solution called Public Key Cryptography. In Public Key Cryptography [22] with the aid of a mathematical algorithm and the use of the public and private keys, the information or the value is transformed in a form that is unreadable for all entities other than the sender or receiver, i.e. encrypted, and can only be converted back to its original format, i.e. decrypted, with the use of a complementary mathematical algorithm and an allied value. In Public Key Cryptography [22] public and private keys perform a one-way transformation on the data. Each key is the inverse function of the other i.e. while one encrypts the other decrypts the message.

With Public Key Cryptography, a doctor can send a private message to a colleague or to a patient by scrambling the message with the intended recipient's Public Key [22, 48]. A Public Key is made publicly available by its owner, while the Private Key is kept secret. Recipients can then decode the message with the recipient's Public Key. Private Keys are stored on a computer's hard disk or on a special cryptographic device called token. In the case that it is stored on a token it can only be used while the token is inserted in the computer.

Public Keys [22, 48] are usually embedded within a digital certificate [50]. Digital certificates are easy to distribute, either via a web site (through the browser) or as an

[2] Content of digital certificates depends on the organizational policies and private issues.

email attachment. Embedding the Public key in the digital certificate gives an identity to the digital certificate, much like the giving of a driving license or a government ID to a person. In other words, the identified entity is strongly associated with the assigned Public Key.

### 2.2.2 Digital Signatures:

Digital signatures [36] are one of the primary ways Public Key Cryptography [22] can be used to make Internet communications safer. It can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. It is easily transportable, cannot be imitated by someone else, and can be automatically time-stamped.

In the health care sector where many times doctors have been accused by patients of mistreatment or wrong prescriptions digital signatures can be used to provide the assurance that any message, for example a message that includes a medical prescription, has not been changed and that the sender is who he claims to be. This will therefore eliminate the chances that an "intruder" posing as the patient's doctor will send a message to a patient concerning treatment or medication leading to mistreatment of the patient. Digital Signatures can authenticate the identity of the health care professional and have the ability to ensure that the originally signed message sent by the health care professional cannot easily be repudiated at a later stage. Digital signatures are part of the digital certificate that is issued by an authority, which belongs to the PKI system. Figure 1 and figure 2 show the complete procedure for encrypting and decrypting a message using the digital signature.

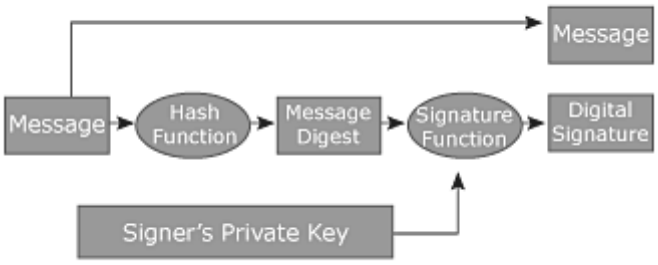


**Figure 1: Creating a Digital Signature for a Message**

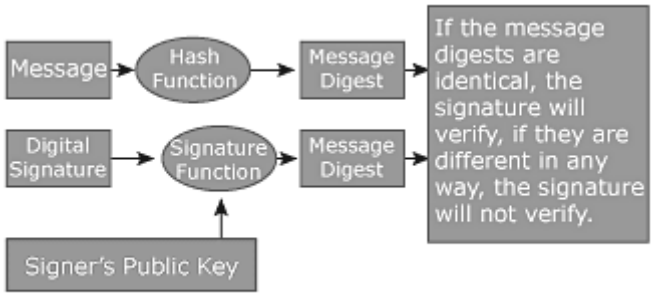


**Figure 2: Decrypting the Original Message**

### 2.3 Health Care PKI System Addressing Issues:

PKI is a trust framework that enables security across networks. It's purpose is to provide synchronous methods of a remote user identification and to establish the correct methods, which imitate- and possibly improve- the written signature. Such a framework can be extended to include every person, computer and electronic entity in an organization or company. However, there are six major services that must be provided for a Health Care PKI system to be functional [36]. These are authentication, non-reputation, data integrity, confidential communication, ease of use, and access control. These services make the PKI a candidate solution to provide the required level of security and protection.

#### 2.3.1 The Full Range of Services Are:

- **Authentication**. A guarantee that a message contents really has come from the person who claims to have sent it. This avoids any disputes among the users i.e. doctors – patients, or doctors – doctors.
- **Non-repudiation**. The certainty of knowing that the sender of the message cannot later deny having sent it. Digital signatures can be used to establish the non-reputation of transactions
- **Data Integrity**. Proof that the message contents have not been altered deliberately or accidentally, during transmission and storage. There has always been a demand for integrity when two or more remote parties need to rely on a given quantity of information. Data integrity is assured using public key cryptography. It is important to achieve data integrity when it has to do with

patients' treatments, pharmacy orders, or doctors' prescriptions given to patients.

- **Confidential Communication**. Only the intended recipient is able to read the file or message.
- **Ease of use**: End users should be able to quickly and confidentially access private information resources via the Internet without worrying about the underlying technology. Health care professionals but more specifically patients should be able to easily use any system that will be created for exchanging information.
- **Access Control**: Access to sensitive information is controlled through the use of authenticated identities. For example in the health care sector doctors are expected to have access to more information compared to nurses.

### 2.4 The Components of a PKI System

To implement all the above-mentioned services there is a need for an infrastructure [37, 48]. A general PKI system is mainly consisted of a certificate authority that accepts user requests for a certificate and at the same time acts as the authority, which issues and manages security credentials and Public Keys [22, 48] for message encryption. The PKI-Enabled applications can also be considered as part of a general PKI system. These PKI-Enabled applications are provided by the PKI system in order to supply the above-mentioned services. Another part of the general PKI system is the End-users, who vary in status, depending on the type of system application. These are the characteristics of a general PKI system. The organization of the components of any specific PKI system may vary, again depending on the application of the system. For example, many PKI systems [43] separate the operations performed by the Certificate Authority (CA) and the Registration Authority (RA) to avoid the complexity of tasks, which are already performed by the CA. This is also necessary if the organization wants to separate the certificate request process from the certificate issuing process.

The advantages of using RAs are:

- Separation of the two authorities minimizes the risks and security constrains that would apply if the CA is also responsible for user registration as a web server.

- With RAs, organizations can set up local or stand-alone enrollment centers at distributed geographic locations. Employees of an international company can be enrolled into PKI via RA centers of the country they are living in and digital certificates will be issued to those employees from the company's CA, which is located in the company's country.
- Requests for digital certificates are sent to the RA instead of the CA, relieving CA administrators of the task of vetting certificate requests.
- Users accessing RA can also configure to access the Certification Revocation List (CRL) database.

### 2.4.1 Certification Authority (CA)

A certificate authority is a trusted authority in a network that issues and manages security credentials and Public Keys [22, 48] for message encryption [9]. As part of a PKI, a CA checks with a registration authority to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a digital certificate. The CA is also responsible for the distributing and revoking of the certificate.

Depending on the PKI implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name and other information about the public key owner [34].

A CA is like a licensing authority. Digital certificates are only issued to users who can prove their identity and credentials to the CA. By using a process called vetting, the CA examines traditional forms of identification before issuing a certificate.

CA's also respond to queries about the validity of certificates they have issued. A validity period of the certificate, specifying how long the CA expects the certificate's contents to remain valid, is also included. A certificate may become unexpectedly invalid if information about the certificate subject changes. On the other hand, a certificate is valid, if it has not expired [34] and the information in the certificate is true. It may be important for a CA to be physically located in the same geographic area as the people it is issuing certificates to.

### 2.4.2 Registration Authorities (RA)

A registration authority is an authority in a network that verifies user requests for digital certificates and tells the CA to issue them. RAs are also used to enroll new users into the PKI. The Certificate renewal request for certificates, which have expired or need updating, are also be done through the RA. Via the RA, users or prospect users have access to a variety of information that concerns the PKI application and the status of a certificate i.e. request or renewal certificate status. Another use of the RA is that it provides these users with the possibility of finding answers to any frequently asked questions. The RA can also be used, as a means of requesting the destruction of a certificate, i.e. to destroy certificates that are no longer needed. It can be used for requesting the revocation of a certificate if suspicions exist that somebody else is using the certificate. Finally the RA can be used for key recovery if the key was lost due to hard disk failure. This can be done, by recovering the lost key from the authority's database.

### 2.4.3 PKI-Enabled Applications

Without the ability to integrate the PKI with applications (making the applications PKI-enabled), the PKI has a limited value in business. Fortunately, PKI systems can be supported through a variety of off-the shelf software programs, which allow the PKI solution to meet demands, as the application environment and requirements evolve over time. Such applications/programs are:

- Web browsers
- E-mail clients
- Virtual Private Network (VPN) software and hardware [36]

Today's most widely used Web-browsers, Netscape Navigator and Microsoft Explorer, are already PKI-enabled, and can provide users with the ability to generate a key pair and download a digital certificate. Popular e-mail programs such as Microsoft Outlook and Netscape Messenger are also PKI-enabled. Users instruct their email program to digitally sign a message simply by clicking a button.

As was mentioned before, nowadays companies use extranets for their transactions. To extend the PKI beyond the firewall many companies PKI-enable their extranet or

create a virtual private network (VPN) [36]. Extranets and VPNs use digital certificates to authenticate users and provide access control.

### 2.4.4 The End-users

The end-users are typically the people that are using the system for example in healthcare the end-users are doctors, medical assistants, nurses etc. End-users are the key element of the system since application, policies, and practices are built up for them. The end-user using the PKI system can establish electronic transactions over a secure network. Transactions could be in any form, such as email, e-banking [25], or e-shopping, that of course, depends on the structure of the application. In general, the end-user may request certificates from a CA, receive the certificate from the CA, use the certified keys and certificates in PKI enabled application services, thus enabling support for strong authentication, encryption and non-repudiation and may search the certificate repository for certificates and status information.

## 2.5 Central processes in a PKI

The PKI's applications main tasks are to accept new user registration, to verify and authenticate the users, to issue the certificate through the CA and finally to apply the service provided to the users, in the way that these are stated in the policies of the system. The first two processes are done most of the times via the RA. In many cases, and depending on the domain of the system, these processes can vary in how their applicability is enforced and not in their general meaning. For example in Health Care, which is the main concern of this thesis, to ensure the effectiveness of a PKI system these processes must be applied in a way that guarantees trust among the users and the safety of any transactions done.

This is also true for E-commerce PKI systems where trust must be present in order for these to be used. However in E-commerce any mistake occurring can be redeemed, whereas for Health Care the damage caused may not easily be undone.

### 2.5.1 Issuing certificates

A certificate can be issued to end users and end entities in accordance with the CA policies, and not before the validation of the given information, since the CA will sign

this information with its public key. By issuing an X.509 [29] certificate to the user or an entity, the CA also binds its private key. A certificate is typically issued for a certain period of time, which depends on the CA policies (Chapter 6 & Appendix A) and the purpose of the certificate. It is usual to provide certificates with different extensions that define the purpose of the certificate, such as authentication, confidentiality and non-repudiation. For the Health care PKI system, the issuing of a certificate can only be done in accordance with the policies that the system follows. Certificates are issued only to those that are eligible for such a certificate.

### 2.5.2 Revoking certificates

This process normally takes place after the party owning the private key directs the CA to revoke the certificate. Specific conditions for certificate revocation are specified in the Certificate Practice Statement (CPS) (Chapter 7). Such conditions may be:

- The loss or exposure of the private key of an end-user or end entity
- The suspicion of exposure of the private key
- The change of basic information of the certificate by a user or entity, leading to the requirement of a new certificate.

Revoked certificates are placed on a list signed by the CA. This list is called a CRL [32, 33]. In accordance to the Certificate Policy (CP), the CRL will be available to all users.

### 2.5.3 Authentication / Verification

Authentication is the process of confirming an identity and creating trust in the digital world. Authentication involves the confident identification of one party by another party, prior to doing business or sharing sensitive information. In the real world, human authentication relies on physical credentials such as a driving license, government ID, etc. to prove if someone is who she/he says they are. In the digital world, this should be imitated so that prior to any transactions, the correct authentication will take place. In other words, authentication in the digital world is the service that assures one party that the credentials of the second party have been validated by a trusted third party.

Proper authentication allows the authentication of the two parties involved. Thus the end-entity verifies the client authentication and the client (end-user) verifies the server. This process basically implies a means of verification, since it ensures that the certificate information is still valid, as this can change over time. In a PKI system, authentication and verification may be assumed as one procedure, during which one starts with the initialization of the other. Authentication, however, is achieved only when both sides trust the public key corresponding to the private key used by the CA when it issued the certificates.

For the health care authentication and verification is a crucial process because of the confidentiality of the information and in many cases the human lives. Doctors should be able to identify that the person requesting information for a specific patient is a legitimate user of the system and has the right to know. Also, in the case of a medical prescription, health care professional should be able to identify that the requestor is the real patient.

### 2.5.4 Non-repudiation / Verification

Non-repudiation is the method used to ensure that a transferred message has been sent by the sender site and has been received by the second party, who claims to be the receiver. Non-repudiation guarantees the transaction with both sides (sender / receiver). Both sides cannot deny having sent the message or having received the message. Non-repudiation can be obtained through the use of certificates, which come about from the use of a digital signature. The digital signature is created, by encrypting given data with the private key specified for non-repudiation, and creating a hash or a message digest [6, 7, 8, 36]. The verifying party using the certified public key will decrypt the message to the expected values. This procedure, as with authentication, ensures non-repudiation at the time of action, since the receiving party should be able to check for certificate validity and revocation status.

## 2.6 PKI Process Flow:

The following is the graphical representation of the PKI process flow

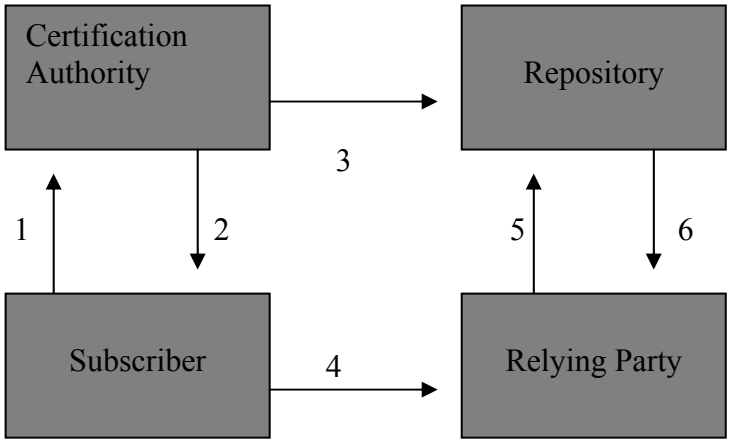


**Figure 3: Graphical Representation of the PKI Flow**

- Step 1: The Subscriber applies to the Registration Authority for a Digital Certificate i.e. a private[3] Health Care professional decides that she/he wants to electronically exchange patient information with other private Health care professionals or clinic. A contact with the Registration Authority as per the policies (proposed certificate policy), should be made. For example as per the policies the user can access the RA web server and apply for a certificate online. When needed she/he must supply the RA with all information in order to proof hers/his identification.
- Step 2: The RA and CA verify the identity of the Subscriber and issue a Digital Certificate. The RA verifies the identity of the applicant according to the policies (certificate policy). If the applicant is who she/he implies to be then the RA will send the application information to the CA. The CA issues the certificate according to the group the user belongs to, as these are defined in the certificate policy. For example, to confirm that the certificate request originated from a Licensed healthcare persons, the RA must contact the Ministry of Health and the National Medical Committee to verify the proficiency license of the Subscriber. The CA expects the user to accept the certificate.

[3] Private means a practitioner who has his own practice

- Step 3: The CA publishes the Certificate to the Repository. The Repository can either be in the RA or in an independent Web Server. An obligation of the CA in accordance with the CA policy is to inform users of the certificate status. It is also obliged to state which users have certificates. The time limits that a CA applies to the updating of the repository are stated in the CP. This tends to be updated every 24 hours.
- Step 4: The Subscriber digitally signs the electronic message with the Private Key to ensure Sender Authenticity, Message Integrity and Non-Repudiation and sends it to the Relying Party [46], i.e. if the above points are followed and the Health Care professional has his own certificate then a signed message may be sent by this Health care professional to another user.
- Step 5: The Relying Party receives the message, verifies the Digital Signature with the Subscriber's Public Key, and goes to the Repository to check the status and validity of the Subscriber's Certificate. For example the receiver of a message (second health care professional) can open the message using the public key of the subscriber (if the subscriber is known and possesses a public key). To find out whom the subscriber is and if she/he has a public key the receiver can go to the repository to check the status as stated before.
- Step 6: The Repository returns the resulting status check on the Subscriber's Certificate to the Relying Party. The repository is just a simple query on the web server which all users can access. This may be part of the RA, which is backed by a database that contains the status of the certificates.

### 2.7 Considerations and approaches for the Design of a PKI System

Nowadays, many approaches for the design of PKI systems have been introduced by vendors. However, many vendors are only considering the financial benefit [27] that such solutions may provide their companies, and not the usability and the applicability of the system and the application in general. They are promising the delivery of an unmatched level of security and reliability to Internet and telecommunications customers around the world, for secure online transactions with reliable authentication and encryption through their well-designed specialized applications. Through strategic considerations they implement applications to cover the needs of big enterprises, small and medium businesses, a personal home or office. Planning for

the maximum share market margin, they even proceeded with the division of the market into different sectors, i.e. hospital, bank, etc., and developed applications for those specific sectors.

Despite all this, their applications suffer from interoperability [2], considering specific organizational or departmental needs that may apply. They are also costly, considering the amount of available freeware software, such as Open SSL. The lack of policy deployment in general is another disadvantage, since the local CA policy, such as certificate content rules and administration authorizations, is hard to be established.

Other drawbacks that these ready made applications may have are:

- The minimal control that can be applied from the organization using the PKI system for the certificate management functions, such as certificate issuance approval (based on RA approval), revocation approval, and general administration functions.
- The failure to support the Certificate issuance, certificate life-cycle compliance and protocol support, cryptographic key management, secure records retention, data based mirroring for disaster recovery purposes, and other core functions.

The second kind of PKI system is the Standalone PKI. When implementing a Standalone PKI system, enterprises assume 100% of the risk by providing 100% of the security infrastructure, operational risk, service infrastructure, and a disaster recovery. In other words, with this system 100% of the responsibility is assumed, by the enterprise / health care organization, for all the surrounding technology, including systems, telecommunications and databases.

### 2.8 Choosing the right solution

Implementing the right PKI solution depends on many factors [31]. For example, the application domain of the system, i.e. E-health [13] or E-commerce, and the capital needed. In this section, a basic description of the general challenges is presented. These should be noted prior to any decision taken for the implementation of a PKI solution, and a specific solution for the application domain should be selected.

### 2.8.1 Scalability

By scalability it is meant that the PKI will address the following issues:

- The PKI's services should extend, not only throughout an organization, but also beyond it, in order to provide the appropriate level of security for all of the organization's internal users, as well as for any external entities that the organization deals with.
- The PKI should operate efficiently and effectively with all the organization's users, i.e with all users of a Health Care PKI system.

### 2.8.2 Usability

A PKI must be easy to use. No one will use a PKI if the enrollment process is complicated or if it is difficult to use. It should be integrated seamlessly into an organization's existing network system and software programs and should require little or no special training to use.

A PKI must also be easy to manage. The administrative interface for the CA or RA should be an intuitive graphical user interface, which can be used to process high volumes of certificates and certificate requests. The interface should also be flexible and customizable.

Implementing a PKI solution should be as easy as possible. The everyday use of the PKI should be intuitive and should not require special training. A system administrator should be able to easily install the PKI software and quickly configure an organization's network systems to use a PKI.

### 2.8.3 Service Provided and Technical Expertise

Due to the high importance of the PKI system for the reliability of Internet and telecommunications' applications, adequate service should be provided by the company that has installed the application. Service should be guaranteed 24 hours a day, seven days a week. Provisions for the minimal downtime should be taken by the organization that applies the PKI system. Such provisions should be clearly stated in a service agreement contract. Organizations that will implement stand alone applications should guarantee the training of its personnel and should also ensure that

the experts and those most knowledgeable, as far as the systems are concerned, do not leave the organization. For that reason, the organization should sign a contract with the personnel. In the contract, the specific job description, along with the employer benefits and any penalty clauses the employees might fall into, should be stated.

### 2.8.4 Cost of such a System

The cost of such an implementation is high due to the high expectations that are addressed, i.e. security, trust, authentication, etc. This cost is also dependent on the domain of the application; for example, in the health care sector the implementation of such a system may be much more costly due to the extra security features that may be needed.

## 2.9 The need and complexity of PKI for the Health Care Sector

The decision for choosing the right PKI solution for the health care does not depend only on the amount of money that can be spent, but also the service provided, and the expertise that may be available within the area that the PKI solution was built on.

The Health Care sector is considered among the most crucial sectors in the market. The right design for a Health Care PKI system is essential not only because many times it is related to human lives, but also because of the economic consequences a mistake may have. For Health Care PKI systems some particularities should be taken into account. Some of these particularities are patient data, which must be kept confidential as well as doctors' prescriptions to patients, which should not be altered. The fact that many times a patient's health depends on a doctor's advice or on a decision that was taken after the collaboration of two or more doctors is also a particularity that should be taken into account when designing a Health Care PKI system. Another particularity that needs to be looked at is the guaranteeing of trust among the users.

All these factors make the design of Health Care PKI applications demanding compared to other PKI applications, i.e. E-Commerce. For example, for an E-Commerce application [28] that lacks application design, if any mistake occurs the result will be some money loss either for the company or for the customer, which may be covered later by an insurance company. Conversely, for Health care PKI

applications this is not the case, and if any error occurs, it may result in a loss of a life that cannot be redeemed by any insurance company. If for example a patient requiring a prescription for hypertension receives the wrong prescription this could lead to the patient suffering a stroke, as a consequence of which permanent neural damage or even death may occur.0 Such consequences would not be present in an incorrectly designed E-commerce PKI system and any damage caused is redeemable. How crucial the design of Health Care PKI systems and in general all E-Health applications is, compared to other industry sectors, becomes apparent when failures, not only in electronic transactions, occur. These might be power failure, fire or flooding, failure of the hardware, failure of the software, failure of the web site. The outcome of such failures would be the distrust of the system, user unfriendliness, delay in performing a service e.g. doctors trying to give timely (could be life threatening) advice or a treatment prescription to a patient.

Prior to the implementation of Health Care PKI systems, policies that govern user access privileges, administrative duties, system maintenance should be well defined within a framework of legal and social responsibilities, which must be addressed through the Certificate Policy (CP) and the Certificate Practice Statement (CPS). These policies determine the operational and technical practices of a PKI and provide clear guidelines for operating the PKI. They also provide guidance for all aspects of implementation i.e. obligations of the authorities, obligations of the users, the role of the different members of the system, the agreements, the restrictions that users may have, the financial responsibilities, the secure access to electronic records as well as the training and monitoring of employees to ensure that they follow the established security protocols.

Consequently, all these give an extra complexity to the system which makes its implementation hard and at the same time it explains why it is not yet a popular solution for the secure transaction of electronic messaging among the health care community.

## 2.10 PKI Security Policies

As was stated above, certain policies and standards, which determine the operational and technical practices of a PKI in the community, should be addressed prior to any implementation; these are the Certificate Policy and the Certificate Practice Statement

The Internet Engineering Task Force (IETF), in one of its informational publication (RFC 2527) [5], clarifies clearly the relation between Certificate Policy, Certification Practice Statements, and interoperability. Through a well-defined Certificate Policy and by employing a product that can support it, interoperation between PKI domains may be possible without causing serious downtime or interrupting workflow. According to IETF a CP states what assurance can be placed in a certificate. A CPS states how a CA establishes that assurance. A certificate policy may apply to a broader scope and not just a single organization; a CPS applies only to a single CA. A CP for the health care community should be developed to cover only the users and the aspects of the health care sector. In accordance the CPS of a specific health care organization that implements a PKI system, should be developed to specify any diversions of that PKI System from the given CP, and to clarify any standards the specific health care organization- PKI System should follow, e.g. the procedure used by the CA to revoke certificates.

**Certification Policy (CP):** According to The Internet Engineering Task Force (IETF), a certificate policy is 'a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. A certificate policy may be used by a certificate user to help in deciding whether a certificate and the binding therein, are sufficiently trustworthy for a particular application. A CP explains the conditions and limitations of use for a digital certificate. The IETF states also that the more detailed description of the practices followed by the Certification Authority (CA) in issuing and otherwise managing certificates, may be contained in a certification practice statement (CPS) published by or referenced by the CA. It can be embedded in or referenced in a digital certificate.

Basically, certificate policies best serve as the medium via which the most common standards, industrial, governmental, and organizational assurance criteria apply. In

other words, within the CP, all globally acceptable criteria are available. It defines the policies for standards and interfaces that the PKI system is using. A CP statement is provided to users via an online documentation or in a writing format. A CP is not an isolated or steady document, but is a document, that over time, tends to evolve and encompass more security issues and other risks that may arise in the future.

**Certification Practice Statement (CPS):** One of the issues in implementing a PKI for a specific CA is to create unique policies, for that CA, and to document that these can only apply for this implementation and for the people that will be the users of the specific implementation. This is called a Certification Practice Statement.
The CPS for an organization may also be referred to as an Organization Policy Model. For the creation of an Organization Policy Model the involvement of administrative people, the heads of the organization, who will be the leaders of the CA and the application, computer administrators and in some cases attorneys, is required. All decisions should then be approved by the organization's legal department. Indeed, this process is expensive and time-consuming but is needed not only to protect the CA, but also the users of the CA.

A CPS is a legal document, created and published by a CA. The CPS explains the CA's certificate issuance and revocation policies. The CPS must clearly state all the legal responsibility of all the prospective users of that CA and all variations of the policy, depending on security and policy requirements of particular situations. It defines the level of trust that the user is showing to the CA and may be associated with the PKI.

CPS as a policy document states the multiple groups of CA users along with the level of the privilege given within the CA. This will permit applications to make programmatic decisions about appropriate use of the certificate. For example, a PKI enabled application can look at an external researcher's certificate, and see that there is an approved non-disclosure agreement on file, and that the holder is a licensed physician. The application can then grant access to clinical research information that would otherwise be confidential.

A CPS finally governs how the PKI participants create, administer, use, and access keys and certificates. The CPS may also cover items like the enrollment process for

users and administrators, the CA's overall operating policy, procedures, and security controls; for example, in protecting their private key. All prospective users must accept all the CPS policies in order to be allowed to use the certificates issued by the CA.

### 2.11 Summary and Conclusions:

In today's computing environment, where the power of the Internet has opened the doors to a whole new realm of e-health, the need for a "solution" for an open and interoperable distributed network security is a must. Over the years a number of solutions have been considered as ideal, but none appear as ready to address the needs of security as Public Key Infrastructure today [45].

PKI today can be implemented to provide services in areas where electronic privacy is sought after with the use of encryption. Such areas may be the transfer of sensitive patient files over a network, the payment of services that were provided by a health care professional, the encryption of E-mails and the sending of messages across the internet. Implementation of a PKI solution is offered today by many vendors. However, many vendors are only considering the financial benefit that such solutions may provide their companies, and not the usability and the applicability of the system and the application in general [27].

Implementing the right PKI solution depends on many factors. For example, the application domain of the system, i.e. E-health or E-commerce or the capital needed. The Health Care sector is considered among the most crucial sectors in the market compared to other PKI applications, i.e. E-Commerce [28]. Patient information criticality and the provision of trust among the users are considered as some of the particularities that should be addressed prior to the implementation of Health Care PKI systems. For that reason, policies that govern user access privileges, administrative duties, and system maintenance should be well defined within a framework of legal and social responsibilities addressed, known as the CP.

# Chapter 3

## Risk Analysis in Health Care PKI Implementation

### 3.0 Introduction

PKI is considered by many as a standard set of flexible services. Certificates provide an attractive business model. Once the system is implemented, they cost almost nothing to make, and if all computer or internet users are convinced to purchase and use a certificate, this will assure the company issuing the certificates, a good income. The same of course applies, if somebody is convinced to purchase a private CA, and pay a fee for every certificate issued. However, the extra complexity of the system as was stated earlier, is considered the main reason for the unpopularity of such a system in the health care sector. Conversely, the complexity of the system is not the only reason responsible for this sentiment; this part of the thesis will focus on other issues that have caused the PKI system to have often come under strong attack and criticism. When such criticisms take place in the health care sector their only result is to discourage organizations from implementing such a system and users from using it. Such, criticisms revolve around trust, key distribution and ownership, key management and storage, as well as pretty basic, unanswered questions such as, what good are certificates anyway? Are they secure? What are they used for? [27, 31]

### 3.1 Risk #1: "What is trust, and who is consider as a trusted person?"

In cryptographic literature trust is defined as "that which you cannot confirm but must assume". However, when a CA is defined as trusted, it basically means that it handles its own private keys well, but this does not imply that it is necessary to trust a certificate from that CA for any particular purpose, i.e. exchange patient information or even proceed with payments for the service provided by the health care professional. But, who gave the authorization for the CA to be called "trusted"?

A CA can do a superb job, in writing a detailed Certificate Policy and a Certificate Practice Statement, as well as in applying these policies. This, however, does not mean that it can be trusted to be used for any specific application. The reason for this is that CAs many times does not query the users' authority for the usage of the particular certificate or the correct usage of it. In spite of this, they issue certificates no matter the risk, because of the financial benefit to their companies. To avoid these

issues, Health care PKI systems should operate at any given time with professionalism and should follow high standards when its time to authenticate users and issue certificates. In accordance should follow a specific way, known to the users, to query the actions of the users among the community.

### 3.2 Risk #2: "Who is using my key?"

Management of a personal private key is considered as one of the biggest risks that PKI users face [27]. Certainly storage of their private key in a desktop computer at home or at work is subject to dangers, such as viruses, malicious program attacks, theft attacks, network users' attacks, or even by people who try to guess the key. The same risks are posed to the private key, even if the owner of the key owns a secure computing system, with physical access controls, shielding, network security, and other protections such as video monitoring of the computer room. Security weaknesses also show up with the use of Smart cards, which some CAs brought into their security policies, as a method of securing the private keys of their users. Even with smart cards, however, critics question whether the card is resistant to any kind of attack and whether it can be easily stolen.

In countries where E-commerce is becoming a part of every day life, the CAs propagate terms such as "non – repudiation" and "trusted", in their advertising campaign. They try to promote similarities between the illegal use of private signing keys and credit card fraud. For example, under mail-order or telephone order rules, if an item on the credit card bill has been found and has not be bought, the card owner has the right to repudiate it by saying that he didn't buy that item. The merchant will then be required to prove that the item was bought. In spite of all the above, this is not always the case for private keys, and the users are exclusively responsible for whatever their private key is used to do, if this has been certified by an approved CA.

To avoid all the above-mentioned for the Health Care PKI system, the CA, in accordance with its policy, must establish a technique to inform its users of the correct use of their private key and its security. The CA must also specify the legal aspects to the legitimate users in case of any private key misuse, in accordance always with the locally applied Laws. For example a suggested technique is to publish and distribute a bulletin of how to use their Private Keys.

### 3.3 Risk #3: "How secure is the verifying computer?"

Another big issue the PKI system has to face is the security of the verifying computer i.e. the one that uses the certificate. Indeed, an attacker can manipulate a certificate by adding his own pubic key to the list of the "root" public keys that a Certificate verification system uses, and issue his own certificates, which will be treated exactly like the legitimate certificates. As a result, such a certificate is self-signed and offers no increased security. For a Health Care PKI system, the only answer to this is to build a PKI system that uses a secure verification system. Such security can only be provided if the verification of certificates can be done on a system that is invulnerable to penetration by hostile codes or to physical tampering.

### 3.4 Risk #4: "Identification of the user."

Certificates generally associate a public key with a name, but unfortunately these create more problems to the system. For example, a CA may have members with identical last names. Imagine that a user receives an email from a colleague called Andreas Andreou. The user may only know one person with this name and last name, but the CA may have several members with this identification. The user at his own risk may open that email and may see that it is an email from his friend, but the opposite scenario is also possible. In such a case the sender of the email can cause serious harm to that user. Prior to the design of the Health Care PKI system the implementation team must think carefully about this issue. They must build a system in such a way, so as to prevent users from blindly accepting a certificate. That system should be able to find out if the particular user certificate received belongs to a colleague? Certificate information could be extended so that is contains information which is unique for each user, in order to avoid such occurances .

A possible solution to this classical PKI problem for a Health Care PKI system could be a directory that keeps track of all the individuals. In that directory a user can pull down all the information needed on whoever he requires to send things to. However, there is a downside to this approach. Whoever is running the Directory needs to be up to date and has to be very careful that what they publish is absolutely right, but at the same time ensure that they do not publish to the outside world more than they want to declare about the organization.

### 3.5 Risk #5: "Is the CA an authority?"

In a PKI system the CA is the legitimate authority that issues certificates. However, for the CA to have such permission, it must be officially registered to any organization that is legitimate for inspection and is able to ensure compliance of the CA with the country's laws at any given time. Only then, the CA can be granted a business license and be able to certify the contents of its certificates and its actions. However, most of the listed CAs are not registered, and since this is the case, the question "what harm is done if an uncertified server were allowed to use encryption?" is often asked. This issue needs to be addressed with care, especially when on many occasions attackers of the PKI system take advantage of and criticize the application and the system. Prior to the initiation of the operation of a Health Care PKI system, external auditors, who are experts in the field, should audit the system along with the policies and procedures. An official government accreditation needs to be given to such a system to verify that it is eligible to operate and act as a Health Care PKI system. As this PKI system is not officially up and running the above has not yet been done. However, contacts have been made and the CP was sent to the European Standards Organization as well as the Information Communication Technology Standards Board for comments.

### 3.6 Risk #6: "Is the user part of the security design?"

At every stage of the implementation design the user should be taken account of. The design team should consider that the users, i.e. elderly patients, many times are not computer literate and should provide different types of assistance so that they can make the use of the system easier and user-friendly. Users cannot, and should not be expected to know, how to operate the system and the risks in doing so. The system should provide an adequate source of information either on line or during the acceptance of the users' registrations.

### 3.7 Risk #7: "Was it one CA or a CA plus a Registration Authority?"

In some PKI system implementations, more specific to the stand-alone implementations, there are two parts of a certification structure: the Registration Authority (RA) part, which is in secure communication with the Certification authority (CA) part. For such systems the security holes are greater and are

considered less secure than systems that run only one of the authorities and have the other run independently by an outside source.

If this is the case, the users should be informed prior to their registrations. Users must know what the available security features are for such a system so that the system could prevent any key misuse or any other type of harm. The CA should sign a contract with the users, which states all these features and clarifies to the users their responsibilities.

For Health Care implementation models, the CA should work independently and must be isolated from the entire network. It should be protected in a secure and monitored environment. If this is the case, it is recommended that this be stated and identified in the CP of the CA, which the users should be able to read, prior to their registration.

### 3.8 Risk #8: "How did the CA identify the certificate holder?"

Subsequent to the user registration, the CA should establish mechanism for the accurate and correct identification of the users and their information. All mechanisms should be mentioned in the CP and should be able to act fast for the best service of the user. In some PKI systems, however, this is not the case. CA authorities looking forward to the financial benefit of their system could register any kind of user without even a certain type of identification or verification of the identification. Use of the Health care PKI system should be allowed only to groups and users as specified by the CP.

### 3.9 Risk #9: "How secure are the certificate practices?"

Health care PKI prospect and former users should understand that Certificates do not secure their systems; they are just an approach followed in order to achieve a secure transaction over a network, i.e. Internet. Certificate holders must use their certificates properly if they want to assure security over their transactions, i.e. pharmacy orders. Prospect users should check the PKI practice policies and standards and confirm their suitability with its expectations. They should also check if the Certificate Revocation Lists (CRLs) are built into some certificate standards and how the revocation is handled. They should check the length of the generated public keys and be able to find answers as to why that length has been chosen. For example they should check if

the vendor supports 512-bit RSA [9] keys just because they're fast or 2048-bit keys because someone over there in the corner said he thought it was secure? Moreover, they should confirm, if for the proper use of these certificates any user action is required. In that case, policies should state the duration of the training needed for the users to be able to perform these actions. Finally policies should also indicate the key lifetime and the probabilities of key loss.

Unfortunately, not all the available PKI applications for the health care sector implement their practices and policies according to their needs and expectations. As a result, such systems do not provide solid security for their applications and do not consider the needs of their users. The system lacks interoperability and is inconsistent with its primary role. For example, many times such systems do not always specify the key lifetime, which depends on the application of the key, and key loss may not even be considered. However, a key has a cryptographic lifetime. It also has a theft lifetime, i.e. the time the key will be valid after it has been reported stolen, which is dependent on the vulnerability of the subsystem storing it, the rate of physical and network exposure, the attractiveness of the key to an attacker, etc. From these, one can compute the probability of loss of the key as a function of time and usage.

### 3.10 Risk #10: "Assurance of Identity"

Due to the high availability of CAs and the fact that all available CAs today follow certain procedures that differ and have different policies for issuing a certificate to a holder, the problem of assurance of the identity of the holder is higher. Today, not all certificates are issued equally. Some certificates are issued based on a valid e-mail address. Other certificates require presentation of photo ID and must be vouched for by a trusted party. Accordingly, the amount of trust that an application or even the user can show in each of these certificates varies and depends on the policies of the issuer. Of course the vulnerabilities of such certificate authorities are not in the certificate that they issue, but in the methods that they used for identifying the applicant. For example, via this method one can acquire a digital certificate fraudulently, by posing as another person if sufficient details of the other person are known.

These methods of impersonation should not be acceptable among the Health Care PKI system implementations. The system should apply different methods to identify the user. All these methods that are based on the Assurance of Identity should be clearly stated in the policies and procedures of such a system.

### 3.11 Risk #11: Definition of Certificate Policy and Certification Practice Statement

Among the PKI community there seems to be a kind of confusion as to what exactly these two policy statements are and what their exact definitions are. The unclear definition of CP and CPS can cause serious system downtime or an interruption of the workflow. For a Health Care PKI system both the CP and CPS should be clearly declared as legal statements whose primary function is the limitation of liability and the declaration of organizational policy about how the PKI will be implemented and used.

### 3.12 Risk #12: Profile Proliferation

Today, the X.509 (Appendix B) is generally accepted as the standard for digital certificates. X509 is currently implemented in three different versions with the latest being the X.509 V3 [2, 29]. X.509 V3 is comparable to Versions 1 and 2 in providing the basic functionality, but Version 3 also provides extra extensibility. X.509 V3 is consisted of several types of extensions, including those for keys, for policy use, for subject and issuer, and for constraints and limitations. Any of the extensions can be marked critical or non-critical. If it is marked critical, the extension is required and the application accessing it must be able to parse that extension, or the certificate will be non-usable. If an extension is marked non-critical, it may be ignored if the application does not support it.

The set of extensions and how they are implemented must be decided during the Health Care PKI system design. This is definitely a vital design decision for the complete implementation, since the more options used, the more likely there will be interoperability problems.

Understanding what the options are, how they work together, and how they are implemented in products and other PKI's is a time consuming task. Many extensions

permit multiple options. For example, the name fields may use an email address, an X.400 address, a URL, an IP address, or an X.500 directory address [36], in almost any combination. In addition to the standard extensions, X.509 permits adding customized extensions. Set of all available options used should be clearly stated in the CP.

### 3.13 Conclusions

There is no doubting that if such a system is developed for the health care sector the security of personal data during and after any transaction process is a must. Unfortunately many systems, which do not take into consideration the threats and the risks to a PKI system, can give short-lived promises that are far from reality. Prospect and former users of any Health Care PKI system with skepticism and knowledge should make the necessary inspections and verifications prior to deciding which system they will use.

During this section of the thesis considerations and risks, which need to be taken into account prior to the proposal of any policies for a Health Care PKI system as well as prior to the implementation of such a system, were analyzed.

# Chapter 4

## European and Cypriot Legislation

Due to the fact that the protection of patient records has become increasingly complex and more critical, when implementing a Health Care PKI system it is important that as many issues as possible are agreed on. This will result in the common benefit of both the patients and the organizations. To achieve a good degree of agreement certain legislation and standards should be followed.

Although this is not a law thesis, the sections that follow where included because they were taken into account during the proposal of the Certificate policy and Certificate Practice Statement, which apply for the Hippocrates CA. These sections provide the reader with an overview of the initiatives and guidelines that are applicable to the health care sector and may have significant impact on how electronic transactions will be made in Cyprus.

### 4.0 Overview

For a system to be well documented and become widely accepted a specific legislation and standards should be followed. The PKI framework [44] requires a combination of legislation and technical standards to succeed. A major achievement was the introduction of papers, called Directives [10, 16]. The European Commission submitted these Directives, which constitute the most common form of European legislation. All Member States are obliged to enforce these directives into their own legislative framework.

### 4.1 European Electronic Signature Standardization Initiative (EESSI) and Guidelines

The EU Electronic Signature Directive [10] has established the legal framework for the recognition of electronic signatures. The industry, with the assistance of European Standard Bodies, is in the process of providing an agreed framework for an open, market-oriented implementation of the Directive. In January 1999, therefore, a new initiative was launched – the European Electronic Signature Standardization Initiative (EESSI) [17], to execute this task. Its task is to identify the standardization activities

necessary to enable electronic signatures and to monitor the implementation of a work program to meet this need.

EESSI's first recommendations, made in July 1999, contained an overview of the requirements for standards related activities and drew up a detailed work program to meet these needs. Three key areas were identified:

- Quality and functional standards for Certification Service Providers (CSPs)
- Quality and functional standards for Signature Creation and Verification
- Products
- Interoperable standardization requirements for Electronic Signatures.

The priorities of EESSI are:

- Security requirements for signature products
- Certification/registration of conformance products and services for electronic signatures
- Security Management and Certificate Policy for CSPs issuing qualified certificates
- Signature creation and verification
- Electronic signature syntax and encoding formats and technical aspects of signature polices
- A standard for the use of X.509 public key certificates as qualified certificates
- Protocol to interoperate with a Time-stamping Authority

Many drafts and standards were created to support the European Electronic Signature Standardization Initiative (EESSI). Such as “ETSI TS 101 456 v1.2.2: Policy requirements for certification authorities, issuing qualified certificates” [19], “ETSI TS 101 862 v1.2.1: Qualified certificate profile”[18], “CEN/ISSS WS/E-Sign N 141: Draft CWA: Security Requirements for Signature Creation Systems” and many others.

### 4.2 EU E-Signatures Directive

The EU Directive [10] “on a Community framework for Electronic Signatures” 1999/93/EC, dated 13 December 1999 (“Electronic Signatures Directive”), lays out

the general framework for the use of electronic signatures, for reliable and legally valid communications via electronic means.

The scope of this directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of e-services.

The directive defines that electronic signatures cannot be denied as legal effects just because they are in electronic format, as they have the legal equality with hand-written signatures [48]. The directive, also allows Certification Service Providers to provide their services without prior authorization by national bodies and outside the internal market. Member Countries may themselves decide how to ensure the supervision of compliance with the provisions of the directive.

The directive also states the requirements for the constitution of a qualified certificate, the requirements for certification service providers issuing qualified certificates and the requirements for secure signature-creation devices.

Member Countries including Austria, Belgium, Denmark, France, Germany, Greece, Italy, Ireland, Luxembourg, Sweden and the UK have already rearranged the Electronic Signatures Directive. They implemented the appropriate legislation based on the directive for recognizing the legal validity of electronic signatures and the liability of certification service providers. Most of the times, the law complies with Annex I, II and III [10] of the E-Signature Directive. Also, all of the countries allow an organization to provide certification services with no prior authorization or license. In some cases a country requires an organization to provide certain information (i.e. name, address, email, legal form services) to an appropriate Telecommunication or other authority, before offering any services. For example, under the French law, a certification service provider must be a provider of cryptography services. Other, non-EU member states have also adopted the directives and have built up their own legislative framework for e-commerce activities. For example, the Utah Digital Signature Act [45] and the American Bar Association Digital Signature Guidelines developed their own legislative initiatives to address secure electronic commerce, with efforts by other states and the federal government, trailing close behind.

### 4.3 EU Directive on Data Protection

These Directives [11, 12] set out the legal framework for protecting the fundamental rights and freedoms of ordinary people, and in particular their right to privacy with respect to the processing of personal data. The Directives applies to the processing of personal data, wholly or partly by automatic means, as well as to non-automated processing of personal data, which are included or will be included in a record. It does not cover the processing of personal data, which is carried out by a person for the exercise of exclusively personal or domestic activities.

The Directives define what kinds of processing of personal data are allowed, along with the general principle that the collection and processing of sensitive data is prohibited; at the same time, the Law enumerates a long list of exceptions to this rule.

Member Countries providing this personal data must ensure that this data is:

- Processed fairly and lawfully;
- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member Countries provide appropriate safeguards;
- Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data, which is inaccurate or incomplete, as regards the purpose for which they were collected or for which they are further processed, is erased or rectified;
- Kept in a form, which permits identification of data subjects for no longer than is necessary. The length of this time period is decided taking into account the purposes for which the data was collected and any further processing this data might require. Member States should lay down appropriate safeguards for personal data stored for longer periods due to historical, statistical or scientific use.

Member Countries must bring into force laws, regulations and administrative provisions necessary to comply with these Directives, at the latest, at the end of a

three year period, starting from the date of its adoption. When Member States adopt these measures, they must contain a reference to these Directives or be accompanied by such a reference on the occasion of their official publication.
The methods of making such a reference shall be laid down by the Member Countries.

### 4.4 Cyprus Legal Framework

In Cyprus the enforcement of the above mentioned regulations became necessary, for the harmonization with the communal possession, and also for compliance with the European Convention of the European Council that makes provision for the protection of the individual from the processing of information concerning his/her person.

#### 4.4.1 Protection of Personal Information

The decree and enforcement of Law 138/2001 regarding the protection of personal information was signed by the Cypriot Government in 1987. The main aim of Law 138/2001 is the protection of individual members of the public, and it concerns information about the individual, such as personal, financial, professional as well as information about the individual's criminal record. Personal information is separated into two categories; the sensitive and the non-sensitive personal information. Financial information of the individual is not classed as sensitive.

The processing of an individual's information is only allowed when the subject in question gives his/her oral consent. The processing of such information is confidential and is carried out exclusively by persons acting under the control of the person in charge of processing this information. Processing means any work carried out by any person on the individual's information. It includes the collection, registration, organization, preservation, storage etc of such information. Information about the individual means any kind of information referring to a subject who is still alive.

Sensitive information according to the Law, is information concerning race or nationality of the individual, and political believes as well as information concerning criminal persecutions and convictions.

According to the Law the collection and processing of sensitive information is prohibited. Some situations may be considered as exceptions under certain

presumptions. Also the inter-association of files, according to the Law, is only allowed after notification of the commissioner. Permission to inter-associate files is given only if certain presumptions coexist.

Inter-association of files is any kind of processing, which gives the possibility of comparing the information of one file with the information of a file or files, which are kept by other persons in charge of processing or which are kept by the same person for another reason.

Unfortunately in Cyprus there is no legislation concerning certificates and encryption of information, especially health care information. However, with the enforcement of this law, the hospitals or health care organizations are obliged to have signed consent forms from the patient which will give them the right to exchange patient data.

### 4.5 Standards and Legislations apply for the Health Care Sector- European Union

The European Council in Feira, June 19-20, 2000 endorsed the Commission eEurope Action Plan 2000 "An Information Society for all"[14]. Under the heading *Health online* the challenge's objective is given as: "The prime objective of this action is to develop an infrastructure of user friendly, validated and interoperable systems for health education, disease prevention and medical care."

In order to allow access to healthcare information electronically, at all points where this is required, the need to secure data appropriately becomes a significant concern. Healthcare stakeholders, including patients, caregivers and administrators, must be confident that any sensitive medical information exchanged over networks will not be compromised, and will be viewed only by authorized individuals.

For these reasons, Security and Electronic Signature Standards, which include requirements for security of patient-identifiable healthcare information, were proposed. Standards for handling patient-identifiable health care information apply to all health care organizations and hospitals regardless of their size.

Standards are implemented to guard data integrity, confidentiality, and availability, as well as to guard data transmitted over a communications network against unauthorized access. Those are classified in to the following categories

- Administrative Procedures - to guard data integrity, confidentiality, and availability, with documented formal practices, covering contingency plans for system emergencies, policies on access control, formal termination procedures, and protection of data.
- Physical Safeguards - covers media controls and security on physical computer systems and equipment.
- Technical Security Services - to protect, control and monitor information access, such as access control, audit controls, consent for use and disclosure, data authentication, and user identification.
- Technical Security Mechanisms - includes processes created for preventing unauthorized access, integrity controls, and message authentication for data that is sent over a network.
- Electronic Signature - includes recommendations for, but does not require, the use of electronic signature.

As part of the information technology requirements some of the above points, require that technical policies and procedures are defined specifically for the following eight areas:

- User authentication
- Access controls
- Audit trails
- Physical security & disaster recovery
- Protection of remote access points
- Protection of external electronic communications
- Software discipline
- System Assessment

Each member state has to assess its own security risks and determine its own appropriate plan of action to achieve all the above.

### 4.6 Assessing Health Information on the Internet outside European Community

The Internet presents a powerful mechanism for helping users improve their health-care decision-making, by providing easy and rapid access, exchange, and dissemination for enormous amounts of health information. The Health Summit Working Group [15] was one of the groups that have developed a set of criteria to address this critical need. These criteria are intended as a resource for users seeking health-related information on the Internet, and should aid in evaluating information to determine whether it is usable and credible.

The Health Summit Working Group has developed a set of seven major criteria for use in assessing the quality of health information on the Internet. Those are credibility, content, disclosure, links, design, interactivity, and caveats (advisories).

### 4.7 Conclusions

Considering that the health care sector is one of the most crucial sectors, where any patient information is important and electronic communication between different parties is essential, the provision for secure, trusted and legislative systems must be provided.

Compared to Cyprus, the European Union[4] has a more mature and sensitive view, as far as patient information is concerned. The European Union has had its legislations and standards, concerning patient data protection, for a number of years, and trust in these has been shown from both doctors and patients. It is important therefore, when implementing a PKI system for Cyprus's Health Care sector, to take these European Directives [10, 16] into account as well as the standards that needed to provide appropriate protection for the data conveyed across the Internet in a practical, cost-effective way.

[4] The comparison with Europe is carried out because Cyprus will be entering the EU shortly and a harmonization with the European standards is a must.

# Chapter 5

## Discussion on PKI-related work

Nowadays, ready made Healthcare PKI solutions can be provided by many companies, such as Verisign, Baltimore, and Entrust. However, the cost of such applications along with the lack of scalability to suite the needs and standards of Cyprus's environment, made the supporting of a custom made application a favorable solution. The fact that the Hippocrates PKI system, which is the PKI system setup exclusively for Cyprus's Health Care System and which will be on trial initially for cancer patients, is custom made prevents any kind of comparison being made with the ready made applications. In order to get a feel of the difference in price between the two solutions consider that an application similar to Hippocrates is to be provided by Verisign or Baltimore. This would cost around 200 Euro per user. Add to this the additional cost for the software modules, which would cost around 30,000 euro for the server module and 30 – 50 euro per user for the desktop modules, as well as the cost needed to configure the application, this would lead to an unnecessarily high cost. However, setting up a custom made system such as Hippocrates would cost a lot cheaper. So far there has been no attempt to analyze the actual cost of the Hippocrates PKI system, although such a costing exercise is needed to identify the cost of the different implementation aspects of the development. Another reason for choosing a custom made PKI solution is that ready made ones are profit-oriented and it was judged that such solutions may not have been fully trusted.

It is also recognized that there are pilot projects and local implementations of systems similar to the Hippocrates PKI system. These pilot projects may apply to E-commerce sites, E-banking [25] or E-health and require an encryption solution [9]. Although these projects may apply to different sectors of every day life, they are all based on the same guidelines as written in the RFC 2527. This reference clearly states that certain modifications can be applied to suit the environment in which the Certificate Policy (CP) and Certificate Practice Statement (CPS) will apply. Even though E-commerce and E-banking have the biggest share of the market as far as applications are concerned, and are considered by many as the most important because they mainly deal with money, E-health care is as important and maybe even more critical than the others. E-health involves patient treatment and in some instances may make the

difference between life and death. For example, if tissue compatibility information for patients waiting for liver, kidney, bone marrow transplants etc, is lost, then some patients may loose their life despite the availability of donors somewhere else in the world. In addition, E-health requires patient information confidentiality. If this information leaks out, the patient can sue the health care organization. Apart from costing the hospital a substantial amount of money, it can also damage its reputation. As a result of this, patient trust towards the doctors may be lost.

PKI was adopted by the Australian Government [54] to enable the transfer of sensitive medical information across the Internet, without compromising the individual's right to privacy.

Health eSignature Authority Pty Ltd (HeSA) [54] acts today as a Registration Authority for the provision of digital keys and certificates within the Australian healthcare sector. HeSA will facilitate the introduction of PKI across Australia's health sector. Certificate authority tasks are appointed by SecureNet. Both HeSA and SecureNet have successfully completed the Commonwealth Government Gatekeeper process to become an Accredited Provider (February 2001) of PKI within the Australian healthcare sector.

The project was coordinated by The Alfred hospital in Melbourne that is currently using it for allowing health records to be accessed via the Internet.

Another PKI related application was adopted by the Government of Canada, which committed to electronic services delivery in 1999 [52]. At the same time an ambitious plan to make all federal programs and services available on-line by 2004, was announced. Since then the Government of Canada has become a recognized world leader in public key infrastructure implementation in a public sector environment.

As per the Canadian project, the Government of Canada Public Key Infrastructure [53] provides departments with an efficient, effective, common basis for the secure electronic delivery of federal services and programs. The ultimate goal of the government's PKI project is the establishment of a secure federal electronic service delivery system based largely on a centrally managed Public Key Infrastructure cross-certified with other PKIs.

Depending on a number of factors, different policies were implemented by the government of Canada which represent four different assurance levels and depend on the sensitivity or complexity of transactions. According to these policies each federal department may have its own Certification Authorities, or choose to enter into a contract with another organization for the provision of Certification Authority services. However, each departmental Certification Authority can issue different types of certificates. The applicability of these certificates will depend on the application used.

For instance, the certificates issued under "the management and use of certificates containing Public Keys [22, 48] used for verification, authentication, integrity and key agreement mechanism", could be used for verifying the identity of electronic mail [23] correspondents or remote access to a computer system, verifying the identity of citizens or other legal entities, or protecting the integrity of software and documents. However, the certificates issued under "the management and use of certificates containing public keys used for encryption key establishment, including key transfer", are suitable for providing confidentiality for applications such as electronic mail or Web communications, including the protection of Global Software Publishing (GSP) designated information.

The President of the Treasury Board acts as the head of the Government of Canada Public Key Infrastructure, and is responsible for entering into and terminating written agreements for cross-certification on behalf of the government.

A third PKI project that was studied was the one proposed by the Health Informatics working group [55], whose task is to define security terminology to be used in healthcare and in ISO/TC 215 standards in particular. It is also responsible for defining the essential elements of a health care public key infrastructure that will support the secure transmission of health care information across national boundaries.

Some other PKI projects which were also studied are the ones undertaken by the Swedish government and the trial PKI system in the United Kingdom, operating under the NHS plan [40, 56]. Unfortunately due to inadequate information in English about the Swedish PKI system, it is not possible for further information to be given on this

system. An announcement from the British Department of Health states that, the pilot trial is the first step in making electronic health records available to everyone in the UK by 2004. In this trial, patients will have access to all their consultations for the last four years. Each time a patient accesses his or her records, they will have their identity authenticated by a "clever mouse" that reads the patients' index fingerprints. Patients will also be given names and passwords to enter in order to validate their identity before they can see their records. Apart from the two above mentioned examples, in Europe there is generally the tendency of enabling health online [14, 51, 59]. The overall purpose of health services is to provide an increasingly good quality care for the patient / citizens not only in their home land but also throughout Europe and the rest of the world**.**

The above systems may not be needed in Cyprus because of the individual characteristics of the Cyprus environment. Cyprus is a small island and despite limited resources it is not difficult for anyone to find detailed information about anybody else in a very short time. There is also the fact that due to the work load many doctors have, it will be hard for them to adapt to a program designed for other environments apart from the one they are used to working in. Consequently, some of the important features of the above systems are of no great importance or use here. However, the need for a secure communication system between healthcare professionals in Cyprus is very important and thus became the incentive for the proposal of the Hippocrates PKI system. The policy statements of this PKI system were based on RFC 2527. The design of the Hippocrates PKI – System was based on the Cyprus culture. As a result there are many individualities and characteristics of the proposed CP, which were explained in Chapter 6, which may not be applicable to other countries.

The Canadian and Australian systems were chosen for comparison, because they provide a description of a complete system, and they are not drafts. They were not however chosen for implementing the Hippocrates PKI system, because this will apply to a close knit community based on cancer patients and oncology treatment and care. Therefore the system was designed in order to ensure that patient data remains within this community, whereas the two above mentioned PKI systems cover a broader community area and there main scope is making money. Some key

differences between the Hippocrates PKI system and the Canadian and Australian systems are also provided below.

These differences are:

(a) Applicability: The applicability of the Hippocrates System is exclusive to the Health care sector and will be pilot for the benefit of the cancer patients. If this project succeeds, then Hippocrates can be the base for developing the Root CA for the Health Care sector in Cyprus. For the application proposed in Canada, certificate policies have been designed to satisfy general public key certificate requirements of the Government of Canada. In Canada, as mentioned before, and under the policies defined by the government, each department may develop its own CA. For example the Ministry of Health may proceed to create a system analogous to the Hippocrates System.

(b) Financial Responsibility: In the Canadian policies each federal department may use a contractor to provide the required CA services. The contractor has to provide satisfactory evidence of financial responsibility. For Hippocrates this does not apply, since the services of Hippocrates will be provided only by the Bank of Cyprus Oncology Center, because of the limited number of people who will get involved. Despite this, the requirement by the government of Canada is correct and can be followed by the Hippocrates system also, if the need of a contractor arises.

(c) Fees: The Cyprus Health Care PKI system will currently charge no fees for the issuance of a certificate. As stated above, the system will initially be applicable to cancer patients. As per the law of the Republic of Cyprus, cancer patients are allowed to receive free treatment. As an extension of this everything concerning patient treatment, such as 3D-planning, dosimetry, calibrations, quality assurance test of medical equipment etc are free. The organizations dealing with these patients are of a purely charitable nature. It is therefore believed that it will be better for such a system to provide free services and be used, since the use of such a system will benefit the patients. For the Canadian PKI system the charging of fees is subject to the appropriate legislative authority and policy. Fees are also applied in all the other systems studied. Fees may be payable for the issuing and re – keying of Certificates, or even for certificate accessing.

(d) Subscribers: All system policies specify members / subscribers of the system. This could be an individual, an Organization, or a group of individuals. For each group, there are policies that use authentication methods as a way to prove identities. However, for the Canadian project, End entities may also be devices, or applications. For the Hippocrates project there are currently no provisions for identifying and issuing certificates to machines or applications. This may be part of any future work carried out by the Hippocrates team. For example sending Magnetic Resonance Imaging (MRI) or Computed Tomography (CT) images from one Hippocrates user to other Hippocrates Users, could well be an option in the future.

Compared to the Australian, the Swedish and the Hippocrates projects, the Canadian project assigns the eligibility for a certificate at the sole discretion of the CA. For the Canadian project, this works as expected, because the CA operates in federal departments. However for a closed community like the one Hippocrates will apply to, this is not the case, as the community does not have the power that a federal department processes. The role of the CA is, therefore undertaken by the PMAC.

(e) Policy Management Authority Committee (PMAC): In some applications, the PMAC is referenced to as PMA. For Hippocrates, the creation of a PMAC as a committee is suggested based on the structure of the application and on the members. This will have the upper hand in registering, interpreting and maintaining the CP. In this case the PMAC, as a responsible committee, will apply all the regulations set by the board of trustees of the BOCOC and the Law of the Republic of Cyprus.

For the system in Canada the Policy Management Authority, a senior executive committee, assists the Secretary and the President in their PKI-related duties. It also provides the overall strategic directions for the PKI in the federal community, and makes recommendations to the Secretary respecting membership in, and cross-certification with, the Government of Canada. In the case of Hippocrates, the PMAC will, for the time being, be the authority that will establish all the duties of the PKI and its members. This may not sound democratic, but the nature of the application of Hippocrates, and the fact that 75 % of the cancer patients treated in Cyprus are treated at the BOCOC, make this a practical setup.

(f) Determination of the Suitability of the CPS: There is a recommendation in the Australian System, that three different parties will determine the suitability of any CPS. Those are the Health Care PMA, the PMA operated by the CA and the Competent Authority. Understandably this may be one possible solution for big PKI systems. In our proposal, suitability of a CPS is performed only by the PMAC, which operates on behalf of the CA and the RA. As stated above, the PMAC is the BOCOC which treats about 75% of all cancer patients in Cyprus. It was therefore considered logical that in the closed community, in which the PKI system will be operating, the organization treating most of the patients should have the right to decide whether or not a CPS is suitable. At the same time, having only one body to take such decisions speeds up the whole process.

(g) Disputes – Disagreements: The policies that were proposed in this thesis, which can be found in Appendix A, suggest that any disputes be resolved through communication between the relating parties and the PMAC. There is no specific time limit for the resolution of such disputes, but it is dependent on the judgment of the PMAC. However, if the disputes are not resolved they should be submitted to an arbitrator. In this case the PMAC will act as the committee relating parties will use, in order to avoid any inconvenience, money loss or trauma, which may be caused if a case goes to court. In a way this results in the speeding up of the whole procedure. The same approach is followed by the PKI system in Canada. In Australia however, although they have the same approach, a specific time limit (max 28 days) is set for settling disputes. After that, the dispute may be submitted to the arbitrator. This direction seems to limit the role of the PMAC and at times may result in the frustration of the parties involved in the disputes.

(h) Records Retaining Period: According to the Hippocrates policies, the Health Care System must establish mechanisms to ensure the retaining of the audit information, Subscriber Agreements and any inspection, audit, application, identification, authentication, acceptance and revocation information for a time period which is equal to 7 years. This was decided following the current policies of the BOCOC for auditing and medical records keeping. In the Canadian PKI system the retaining period is two years. Nothing is mention in the Australian PKI System about the record retaining period.

(i) Identification & Authentication: Identification in the Australian PKI system is based on a points system. For example if a health care professional presents his/her birth certificate she/he earns 70 points. Upon receiving 100 points she/he is identified as a legitimate user of the PKI system. For the application proposed in Cyprus, this is not the case. Identification/Authentication of members depends on the group the user applying for a certificate, belongs to. For example, Authentication of an Individual -- Independent Practitioner can be done by contacting the Ministry of Health, the Subscriber, and the National Medical Committee. Even though the points system in operation in the Australian PKI system is a well organized system, such a system is not needed in Cyprus. This is due to the fact that Cyprus is a small place with a closely knit community. The Hippocrates community is an ever smaller community that this. It is therefore relatively easy to identify if an individual is who she/he claims to be and if they are eligible to become legitimate users of the PKI system.

(j) Name Uniqueness: For all applications studied, distinguished names (DN) must be unique for all End-entities of a CA. For the Hippocrates PKI – System the CA may issue additional numbers or letters to the commonName to ensure the uniqueness of the DN. The subject name (for certificate applicants) must have a distinguishable and unique Distinguish Name (DN) in the certificate subjectName field. The subjectName and issuerName must have a reasonable association with the authenticated name of the Subscriber. It is also recommended that the organizationName component be included in the DN and that it should be the official name of the Organization.

(k) Suspension: Another major difference with the applications that were studied deals with the suspension of the certificate. For example, Suspension of Certificates for the Canadian PKI system is not applicable at all. In the Australian PKI – System suspension may occur when circumstances for revocations are suspected, but are not confirmed. For the application proposed in Cyprus, Certificates should be suspended by the CA, if the CA suspects unauthorized use of the certificate, and should proceed with further investigations. Also, upon notification of a temporary change in employment status of the Subscriber, a restriction of the Subscriber's rights to access health information for a certain time period may occur.

(l) Training: In the Hippocrates PKI – System extensive training and seminars are suggested for all group users, taking into account that many of them do not have the required computing knowledge. Users must have knowledge of how to back up and protect their keys and also how to operate the system. Training is also advisable for all the PKI –System personnel. However from the systems studied, adequate training is only reffered to in the Canadian PKI System.

(m) Cross Certification: Due to the non-existence of other CAs in Cyprus, cross certification was not taken into account. However, this shall be taken into account in any future expansion of the PKI – System.

In the Government of Canada Public Key Infrastructure, departments may operate more than one Certification Authority. In such instances, the department designates one of its Certification Authorities to be its Level 1 Certification Authority. It cross-certifies with the Canadian Central Facility, and signs the certificates of the department's subordinate Certification Authorities. If a department has only one Certification Authority, it is automatically a Level 1 Certification Authority. A department's Level 1 Certification Authority is responsible for the creation of the departmental Certificate Policies and Certification Practice Statement.
In the Australian system, however, there is nothing mentioned on cross certification. Although not mentioned in this thesis, it seems that cross certification will be needed to connect other future services the government of Cyprus may need to provide, in the case of the expansion of Hippocrates.

(n) Group Division: Another innovation of the policies in the Hippocrates PKI - System is the division of authorized personnel into groups ranging from doctors to anti-cancer societies, with a different scope of authority for each group. In Cyprus, the authentication of these groups is hard to implement, therefore it is suggested that this be done by the authorities to whom these groups belong, i.e. for doctors by the Medical Association or the Ministry of Health. For patients authentication takes place after doctor recommendation and approval from the PMAC. Other applications do not seem to provide such a group division, but they offer different types of certificates, which, in a way, control the user privileges in the system. This application effectively has the same result as the one suggested in the Hippocrates PKI – System. In the Hippocrates- PKI system however, due to the small community the system applies to,

and due to the fact that closer control and higher security levels are required, the suggested division of groups is the ideal solution.

(o) Revocation List : For a more efficient operation of the Hippocrates – PKI system it is very important to notify all members and Relying Parties of the issuance or revocation of a certificate. The same strategy, applying to the revocation or issuance of certificates, as the one suggested for the Hippocrates PKI system, is also followed by the Australian PKI – System. For the Canadian PKI – System there is no requirement for a revocation list and currently it does not support an on-line revocation/status checking.

(p) Auditing: Auditing for Hippocrates is being made by external auditors only. Periodic inspection of the performance of the PKI system is at the sole discretion of the PMAC. For the Canadian system only one of every five audits must be done by an external department. The rest are made by the PMA. Due to the lack of experienced people in Cyprus it is believed that external auditors, who have sufficient knowledge of the PKI technology and cryptography techniques, should carry out these audits. External inspectors must also have knowledge of the operation of the relevant PKI software and the operation of the PKI components [48] in accordance with this policy.

In this chapter related work to the Hippocrates system was summarized. From this related work a few differences - innovations of the Hippocrates system were extracted. In general applicability of the Hippocrates system is primarily only for the benefit of cancer patients from whom no fees will be charged. Each subscriber of the system will be divided into different groups which will be given different rights accordingly. The complete authentication of each group of subscribers will be a decision of the Policy Management Authority Committee which will apply all the regulations set by the BOCOC, the law of the Republic of Cyprus, the CP and the CPS. When disputes arise the Hippocrates approach is that disputes will be resolved through communication between the related parties and the PMAC. The time taken for a dispute to be resolved is in the sole discretion of the PMAC. A record retaining period has been set according to the BOCOC policies. Identification-authentication of a member can be done by contacting the ministry of health, the national medical committee and the organization/society to whom the subscriber belongs. Another

innovation recommended by the system is that there will be no cross-certification with other CA's in Cyprus. There will also be extensive training of the personnel. For a more efficient operation of the Hippocrates – PKI system a revocation list that notifies all members and Relying Parties of the issuance or revocation of a certificate is suggested. Finally for Hippocrates, Certificates should be suspended by the CA, if the CA suspects unauthorized use of the certificate, and should proceed with further investigations.

# Chapter 6

## HIPPOCRATES-PKI Certificate Policy (CP)

This part of the thesis summarizes the design issues and procedures that indicate the applicability of a certificate, for the operation of a particular community with particular security requirements, in this case the Health Care sector. It also highlights the design choices for the set of rules in the so called Certificate Policy (CP), which form the basis for the operation and management practice of certification authorities (CAs). The aim of the CP is to create the appropriate confidence in certificates, issued by a Certification Authority (CA). Subscribers and other parties, certified by any particular CA, must have confidence in the applicability of the certificate.

Due to the high volume and the structure of the certificate policy, it was decided to include in this part of the thesis only a brief description of its content along with a description of issues that make the design of this CP both unique and, applicable to the Cypriot standards. The complete CP can be found in the appendix section. Although, the structure of the CP was based on the Internet X.509 V3 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [5], some diversions were made based on the demands and the needs of the health care sector in Cyprus. Those diversions are explained in this section.

### 6.0 Introduction

In general, the aim of issuing this CP is to set the policy requirements for the operation, management, and use of certificates containing public keys for digital signatures. This is to assure that the verification, authentication, data integrity and key agreement mechanisms will be well established.

The role of each part or member of the PKI system is briefly described. These parts are the Policy Management Authority Committee (PMAC), the Certification Authority (CA), the Registration Authority (RA), the Sponsors, and the Subjects which represent the community on which the system is built and to which this policy will be applicable. The members are fully responsible and liable for any actions that diverge from the provisions of the specific CP.

Other issues described are the role, the function, and the need of repositories, which are closely related with the certificate status checking, and the contact details regarding the policy.

The proposed CP of the Hippocrates-PKI differs from other CPs in that it applies only to the Health Care system. Another innovation of the Hippocrates-PKI system, as detailed in the Certificate Practice Statement (CPS), is that it is a closed system, which applies only to cancer patients in Cyprus, who receive treatment from the Bank of Cyprus Oncology Centre (BOCOC), and who are registered patients for receiving home-care from the Cyprus Association of Cancer Patients and Friends (PASYKAF) and DITIS[5] research team, i.e. the two non-profit organizations who offer assistance to cancer patients in Cyprus. A special feature of the system is that a Policy Management Committee (PMAC) is proposed, which, as discussed later has extra responsibilities and more power. The PMAC according to the CP and CPS is the Bank of Cyprus Oncology Centre (BOCOC), as this treats more than 75% of cancer patients in Cyprus. All subscribers are Health Care employees and professionals as described in the CP. According to the CPS of this PKI system, however, the subscribers here are all Health Care professionals related to Oncology. These belong to the closed system, described earlier. Their role, as specified in the CP, is approved by the PMAC. A real time online status checking (repository) is also proposed for checking the status of the certificate. The repository, as described in the CP, will give the opportunity to users for checking the status of other certificates on a 24hour basis. Finally, another innovation proposed in this section regards any future expansion in users of the Hippocrates-PKI system. In such a case Hippocrates will be able to use a contractor to provide some of its services. It will however, be responsible and accountable for the CP.

### 6.1 General Requirements

All requirements relating to the obligations of the CAs, RAs, PMAC, Sponsors,

[5] DITIS is a system that supports Collaborative Virtual Healthcare Teams dealing with the home-healthcare of cancer patients in Cyprus. Through a pilot project DITIS will support the activities of the home healthcare service of the Cyprus Association of Cancer Patients and Friends (PASYKAF), using a patient centric philosophy. It is based on the Internet (web) and on GSM mobile communications.

Subscribers, Relying Parties (inspectors), and other issues pertaining to law and dispute resolution are clearly stated in this section.

This section also explains in detail the role that the different authorities and subscribers of the system have, as well as the authority that one has over the other. For example, in the relation of the CA with the RA, the RA always operates in the interest of the CA. The CA's role, is to ensure that all RAs operate and act in accordance to relevant provisions of this CP. Some of the unique obligations of the CA are:

- The maintenance of a CA Repository which will not be accessible to the public, but will be for the CA's use only. This Repository is a reference for keeping records of the certificate as well as a means for backup and protection of the CA's data.
- The providing of relevant information about the issued certificates to the interested authorities, as required by the law governing the Republic of Cyprus, in the case of disputes concerning digital certificates.

The RA has some unique obligations in the Hippocrates-PKI system as well. Some of these unique obligations are:

- Prior to submitting the information of a subscriber to the CA, the RA is obliged to verify the identity and any other given information of that subscriber. It also has the obligation to verify that the subscriber has the right to receive a certificate. As mentioned in the later section of this Chapter as well as in the CPS, the RA, for example, must identify that the physician is a certified one and eligible to work in Cyprus as per the governing Laws of the Republic of Cyprus.
- The identification and recording of all subscriber actions which are helpful in the case of disputes or any other violations against the RA.

As per the General requirements section, the guaranteed conservation of these obligations is achieved through an agreement between the CA and the subscriber which clearly outlines the minimum obligations and responsibilities of all members of the system. In this agreement certain obligations and responsibilities are assigned to

each category of Hippocrates users, whether these are individuals, organizations or groups of individuals.

Emphasis is also given to the financial responsibilities and liabilities of the subscribers. As per this CP, any financial costs for the use of the CA services are paid for by to the Organizations, individuals, or any other relying parties of the Hippocrates-PKI. The CA has no obligations, and disclaims all liability for any use, other than the intended, as identified by this CP, for the certificates issued under this CP. However if the CA fails to comply with the terms of this policy, then the CA itself becomes responsible and liable for any damages to the users.

A unique characteristic of the Hippocrates-PKI system is that any services provided to the closed Health Care system mentioned above, will be free of charge as stated in the CPS. Finally this CP suggests that external auditors should inspect both the CA and RA performance and check the compliance of PKI components [37, 48] of this CP as well as checking whether the CPS meets the requirements of the provided CP. As suggested in the CP, external auditors must have sufficient knowledge of the PKI technology. Additionally, as stated in the CPS, periodical inspections will be performed by the PMAC.

### 6.2 Identification and Authentication

The registration process to obtain a Hippocrates certificate is given in this section. According to this process there are two ways that the certificate application will reach the RA; via the electronic way, over a secure channel using the public Internet, or by bringing the application directly to the RA, in person.

In the process of identification and authentication emphasis is given to the type of names and the need for these names to be meaningful. Although this CP was designed in accordance with the RFC 2459, like other CPs, the individuality of this CP is due to the fact that it stresses the uniqueness of names in all groups mentioned above e.g. Medical Oncologists, Home-Care Specialist Palliative Care Nurses, Psychologists, Physiotherapists, Social workers, other members or patients, organizations or groups. The CP requires that the Distinguish Name (DN), listed in a certificate must be unique among all entities of a CA. For each entity, the CA must

issue additional numbers or letters to the common name to ensure the uniqueness of the name.

A final point on the uniqueness of this system is the lack of any points system for the evaluation and authentication of individual subscribers, organizations, or groups. Specific rules for the authentication are given in the CP. However, organizations that do not belong in the Health Care sector and act as agents or as business partners of healthcare organizations, are not allowed at the moment to be authenticated.

### 6.3 Operational Requirements

This section describes the requirements imposed upon the issuing CAs, RAs, and the end entities with respect to various operational activities. These requirements have to be satisfied when applying, issuing, or accepting certificates. They can also be used for justification of revocation and suspension of certificates. This section also discusses the auditing procedures as well as the types of events which are recorded, and refers to the way the RA will handle the application of the certificate. As mentioned earlier, applications may be submitted via two methods; online or by completing a printed version of the electronic form. In both cases the applicant should provide adequate proof of his/her information in written form. Beyond this, the future needs of cross certification were not overlooked, although the CP was designed with the knowledge that the Hippocrates – PKI system will initially be applicable to a closed community. Furthermore, according to this policy certificates will not be published to the RA repository unless they have been accepted by the user via electronic means.

Revocation requests can only be done through the authorized RA electronically or if the Subscriber contacts the CA or RA in person and provides adequate proof of identification. Certificates should be suspended by the CA when there is suspicion of unauthorized use of the certificate, as well as upon notification of a temporary change in employment status of the Subscriber; this may result in the restriction of the Subscriber's rights to access health information for that time. However, during suspension, a limited valid license period healthcare certificate may be issued to the Subscriber.

Weight is given on the importance of the existence of a disaster recovery plan, as well as the existence of physical, procedural, and personnel security controls. As specified, the site that will implement the PKI system must have the above well documented. These must also be publicly available to all members through the RA website.

Finally, the CP gives the freedom to each CPS for the retention of the audit and archive logs. However, it specifies that for audits, the time should not exceed 30 days, and for archiving, as in most of the health care organizations, all patient records should be retained for at least 7 years.

### 6.4 Physical Security -- Access Controls

Both the CA and RA shall implement security controls in order to ensure that access to the sites is limited only to authorized personnel, listed in the access list. For this reason security personnel shall monitor and inspect the site on a 24 hours a day, seven days a week basis. In the case of the RA, security access controls may be varied due to the fact that candidates for a certificate as specified in this policy are allowed to deliver Hand Written applications. To control access from the Internet the RA will operate under a secure network that includes intrusion detection and firewall systems. This is, however not described here because it is not a concern of this thesis. Other procedural controls will also be assigned. These are the different trusted roles assigned among the CA and RA personnel. For example, the CA Security Manager's role includes assigning security privileges and access controls of CA Operators and System Administrators. The CA operator's tasks are limited to operating the system. In this CP, particular emphasis is given to the fact that more than one person is required for each task. This is to ensure the high quality of services and proficiency. At the same time it gives the CA the flexibility not to depend on the knowledge of one person only. However, personnel must have the adequate qualifications required for the duties to be performed. Additionally, as suggested, comprehensive training should be provided to all personnel. None of the above was addressed in any of the other CPs studied while implementing the CP suggested in this thesis. The CA will operate in isolation i.e. it will not be connected to any networks.

### 6.5 Technical Security Controls

This section contains provisions of the public/private key pair management policy for CAs, RAs and end entities, and the corresponding technical controls. More specifically, it refers to the key size which should be long enough to provide adequate protection [41, 42]. As stated by Health Care Financing Authority (HCFA) Internet Security Policy, 24th November 1998, a 1024 bits key will be used. Both the CA private signing key and the end entity private signing key must be well protected from any disclosure and unauthorized use, especially when not active. Guidelines on how to protect the keys should be issued to the subscriber upon the acceptance of the certificate. It is recommended that the CA's private key be stored in an isolated machine within a restricted area and under strict access control. Regular backups for both keys should be made so as to minimize the recovery time in case of system disaster. A reference is also made to the period of validity of keys. In particular the Policy CA public and private signature verification keys have ten and seven years' validity period respectively. If this was not the case then the CA would have to go through the procedure of notifying all users of these changes as well as having to issue other certificates for all its members more frequently. Changing these keys, therefore, on a frequent basis would hamper the operation of the system. Because by changing the CA must provide appropriate notice to all its members, revoke all certificates issued using the old key, request revocation of cross-certificates issued to the CA, and finally re-issue certificates to all Entities and ensure all CRLs are signed using the new key. In contrast to this, other public and private keys should be valid for one or two years, depending on the importance of the key.

Another characteristic of this CP, is the reference to the specific computer technical requirements regarding security. This covers the Network Security Controls of the system that must be protected from any attacks through any open or general-purpose network with which it is connected. Also covered by these security manners are the Web Server Security, the Operating System Security, and the Database Security. The Web Server Security must be such that the web server limits user's access to specific resources and folders. The Operating System Security should provide filesystem security; that is, every user account should have limited, predefined access to the system's folders and files. Finally, Database Security with Discretionary Access Control in which the selected DBMS must allow the ability to create, modify and

delete user accounts in the database level. The DBMS must support discretionary access control; i.e. it should provide the DBA with the ability to define the tables to which a user has access to, as well as the kind of access (INSERT, UPDATE, DELETE, SELECT).

### 6.6 Certificate and CRL Profiles

Section 6.7 gives a summary of the technical make up of a certificate, and the revocation list, as present in more details in Appendix A. In general terms, information is provided on the following:

- Certificate and CRL profile
- Version Number
- Certificate Extensions
- CRL and CRL entry extensions

Appendix A includes tables for the above and the user can see the structure of the certificate from these tables.

### 6.7 Specification Administration

Administering a specification requires certain actions to be taken by the PMAC in case of changes made to the CP. The PMAC is responsible for providing advanced notice to all entities and all authorities before any changes are made to the CP. The notification mechanism will be determined by the PMAC. Comments to the PMAC, by affected users, on any changes of this policy are accepted. However, decisions with respect to these comments are at the exclusive discretion of the PMAC.

### 6.8 Policy Administration

This section refers to any relying parties that may need to register an object identifier number for this policy. This may happen in the case of cross certificate authorities.

### 6.9 Personnel Expertise

The use of familiar and easy to learn technology is highly desirable, for this policy as it will lead to easier understanding, faster implementation, quicker response, less training cost when changes are required.

# Chapter 7

## Certificate Practice Statement (CPS)

### 7.0 Overview

To illustrate the proposed CP the following Certificate Practice Statement (CPS) for cancer patients is proposed. This CPS is adopted by the Bank of Cyprus Oncology Center and PASYCAF to enable the provision of continuity Cancer Care, extending from the treatment center to home care. Shown in the ensuing sections of Chapter Seven (7) is this CPS, which is based on the proposed CP (Appendix A). The naming of sections and subsections is the same as in the CP.

### 7.1 Introduction

**Introduction**

This is the Certificate Practice Statement (CPS) for BOCOC CA. It states the practices the CA employs in issuing and managing certificates. The CPS outlines the technical, procedural and personnel policies and practices of BOCOC CA. Only the sections where practices are added are present in the CPS.

**Identification**

This is the CPS of the BOCOC CA, a member of the Cyprus Public Key Infrastructure. (This CPS has not yet approved by any PMAC, however prior to being applied it should be approved and the date of approval should be stated here.

The CPS is published at URL: www.hippocrates.org.cy/policies.htm[6]
As a member of HIPPOCRATES-PKI, the BOCOC CA is operating in compliance with the CP of HIPPOCRATES-PKI:

- Certificate Policy Name: HIPPOCRATES-PKI-DigCertV1.0
- Object Identifier: 16582 : More on Object Identifier can be found at http://www.iana.org/assignments/enterprise-numbers
- Document version: 1.0

[6]The domain name hippocrates.org.cy is registered. However, all relevant sites are available, but will only become operational after receiving approval from the closed community that will use Hippocrates.

- Document date: May 2003.

Due to the specific application of this PKI system, this CPS is only applicable to Oncology and more specifically a tight group consisting of the Bank of Cyprus Oncology Centre (BOCOC), PASYKAF and DITIS.

**Policy Management Authority Committee (PMAC)**

A committee employed by the Bank of Cyprus Oncology Center will act as the PMAC. PMAC will be responsible for the compliance of the HIPPOCRATES-PKI members with the CP and the CPS. It will also define the rights of the subscribers.

**Repositories**

Each CA is responsible for maintaining an on-line repository or another certificate validation service that is available to the Relying Parties in a 24-hour, seven-day-a-week period.

CRL information**:** http:// www. hippocrates.org.cy /repository/information.htm

**Sponsors**

The committee employed by the Bank of Cyprus Oncology Center will initially be the only sponsor. This committee will act in accordance with the rights given by the PMAC. Future progressive sponsors will be added in later CPS versions. The PMAC is the sponsor of the Policy CA.

**Subscribers (subjects)**

As per the groups that are specified in the CP. However, due to the closed system that will at first be applicable, only health care officials concerned with Oncology will be eligible to become subscribers.

**Policy Applicability**

This CPS along with the CP is applicable to all PKI authorized members.
Certificates may be used because of the reasons stated in the CP. For:

- e-mail signing and encryption (S/MIME) [36, 47]
- server certification and encryption of communications (SSL/TSL)
- Object-signing.

## CERTIFICATE AND CRL PROFILES

### Certificate Profile

As per the CP and Reference ISO DTS (Draft Technical Standard) 17090, Part 2 – Certificate Profile [57].

### CRL Profile

The BOCOC CA will issue X.509 version two (2) CRLs in accordance with IETF RFC 2459.

### Contact Details

Questions concerning this policy should be addressed to the Hippocrates Home site, on which a feedback mechanism is included for users to offer their comments, corrections, and criticisms, and raise questions about any information provided.

The Hippocrates home page is: http:// www.hippocrates.org.cy

## 7.2 Requirements

### General Requirements

All requirements stated in the CP for the obligations of the, CAs, RAs, PMAC, Sponsors, Subscribers, and Relying Parties, are applied in this section. Further to that, this section is concentrated on any specific requirement that may apply exclusively to the CP.

### Other CA obligations

In order to verify all information given by the subscriber, the CA follows certain measures and procedures. Such measures depend on which category the subscriber belongs to. Such measures are:

- Groups: Directly contact the head of the group or the manager of the organization to verify the information given and the purpose of the need of a certificate. Further investigations may depend on the type of members included in the groups. For example, if in one group all the members are

doctors then the CA will follow the procedures specified for the health care professionals.

- Healthcare Professionals (physicians): Contact the ministry of health and the Medical Association.
- Nurses: Contact the general manager, Heads of the departments, Matrons or sisters of the organization that the nurse is employed by.
- Healthcare workers: Contact the general manager and the Heads of the department of the organization that the employee works for.
- License Healthcare organizations: Contact the ministry of health to verify the license and any other information that is given.
- Patients: Directly contact the professional health care member, for the approval of their application and to verify any given information.
- Medical Societies i.e. Anticancer Societies: contact the ministry of health to verify the license and any other given information.
- Home-Care Specialist Palliative Care Nurses: Direct contact with the appropriate Medical Society to which the nurse belongs to.
- Administrators: Contact the PMAC to approve their actions.

The PMAC must ensure that all the CA personnel associated with any PKI actions, have signed an employment agreement that clearly specifies their penalty clause for any actions that can be considered as violating this CP and CPS.

Both the CP and the CPSs are publicly available on the Hippocrates Web Site.

**Certificate Status**

The CA must inform all the Subscribers and all Relying parties of the Status of their certificates. This will be done in terms of Validation, Renewal, Expiration, and Revocation in the Hippocrates Web Site. At the Hippocrates web site, the user may access the Certificate Repository section and search for the status of a certificate, depending on any information the user has for a certificate or the certificate code. The output result will specify the current status of the certificate.

**PMAC Obligations**

The PMAC will employ a committee that will be responsible for checking the compliance of the users with this policy. The PMAC will periodically inspect the work done by the committee and will ask for specific user reports or any other reports regarding the operation of the PKI system. Another of the PMAC's duties will be the performance of periodical inspections of the PKI system to check its compliance with the CP.

**Subscriber Obligations**

The Subscriber Agreement is included in Appendix C. Generally, in order to ensure that the certification process is trustworthy and to secure the exchange of data / communication, the subscribers and relying parties are expected to comply with all the policies and duties mentioned in the CP.

**Repository Obligations**

BOCOC CA is responsible for maintaining an on-line repository or other certificate validation service that is available to the Relying Parties on a 24-hour, seven-day-a-week period. The BOCOC CA will maintain a second repository to minimize the risk of data loss and to guarantee data availability.

**Liability**

CA only guarantees the control of the identity of the subjects requesting a certificate, according to the practices described in this document. No other liability, implicit or explicit, is accepted.

CA will not give any guarantees about the security or suitability of the service. The certification service is run with a reasonable level of security, but it is provided on a best effort only basis. It doesn't warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

CA denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

However, the CA is responsible for any damages due to the failure of the CA to comply with the terms of this Policy. CA is also responsible to Qualified Relying Parties for any damages that are caused to any suitable applications or any loss of information due to this failure of compliance with this policy.

This CA, as mentioned earlier will be exclusively used for the good of the Cancer Patients. All parties involved, namely the BOCOC, PASYKAF, and DITIS want to have this CA working properly and are offering important help towards this. They do not expect to have warranties for its operation. However, once the system is proven for its reliability and applicability in other areas of the health care system, other prospective users, i.e. other hospitals, clinics, or even the Ministry of Health itself, may come to trust the system enough as to apply it for other groups of patients. If this system is developed to the point where it can be released as a commercial product, then it does not only have to instill trust in the users, but it has to have internal ways for verification of its reliability (self test). This CA will exercise its ability to ensure that the system is available 'most' of the time.

**Financial Responsibility**

The HIPPOCRATES-PKI assumes no financial responsibilities with respect to its members. However, the services provided will be free of charge to the closed community mentioned above.

**Governing Law**

Interpretation of this CP and CPS is according to the Republic of Cyprus Laws.

**Severity, Survival, Merger, Notice**

In case that it is determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated

**Frequency of Publication**

- Certificates will be published as soon as issued.
- CRLs will be published as soon as issued and at least every month.

- Changes to this CP and CPS will be published as soon as they are approved. Previous versions will remain available on-line.
- Any information available to the CA must be published in the repository within 72 hours.
- Certificates issued by the CA, which reference this Policy, will be published within 48, upon the receiving of the certificate from the Subscriber.
- Any information related with this policy that affects the operation of the CA, i.e. information regarding revocation of a certificate, obligations, etc. must be available to the Subscriber immediately after the modification or alteration of this policy.

Publications will be available on the Hippocrates Web site at the following pages:

CA information: http://www.hippocrates.org.cy /ca/information.htm
CRL information: http://www.hippocrates.org.cy /repository/information.htm
CP/CPS: http://www.hippocrates.org.cy

**Confidentiality Policy**

In order to ensure trust and confidentiality among its members, the BOCOC CA divides confidentiality in the following categories

- **Users Key Privacy:**
  Although some of the CA employees may have access to the users' private keys issued by the CA, the BOCOC CA guarantees the subscribers that under no circumstances will it use the private keys of any subscriber to whom it issues a certificate.
- **Personal Information:**
  BOCOC CA doesn't collect any kind of confidential information. However, any information included in issued certificates and CRLs is not considered confidential.

**Certificate Revocation:**

All revoked certificates will remain in the CRL list in order to inform other members of the system about the certificates' status. However, when a certificate

is revoked, a reason code will be included in the CRL entry for the action. This reason code is not considered confidential. A reason code will be included to briefly explain the reasons for revoking a certificate and also as an example of avoidance to the others. More specific details concerning the revocation will not be disclosed unless required by a legal authority of competent jurisdiction.

### 7.3 Authentication

**Identification and Authentication**

As per the methods, which were described in the CP.

**Types of Names**

As per the Hippocrates CP and according to "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [1, 2], each entity of the BOCOC CA must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subject name field. BOCOC CA will include no alternative names in the subjectAltName extension field of the certificate.

**Name Meanings**

For the BOCOC CA the following will apply:

- The Subject Name must represent the subscriber in a way that is easily understood for humans.
- The organization name component is included in the DN.

**Name Uniqueness**

- The Distinguished Name must be unique [30] for each subject certified by BOCOC CA. In case the uniqueness of the name cannot be achieved then additional numbers or letters are appended to the common name to ensure uniqueness.
- Certificates must apply to unique individuals or resources. Users may not share certificates unless they are group certificates. For CAs the English name is recommended.

**Re-key after Revocation**

Re-keying after revocation will follow the same rules as an initial registration.

**Revocation Request**

Certificate revocation requests must be sent by

- E-mail, signed by a valid BOCOC CA certificate, to revocation.request@hippocrates.com.cy
- Request directly on the web site.

If requests cannot be signed by a valid BOCOC CA certificate, BOCOC CA will verify the same procedure used for the authentication of identity of a person.

**Types of assurance**

Interoperability of PKI technology and supporting policies, procedures, and practices is of fundamental importance, if information is to be exchanged between organizations and between jurisdictions in support of health care applications (for example between BOCOC and PASYKAF).

Achieving interoperability between different PKI schemes, requires the establishment of a framework of trust, under which, parties responsible for protecting an individual's rights may rely on the policies and practices and, by extension, the validity of digital certificates issued by other established authorities

The proposed solutions for this issue are:

- To develop a standard Healthcare X.509 V3 certificate profile. This will enhance interoperability and reduce implementation efforts.
- Follow in a way that is possible the internet standards as mentioned in the IETF PKIX (Public Key Infrastructure using X.509) [1, 2] Working groups and the ASTM E-31 (Healthcare Informatics). These are very generic profile policies for healthcare, with widespread recognition.

### 7.4 Operational Requirements

**Application for a Certificate**

Procedures vary according to the category that the applicant belongs to. However, applications for Certificate requests may be submitted via:

- An online procedure, using a www browser and contacting the Hippocrates RA web server.
- By downloading the application form and delivering it by hand, with all the appropriate information.

**Certificate Issuance**

The BOCOC CA issues the certificate if, and only if, the authentication and the validation, of any given information of the subject, are successful.

If the authentication is unsuccessful, the certificate is not issued and an e-mail, with the reasons behind the denial of issuance, is sent to the subject.

**Procedure for Revocation Request**

This can be done through the authorized RA electronically. The entity requesting the revocation must authenticate itself in one of the following ways. By:

- An e-mail to revocation.request@hippocrates.com.cy, signed by a valid BOCOC CA certificate belonging to a natural person.
- Contacting the CA or RA authorized personnel and providing adequate proof of identification.

**Certificate Status or CRL Update**

CRLs shall be updated at least every 24 hours to ensure that the most recent CRL is available to the Relying Parties. A relying party must verify a certificate against the most recent CRL issued, in order to validate the use of the certificate. Hippocrates RA was designed to have an on-line service that provides timely information regarding the revocation status of a certificate: certificate status can be viewed from the RA repository page. It is possible that some time passes until CA forwards updated CRLs and certificate statuses (see next paragraph).

**Revocation Request Grace Period**

Unless there is a suspicion of a key compromise, any request for a revocation should be processed according to the order in which the requests are received (First In First Out).

**Types of Event Recorded**

The BOCOC CA should record in audit log files all events relating to the security of the CA system. Logs should be electronic and should contain the date and time of the event, and the identity of the entity which caused the event.

The BOCOC CA should also collect and consolidate, security information (not CAsystem generated) either electronically or manually. Such security information may be:

- physical access logs
- system configuration changes and maintenance
- personnel changes
- discrepancy and compromise reports
- records of the destruction of media containing key
- material, activation data, or personal Subscriber information

**Frequency of Processing Audit Log**

Audit logs will be reviewed at least weekly. Reviewing will give significant information on events such as security threats, CA compliance with the CP , and User compliance with the CP and the CPS.

**Retention Period for Audit Log**

This is for statistical analysis in case any security threats or disputes arises The BOCOC CA will keep the Audit logs for a minimum retention period of three years.

**Audit Log Backup Procedures**

Logs are copied monthly to removable media and encrypted with a pass phrase of suitable length. All backup procedures that are described in the Backup procedure chapter should be followed.

**Audit Collection System**

All actions taken by the Subscriber, along with the date and time of the actions, and the identity of the Subscriber, who caused the action will be audited.

**Retention Period for Archive**

The minimum retention period is three years; the maximum retention period is seven years.

**Integrity of the Backups**

As per the instructions that are given in the Backup policies of the BOCOC.

**Disaster Recovery Plan**

As per the instructions that are given in the Disaster Recovery of the BOCOC.

**7.5 Physical Security**

**Physical Security -- Access Controls**

The CA operates in a controlled environment, where access is allowed to authorized people only. The CA and RA are housed in the Bank of Cyprus Oncology Center in the Physics Department in the IT Room.

**Other Physical Security Aspects**

No unauthorized access to the hardware is permitted and all removable media are stored in secure containers. Aspects such as: Air Conditioning, Water Exposures, Fire Prevention, Protection Media Storage Waste, and Disposal Off-site Backup should be covered in the disaster recovery plan of the Bank of Cyprus Oncology Center.

**Multiple Roles (Number of Persons Required Per Task)**

The PKI should not be depended on a single person's knowledge. At least two people per role are expected to be available. The administrators of the system will be assigned personnel duties as per their qualifications and will also decide on how the secrets of the CA system will be shared between them.

**Personal Security Controls**

Only trained persons, who are well aware of the necessary security requirements, may be CA managers.

**Background and Qualifications**

People with computer background and specialized in security aspects are definitely preferable.

**Documentation Supplied to Personnel**

The Personnel Agreement is included as an Appendix C.

### 7.6 Technical Security Controls

**Technical Security Controls- Key Pair Generation**

For security reasons and to avoid any key compromise, users of the BOCOC CA will not be allowed to generate any key pairs. The BOCOC CA generates both public keys and private keys for end-entities.

**CA Public Key Delivery to Users**

CA certificate is available from its public repositories.

**Key Usage Purposes (As per X.509 v3 field)**

Keys may be used for authentication, non-repudiation, message integrity, and session key establishment. Other key usages are:

- BOCOC CA private key is the only key that can be used for signing Certificates and CRLs.

The Certificate key Usage field must be used in accordance with RFC2459 [2]

**Policy CA Private Signing Key**

The private signing key of the CA must be stored in an isolated machine, within a restricted area and under strict control, using at least a monitoring system.

The key should be in an encrypted form and the activation data for the private key will be in the form of a password. For the activation of the Policy CA Private Key, two persons must be presented.

**Private Key Backup**

A BOCOC CA private key is kept, encrypted, in multiple copies and in different secure locations, on CD-ROMs.

**Public Key Archival**

The public key is archived as part of the certificate archival. Backup copies can be used as an archival service.

**Usage Periods for the Public and Private Keys**

The BOCOC CA has adopted the Constrains for Health Certificate Validity periods as mentioned in to RFC2459 for validity dates and to ISO/DTS 17090 - Part 3, Policy Validity Period [57]

In general the following Validity period for keys will be applied:

- Policy CA public signature verification key (2048 bits) and certificate – Twenty (20) years;
- Policy CA private signing key (2048 bits) – Eight (8) years;
- CA public signature verification key (2048 bits) and certificate – three years;
- CA private signing key (2048 bits) – one year;
- End Entity public signature verification key (1024 bits) and certificate – Twelve (12) years;
- End Entity private signing key (1024 bits) – two years.
- Key lengths must be at least 1024 bits and should be determined in organizational Threat-Risk Assessments.

**Specific Computer Security Technical Requirements**

CA servers include the following functionalities:

- Operating systems are maintained at a high level of security by applying all recommended and applicable security patches;
- Monitoring is done to detect unauthorized software changes;
- Services are reduced to the bare minimum;
- Machines are protected by a suitably configured firewall, intrusion detection, and other spamming control machines.
- The BOCOC CA used for signing certificates isn't connected to any kind of networks, but instead is isolated and monitored.

**Security Management Controls**

The Local Area Network that hosts some of the PKI services i.e. RA services, is checked yearly, for tampering, using strong cryptographic techniques.

**Network Security Controls**

Intrusion detection and firewall were configured to allow requests only through port 80 for http request, and SMTP connections for email requests.

### 7.6 Certificate and CRL Profiles

**Certificate and CRL Profiles-Version Numbers**

X.509 v3.

**Name Forms**

Issuer: C=BOCOC CA, O=HIPPOCRATES-PKI, OU=Authority, CN=BOCOC Oncology CA (2)

The Subject field contains a distinguished name of the entity with the following attributes:

- countryName: "CY"
- organizationName: "HIPPOCRATES-PKI"
- organizationalUnitName: "Personal Certificate" (for personal certificates);
- "Object Signer" (for object-signing certificates)

- localityName: the organization/Hospital where the subject resides;



Other fields are: commonName: name and surname (natural person and object–signing certificates) or DNS name (Digital Processing Entity certificates) and e-mail address of the subject (natural person and object-signing certificates) or of the manager (Digital Processing Entity certificates).

**CRL Profile**

X.509 v2

### 7.7 Specification - Administration

**Specification Administration - Changes with Notification**

Prior to any changes to this certificate policy, the PMAC will notify all entities including subordinate CAs, and all CAs that are directly cross-certified with the Policy CA.

**Comment Period**

The comment period will be maximum 30 days.

**Publication and Notification Policies**

This policy definition, digitally signed by an authorized representative of the CA, is (currently) available in electronic form on the Internet at: http://www.hippocrates.org.cy or via email from cp@hippocrates.com.cy. Other CAs issuing certificates that identify this certificate policy shall post copies of this CP on their CA web site.

**CPS Approval Procedures**

CPS contains information, relevant to the security of a CA, and more specific to this CP. CPS must also be available on line for all Subscribers. The subscriber must accept both the CP and CPS prior to receiving the Certificate. CPS can be found at http://www.hippocrates.org.cy/policies or via an email from cps@hippocrates.com.cy

# Chapter 8

## Conclusions

In today's computing environment where the power of the Internet has opened the doors to a whole new realm of commerce, the need for a "solution" for secure, open and interoperable distributed networking is a must. Many solutions have been considered in order to address these security concerns over the years, but none appear to provide a comprehensive solution, as the necessary trust by the users is still missing. A Public Key Infrastructure (PKI) was proposed to partly address the issue. This offers authentication, privacy, and non-repudiation, which are essential components to building the public's trust [13, 29]. This thesis concentrated on a Health Care PKI System. A detailed analysis of the policies for the implementation of a Health care PKI System for Cyprus's environment was given and contrasted with a number of other overseas PKI implementations. Both the Certificate Policy (CP) and the Certificate Policy Statement (CPS) were based on the RFC 2527 and they were both modified to suit the Cyprus's Environment. The CP issues that were mentioned can be considered as general policies that some CAs can use as a reference to build up their own CPS.

The advent of Health Care PKI System introduces new methods of providing security into unsecured networks and mistrusted areas such as the Internet. As a result of the increasing demand for electronic transactions [58], the need for the adoption of the Health Care PKI System technology by health care organizations is rapidly increasing [58]. Nowadays a Health Care PKI System is the technology that can offer an integrated solution that alleviates the lack of insecure transactions and the fear of "spoofing" by third parties. It also provides the capability for authentication, integrity, and confidentiality, which are not given by any other security systems. A Health Care PKI System guarantees secure communication of individuals through a blend of technology, policy and administrative processes, which enable the exchange of sensitive data in an unsecured environment. This is done through: (a) the use of "public key cryptography" in order to protect information in transit and (b) "certificates" to confirm the identity of a person or entity and establish a trusted relationship.

In addition to this a Health Care PKI System enables a whole realm of key management. The management capabilities of a Health Care PKI System include certificate validation and revocation, key backup and recovery, support for non-repudiation of digital signatures, automatic update of key pairs and certificates, management of key histories, time stamping, and support for cross certification. Each of these capabilities makes the maintenance of a Health Care PKI System easier and at the same time fewer resources are required.

Further to that, the secure distribution of keys through the use of a certificate repository increases the trust within the Health Care PKI System community and makes the electronic communication easier. As a result search requests are able to be serviced efficiently and distributed throughout the network to meet the requirements of even the highest volume of transactions.

However, one of the overwhelming disadvantages of the Health Care PKI System solution is its high cost of implementation, especially the maintenance cost of the CRL [49]. Implementing a Health Care PKI System solution requires a good planning process and the necessary design. Many planned Health Care PKI System implementations failed due to fact that the demanded attention was not shown to sensitive areas like the infrastructure security, training, etc. Its high cost can also be increased if additional maintenance, redundancy and administrative overhead with multiple solutions are considered.

Another disadvantage of the Health Care PKI System is the lack of standards supporting it. While a number of standards have distinguished themselves as the standards to be followed, there are still too many other standards around that have not gained universal acceptance. Only lately ISO, the International organization for standards, and the Internet Engineering Task Force (IETF) have tried to find a solution to this problem by introducing the X.509 standard, which describes a basic electronic format for digital certificates and the Health Care PKI System standard using X.509

The outcome of this thesis was the design and implementation of the Hippocrates PKI system, which is expected to become a general CA for the Health Care Sector in Cyprus. All the hospitals and private health care organizations in Cyprus, whether

these are public or private, can belong to the Hippocrates PKI system. The Hippocrates CPS was derived from the CP mentioned in Chapter five (5) of the thesis. The sub-sections present in the Hippocrates CPS are there either due to small divergences from the general CP or to give specific information and details which a general CP does not cover.

Hippocrates is expected, as far as architecture is concerned, to belong to the Cyprus root CA. The users, i.e. health care professionals and patients need to support and trust Hippocrates for it to be widely adopted. Hippocrates will initially be used as a pilot by the Bank of Cyprus Oncology Center in conjunction with the PASYKAF and the DITIS Project for the benefit of the Oncology Center, all oncologists, and the cancer patients. However, a detailed auditing of all the policies is recommended, prior to its wider deployment. Accreditation from the Ministry of Health and the European Standards Organization is also required. Also a more formal mapping and evaluation of policies will enhance trust on Hippocrates and is recommended for future work.

# Appendix A

## HIPPOCRATES-PKI Certificate Policy (CP)

### 1.0 Introduction

This part of the thesis specifies the procedures indicating the applicability of a certificate, for the operation of a particular community and/or class of application, with common security requirements. It also defines the set of rules, called Certificate Policy (CP), for the operation and management practice of certification authorities (CAs) issuing qualified certificates. Its purpose is to explain how the use of a CP creates the appropriate confidence in certificates, issued by a Certificate Authority (CA), complying with the particular policy. Subscribers and other parties, certified by any particular CA, must have confidence in the applicability of the certificate.

Considering that the health care sector is one of the most crucial sectors, where any patient information is important and any electronic communications between different parties is essential, the provision for secure and trusted systems must be provided.

This CP is customized for health care; it focuses on requirements bound especially to the health care sector. Each Certificate Authority (CA) that will be bound to the health care PKI system in the future is responsible of having its own specific Certification Practice Statement (CPS), which complements this CP. This CP intends on complying with PKIX "Internet X.509 V3 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [1, 5].

### 1.0.1 Overview

The aim of issuing this CP is to define policy requirements on the operation, management, and use of certificates containing public keys for digital signatures so that the assurance of the verification, authentication, data integrity and key agreement mechanisms will be well established. The use of the certificates for any member of the PKI system is well identified by this CP. The members are fully responsible and liable for any divergence of

the specific CP. Certificate holders, who are using certificates, are obliged to consult their CA, in order to obtain further details for the implementation of this CP. This CP identifies specific roles, responsibilities and obligations for management, as well as supervising, and maintaining the PKI, which also assigns responsibilities for registering, and interpreting the specific CP. All assigned duties and responsibilities of this policy shall be reflected in signed agreements between a CA and subscribers. A CA shall instruct Subscribers of their obligations, and of the intended use of certificates issued in compliance with this CP.

Certificates may only be issued under this policy following validation of the Subscriber's identity and of the Subscriber's responsibility and accountability for the certificate Subject. Identification and authentication shall be carried out in the manner set out in this policy. All personal information collected by a CA, and not included in the certificate, may not be disclosed without consent of the Subscriber unless required by law.

Any CA operating under this CP is required to have a Certificate Practice Statement (CPS), which states the practices the CA employs in issuing and managing certificates. It is also required to assign tasks for the Registration Authorities (RAs).

Any dispute concerning key or certificate management under this policy is to be resolved by the parties concerned as stated in this policy.

### 1.0.2 Identification

A unique object identifier for this CP has been assigned following the procedures specified in ISO/IEC and ITU standards. This unique object identifier is part of a standard extension field of the X.509 certificate and specifies whether a particular certificate is suitable for the intended use.

**Certificate Policy Name:** HIPPOCRATES-PKI-DigCertV1.0

**Object Identifier:** 16582 (For General Internet Enterprise Number)

More on Object Identifier can be found at http://www.iana.org/assignments/enterprise-numbers

### 1.0.3 Community and Applicability

HIPPOCRATES-PKI is designed to provide trust within the health care sector. Members of this community can be any organization specialized in the health care sector, i.e. Private or governmental hospitals or clinics, doctors, health care professionals, and patients after the authorized approval from his/her health care professional. Members of the HIPPOCRATES-PKI community shall provide services operating in compliance with this CP.

#### 1.0.3.1 Policy Management Authority Committee (PMAC)

One member of HIPPOCRATES-PKI has the specific responsibility of being the Policy Management Authority of the PKI.

The PMAC is responsible for:

- Registering, interpreting and maintaining this CP,
- Appointing a member of HIPPOCRATES-PKI to serve as the Policy CA for HIPPOCRATES-PKI,
- Approving the CPSs of CAs in HIPPOCRATES-PKI,
- Compliance inspections and general supervision of HIPPOCRATES-PKI,
- Cross-certification with other PKIs and with CAs of other PKIs.

The Bank of Cyprus Oncology Center[7] will act as the PMAC for the HIPPOCRATES-PKI.

#### 1.0.3.2 Certification Authorities (CAs)

A Certificate Authority is a trusted authority in a network that issues and manages security credentials and public keys for message encryption. As part of a PKI, a CA is

[7] State of the art hospital built in Nicosia, Cyprus and specialized in cancer patient treatments. At this point, the system is intended to be used by BOC Oncology Center and DITIS-PASYKAF, always in accordance to Certificate Policy (CP) and Certificate Practice Statement (CPS) guidelines and procedures. In the future, the system is intended to be used by other healthcare organizations and individuals.

responsible for creating and signing certificates, distributing, and revoking digital certificates, binding subscribers, PKI personnel and (where permitted) other CAs to the public signature verification keys attributable to them.
A Certificate Authority acts like a licensing authority. Digital certificates are only issued to users who can prove their identity and credentials to the CA. By using a process called vetting, the CA examines traditional forms of identification before issuing a certificate.

The Certificate Authority assigns responsibilities and duties to the RAs according to the CP compliance and is responsible for providing a Certificate Repository and a Certificate Status Service (CSS).

Depending on the PKI implementation, the issued digital certificate of the CA includes the owner's public key, the expiration date of the certificate, the owner's name and other information about the public key owner along with the publishing of a CPS that includes reference to this CP.

While an organization in the HIPPOCRATES-PKI community may use a contractor to provide (some of its) CA services, it remains responsible and accountable for the operation of its CA.

**1.0.3.3 Certificate Status Checking**

CAs revokes certificates when:

- Information in the certificate becomes unexpectedly invalid
- It is necessary to revoke the PKI privileges of a user

The CA cannot delete the certificate or retrieve it from the user because the certificate is a public document that is used by thousands of PKI participants. Instead, the digital certificate is marked as "revoked" in the CA's database.

PKI users can discover if a digital certificate has been revoked, by looking up the certificate's validity in the CA's database using a process called "real-time online

certificate status checking". By using this process, companies and organizations are always sure that certificate validity information is always fresh and accurate.

Another method of certificate status checking requires PKI users to download a certificate revocation list (CRL), which is simply a list of certificates that have been revoked by the CA. CRLs are generated periodically by a CA.
Unfortunately, CRLs have many disadvantages. Firstly, they can be difficult to download and use. Secondly, nobody is sure that their information is true, because if a CA issues a CRL daily and it revokes a certificate right after issuing a CRL, then the revocation will not be known to PKI users until the next day when the next CRL is issued. Finally if a CA issues a CRL every day, then the users must download the CRL on a daily basis.

Instead of doing all the above work, a real-time online certificate status checking, provides a better solution, by simply making the PKI users look up the certificate's status in the CA's database. This method is fast, easy to use, provides accurate and fresh status information and reduces risk.

**1.0.3.4 Registration Authorities**

Registration Authorities (RA) are primarily responsible for vetting certificate request. Approved certificate requests are sent to a CA and the CA creates the requested digital certificate. Digital Certificates are distributed to users via the RA. RAs are also used to enroll new users into a PKI. New users will apply for a certificate to the RA of their interest. The Registration Authority of the HIPPOCRATES-PKI is operating in compliance with this CP, and is responsible for all duties assigned by the CA and this CP. In some cases the RA may perform duties of more that one CA, provided that in doing so it satisfies all the requirements of this CP.

The advantages of using RAs are:

- With RAs, organizations can set up local or stand-alone enrollment centers at distributed geographic locations. Employees of an international company can be

enrolled into a PKI via RA centers of the country they are living in. Digital certificates will be issued to these employees, by the company's CA, which is located in the company's country.

- Organizations can separate the PKI operations performed by the CA and the RA. This is necessary if the organization wants to separate the certificate request process from the certificate issuing process.
- Requests for digital certificates are sent to the RA instead of the CA, relieving CA administrators of the task of vetting certificate requests.

#### 1.0.3.5 Repositories

All relying parties must be provided by the CA, with a Certificate repository or other certificate validation service. Both repositories and services must comply with the standards stated in the CPS, and must contain the following:

- A copy of this policy and all other policies that affect the issue of the certificate along with all the policies referenced by issued certificates.
- All issued certificates that reference this Policy.
- Any past and current versions of the CA's CP and CPS.
- A Certificate Revocation List (CRL), or a certificate status database that may be accessed online (optional).
- The CA's certificate for its signing key.

#### 1.0.3.6 Sponsors

A Sponsor is an organizational unit or officer with the authority to nominate a person to be a certificate Subscriber.

The Sponsor may suggest appropriate distinguished names for Subjects and is responsible for either supplying or confirming authentication and certificate attribute details to the CA or RA. The Sponsor is also responsible for informing the CA or RA if the sponsor

relationship with the Subscriber has been terminated or changes such that certificates should be revoked.

The PMAC is the sponsor of the Policy CA.

**1.0.3.7 Subscribers (subjects)**

A CA may only issue certificates after receiving approval from the RA. Any HIPPOCRATES-PKI Certificate holder that receives a certificate satisfying all the requirements of this CP, from a CA, is considered to be a subscriber. Subscribers have a legitimate requirement to access, disclose, record, or otherwise manage personal, identifiable health information. Eligibility for a certificate is at the sole discretion of the CA.

According to this, CP Subscribers have been divided into different groups depending on their privilege for access to health information.

**Such groups are:**

- Healthcare Persons: All licensed healthcare professionals or affiliated with licensed healthcare organizations. As a matter of statute, all licensed healthcare persons have health information privileges and responsibilities. This group has the highest privileges among all other groups.
- Nurses: All licensed nurses working in a license health care organization, which is a member of this PKI system, are eligible for a digital certificate.
- Healthcare workers: This category includes all paramedic certified healthcare workers e.g. biomedical engineers, IT, secretaries, and also other persons, who have roles primarily within healthcare organizations. PMAC is responsible for the status of the privilege that shall be given to this group.
- License Healthcare organizations: Includes other licensed healthcare organizations or clinics. Healthcare organizations are eligible for healthcare certificates, which can be used for:

i. Certificate issuance, where the organization wishes to be a CA for its staff;
ii. Authentication of health resources (servers);
iii. Authentication of "role" proxies to provide support for the authentication of a functional group within the organization, where the individual identity of staff members is unimportant to business or practice partners.

Examples of health care organizations include hospitals, Internet health care website providers, and health care research institutions. However, the organizations should be recognized as being legally liable for their activities.

- Patients: this group includes only those patients that have been appointed by the health care professional, as legitimate persons for the issuance of a digital certificate. This group has limited rights and the use of certificates is limited to communications about the subject person's health information.
- Groups: These are collections of persons within an organization that share some common role. Groups may be identified with a system account or NT domain. The Policy makes provisions to issue a certificate to a Group, provided some controls are maintained over the exercise of the related private key.
- Medical Societies i.e. Anticancer Societies. This group includes only licensed medical societies. All legitimate societies are considered as healthcare organizations and their staff is subject to the groups that have been specified above.
- Administrators: Have full rights to maintain, assist members, answer requests, and provide service of the system. Specific rights to administrators of the PKI system are given by the PMAC. Such rights may include different subcategories of administrators such as system maintenance, backup administrator, etc.
- Relying Parties for healthcare certificates are, by definition, persons or organizations that have a legitimate need to access, disclose, manage or otherwise

manipulate personal identifiable health information. Relying parties are themselves eligible for healthcare certificates.

- 

Future Provisions may include also the following categories:

**Application /Devices:** an identifiable computer running software process that is the holder of a private encipherment key

**Supporting organization:** Officially registered organizations that may provide services to a health care organization but which are not providing health care services. Examples include health care financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods

### 1.0.3.8 Subjects

Provided that responsibility and accountability is attributable to the Subscribers as classified in 1.3.7, a CA may only issue certificates where the Subject is the Subscriber, or is an organizational role or an IT system.

### 1.0.3.9 Policy Applicability

This CP is applicable to all PKI authorized members. However, the applicability of certificates issued in compliance with this policy does not rely solely on this compliance, but is critically dependent on involved IT-systems, as indicated in section 2.1.2.3.

## 1.0.4. CERTIFICATE AND CRL PROFILES

### 1.0.4.1. Certificate Profile

Certificates that reference this Policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages, including public keys used for digital signature verification. All certificates that reference this Policy must be issued in the X509 format. CAs should identify in their CPS, the certificate extensions supported and they should state that such support should be

consistent with the Healthcare Certificate Profile detailed in an Attachment to this document.

#### 1.0.4.2 CRL Profile

Any issued CRL by the CA must reference this policy and must be issued in the X.509 version 3 formats. In CRL's it is recommended that the CRLNumber extension and the CRLReason extension be included and well indicated. Finally, the CA's public CPS shall identify the CRL extensions supported.

### 1.0.5 Contact Details

Any future modifications, alterations, interpretation, or maintenance which might be needed will be done once the system is up and running.

Questions concerning this policy should be addressed to: hippocrates@hippocrates.org.cy

### General Requirements

All requirements relating to the obligations of the, CAs, RAs, PMAC, Sponsors, Subscribers, and Relying Parties, and other issues pertaining to law and dispute resolution are clearly stated in this section.

### 1.1.1 Obligations

#### 1.1.1.1 CA Obligations

In the PKI model [48] the CA is the only responsible component for the issuance and general manageability of a certificate, i.e. verification of information contained in the certificate, revocation of a certificate, and renewal. The CA may also take complete control over the application/enrollment process, the certificate manufacture, and the certificate publication. The CA must ensure that all aspects related to services provided by its authority, and all of its operations performed, fully comply with the requirements,

representations, and warranties of this Policy and with the CA's Certification Practices Statement (CPS).

#### 1.1.1.2 The Certificate Authority role over the Registration Authority

The RA always operates in the interest of the CA. The CA's role, over the RA, is to ensure that all RAs operate and act in accordance to relevant provisions of this CP. A CA may not assign the duty of issuing a certificate to an RA.

#### 1.1.1.3 The Certificate Authority role over the Subscribers and Relying Parties

The CA obligations over all subscribers, relying parties, and other certificate holders are firstly, to ensure that all are aware of their respective rights and obligations with respect to the operation of the CA and this CP. Such an obligation should be in the form of a Subscriber Agreement, and with the issuing of a certification and its immediate publication to the repository, the CA should be able to certify that it has issued a certificate to a Subscriber that has entered into a Subscriber Agreement with the CA.

#### 1.1.1.4 Other CA obligations

In accordance with this policy the CA that issues a healthcare certificate, certifies to the subscriber, and to all Qualified Relying Parties, that;

- The CA is obliged to issue the CPS, and due to the fact that the CPS states in detail all the technical, procedural and personnel policies and practices of the CA, according to the requirements of the CP, it must be approved by the PMAC.
- The CA is responsible of managing, and if necessary of revoking the certificate in accordance with this Policy.
- The CA has taken all necessary steps to verify all information in the certificate. The CA guarantees that there are no misrepresentations of facts in the certificate.
- The CA must include in its CPS, the specific measures undertaken to verify all information included in the certificate and articulate the major risks leading to

misinformation, which are not addressed by these measures. If desired, the CA may assert in its CPS, dollar or other limits to its liability.

- The CA guarantees that all issued certificates meet all requirements of this Policy and that they were processed according to the CA's CPS.
- The CA has a safe place to store all the Subscriber's acceptance certificates[8].
- Maintain a CA Repository
- Establish reliable mechanisms and procedures, to ensure that its RAs and Subscribers are aware of, and agree to conditions of this CP that apply to them.
- Establish techniques to recognize any subordinate CA that complies with this CP.
- Ensure the relying parties, by known mechanisms, that all the CA personnel associated with any PKI role must be individually accountable[9] for any actions that will be performed.
- The CA must structure its CPS so that proposed common practices for the PKI as a whole, are easily identified and referred to in the CPSs of subordinate CAs;
- Must establish compliance inspection to be able to verify to the cross-certifying CAs that it complies with this CP.
- Document any agreement with the cross certified CA regarding enhancements and assurances of the operational procedures, restrictions on the usage of the cross-certificate, validity period for the cross-certificate, liability issues, etc.
- Establish mechanisms to inform all relating parties, i.e. subscribers for all the disclaimers available to both CAs.
- Ensure that the CP and the CPSs are publicly available on the CA Web Site
- To prompt upon issuance published CA certificates and other certificates (after Subscriber consent) in the CA Repository
- To ensure access controls for all authorized CA personnel. Ca personnel may need to configure or modify the CA Web Site, CA Repository and CSS.

---

[8] Acceptance Certificate, by the subscriber, states that the Subscriber accepts all obligations under this Policy.

[9] "Individually accountable" means that the CA and RA practices must ensure that there is evidence, which attributes an action to the person performing the action.

- The CA shall provide relevant information about issued certificates when necessary, to aid in resolving any dispute concerning digital signatures
- Establish a certificate status service (CSS) mechanism to Subscribers and Relying Parties. A CA must notify a Subscriber when a certificate, whose Subject is attributable to the Subscriber, is issued or revoked

In general, the CA is responsible for performing all identification and authentication functions as well as all certificate manufacturing and issuing functions. The CA warrants that all of its activities will be conducted in accordance with this Policy.

#### 1.1.1.5 CA- Subscriber Agreement

The CA- Subscriber agreement should include key manageability, key protection, certificate validation, hardware and software relating aspects that are used in the PKI model [48], the certificate policy, and any other policies relating to the model. Procedures for communication between the Subscriber and the CA or RA, should also be included. These procedures include communication of changes in service delivery or changes to this policy, procedures for dealing with suspected key compromise, CA termination, description of the obligation of a Relying Party with respect to use, verification and validation of certificates and finally any limitations of liability as per the definition stated by the PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [1,2] in the user Notice field of the certificate. All responsibilities for the above belong to the CA, which must be sue that all parties are fully aware and fully knowledgeable for their limitations and rights.

The agreement should also specify to subscribers, the minimum requirements for the applications that are to be used with the certificates and services of the PKI. As minimum requirements this policy states that the applications must correctly generate, protect, transfer and use the public and private keys, be capable of performing the appropriate certificate validity and verification checking, report appropriate information and warnings to the Relying Party, be operated in accordance with the IT Security Policy of the Organization. Finally, the Subscriber should, in the agreement, give the CA

consent to collect, for the issuance of a certificate and otherwise for the agreement, necessary personal information about the Subscriber. Personal information collected by a CA, and not included in the certificate, may not be disclosed without consent of the Subscriber, unless required by law.

#### 1.1.1.6 Certificate Status

The CA must inform all the Subscribers and all Relying parties of the Status of their certificates. This will be done in terms of Validation, Renewal, Expiration, and Revocation.

##### *1.1.1.6.1 Validation Obligations*

The CA must establish mechanism that informs all Relying Parties of the certificate status (valid, suspended, or revoked). Some of the acceptable mechanisms are, the distribution of certificate revocation lists (CRL) and an Online Certificate Status Protocol (OCSP) [24].

##### *1.1.1.6.2 Certificate Expiration, Revocation and Renewal*

A CA must ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this CP; and be expressly stated in the Subscriber Agreement, and any other applicable document outlining the terms and conditions of the certificate use.

#### 1.1.1.7 Protection of CA's data

The CA must ensure its personnel and its members, that all operational requirements and all physical and technical securities are applied for the safeness of their private keys and activation data.

#### 1.1.1.8 Restrictions on CA's Private Key Use

A CA must be able to ensure that only its private key is used to sign certificates, CRLs and entries in an OCSS. In case a CA undertakes to act in accordance with other policies, using the same private key or issuing identity, these shall be identified in the CPS.

### 1.1.2 PMAC Obligations

The PMAC will be responsible for the supervision of HIPPOCRATES-PKI system. The PMAC is the sole responsible for the interpretation, maintenance, and registration of this policy. The PMAC has to approve of all the policies and the CPS, before the CA starts its operation. It shall also give further instructions to ensure that the policy CA operates in compliance with this CP and the intentions of the HIPPOCRATES-PKI .

Periodic acceptance and compliance checks of the CA in accordance with this CP have to be done by the PMAC, in order to ensure that the performance of the CAs in HIPPOCRATES-PKI meet all the standards, established in their CPSs, and satisfy all the requirements of this CP.

The PMAC, along with the committee it hires, will be responsible for accepting organizations, hospitals, health care professionals, etc as members of HIPPOCRATES-PKI as far as the applicants meet all requirements specified in the subscribers section.

Prior to the acceptance of other CAs, the PMAC has to validate and approve its CP and CPS. In such cases the PMAC shall be able to include in the acceptance or rejection declaration form, any requirements that may need adding, for the compliance with this CP, for cross-certification or any other reasons for the denial of cross-certification.
The PMAC decides whom to nominate as a Subscriber of certificates. This is to ensure that the subscriber can still work, in case of a debate between a subscriber and organization. The PMAC is also responsible for informing the CA or RA if the relationship between the Organization and the Subscriber terminates or changes such that certificates should be revoked.

### 1.1.3 RA Obligations

Registration Authorities (RA), are used to enroll new users into a PKI. The RA must be in full compliance with this CP and the CPS. The RA is appointed by the CA to perform some of the duties of the CA and must operate on behalf of the CA. If no RAs are appointed, all of the RA obligations turn to CA obligations. In the PKI model [48] the RA is responsible for informing all related parties i.e. subscribers, certificate holders, etc, of all relevant information regarding the rights and obligations of the CA, RA, and Subscriber contained in this CP, the Subscriber Agreement, and any other relevant document outlining the terms and conditions of certificate use. The RA is the only authority that submits subscribers' information regarding an application for a certificate or renewal of a certificate to the CA. However, prior to the submission of any information the RA is obliged to verify the identity and any other given information of that Subscriber and also to verify the authority of that Subscriber in receiving a certificate. RAs must not issue certificates; approved certificate requests are sent to a CA from an RA and the CA creates requested digital certificates. There is no requirement for an RA to notify a Subscriber of the issuance or revocation of a certificate.

In accordance with this policy the RA Obligations also include

- Ensuring that private keys and activation data, used to access and operate RA applications for each person involved in RA duties, are protected in accordance with all security requirements stated in this policy.
- Ensuring that private keys used by RA personnel to access and operate RA applications must not be used for any other purpose.
- Identifying and recording any actions that are carried out by any individual in performance of RA duties

### 1.1.4 Subscriber Obligations

To become part of this PKI model [48] the subscriber must accept this CP and the CPS. The acceptance must be in the form of an agreement, which every Subscriber must enter.

This agreement clearly outlines the obligations of the subscriber and states the terms and conditions of use of the issued certificate, including permitted applications and purposes. The Subscriber must fulfill its obligations as stated in this Agreement.

In the healthcare sector where many health care professionals operate as individuals and others as part of an organization or part of a referring group of people, the subscribers' obligations vary and are depended on the individual situation.

However, standardized obligations are often available, and cover all situations and users. Such obligations are:

- Subscribers must take all reasonable measures for the protection of their private keys, and the prevention from loss disclosure, modification, or unauthorized use.
- Upon any actual or suspected loss, disclosure, or other compromise, subscribers must immediately notify the CA that issued the certificate.
- Subscribers are obliged to use their private keys of Subjects attributable to the Subscriber, only for the purposes identified in the CP

The subscriber must be aware that at any given time the CA or RA may require additional information regarding its membership or its action within the PKI model. The CA or RA may also require, from the subscriber, additional information regarding its application for a certificate. The Subscriber is obliged to submit this information to the required authorities. Any submitted information must be complete and accurate.

Further to the standardized or better to say "general" obligations that individuals, organizations, or groups must follow, there are obligations that are considered separately, depending on the category the subscriber belongs to. These categories are defined depending on whether the Subscriber:

- Is an individual,
- Is an organization acquiring the certificate and managing a private key on behalf of an identified individual,

- Is an organization obtaining certificates where the subject is a named Group.

Obligations of Subscribers who act as individuals:

In such a case the Subscriber Agreement will require that the Subscriber;

- Use the certificate exclusively for authorized healthcare purposes, consistent with this Policy and this CPS.
- Must attend any “individuals” subscribers’ meetings regarding training, problem discussions, and any other additional information.
- Generate a key pair using a trustworthy system, or use a key pair generated in a secure hardware token by the CA or RA and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key.

Obligations in the case where the Subscriber is an organization acquiring the certificate and managing a private key on behalf of an identified individual:

In such a case the Subscriber Agreement will require that the Subscriber;

- Uses the certificate exclusively for authorized healthcare purposes related to the organization.
- States clearly on the certificate that the private key is maintained on behalf of the organization.
- Uses the certificate in such a way so as not to go against the rights of any individual members of the organization. Further, the Subscriber must maintain a log of all use, of the organization’s private key, including the date and time of key use.
- Makes sure that all users of the organizations attend any meetings held between other organizations that are members of this PKI model, to discuss variable problems, and for further training of the applications and the use of the certificate and the private key.

- Generates a key pair using a trustworthy system and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key.

Obligations of an organization obtaining certificates where the subject is a named Group the CA shall require the Subscriber to:

- Generate a key pair using a trustworthy system.
- Clearly indicate on the certificate that the private key is maintained, by a party on behalf of a group of individuals.
- Maintain processes that assure that the private key can be used only with the knowledge and explicit action of current member or members of the subject Group. The Subscriber must detail conditions under which the Group private key may be used. Further, the Subscriber must maintain a log of all use of the Group private key including the date and time of key use and identity of the person or persons invoking the key use.
- It is intended that the Subscriber will place access control mechanisms to insure that only authorized persons are allowed to invoke use of the Group private key.
- Assure that all members of the subject Group have received security training appropriate to the health information functions for which the certificate is issued. Also assure that all members will attend any discussion meetings held between individual groups of the PKI model.

In General, each Subscriber must have explicitly acknowledged, to the CA, the Subscriber's acceptance of the Subscriber's obligations under this Policy.

### 1.1.5 Relying Party Obligations

Prior to the use of the healthcare certificate a Relying Party must ensure that the certificate is appropriate and valid by checking the most recent CRL, other published revocation information, or any other list as specified by the X.509 and PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [1, 2]. The Relying Party

must check if the PKI can be trusted as well as checking that the purpose of issuing the certificate complies with this Policy and the CA's CPS.

### 1.1.6 Repository Obligations

Each CA is responsible for maintaining an on-line repository or other certificate validation service that is available to Relying Parties in a 24-hour period, seven days a week.

This repository shall contain

- All CA-certificates and other published certificates.
- An online certificate status database[10] or an online Certificate Revocation List (CRL) [24].
- The issued certificates that reference this Policy.
- Past and current versions of the CA's CPS or summary of key provisions.
- Copy of this Policy and other policies referenced by issued certificates

### 1.1.7 Liability

This policy ensures that all PKI components [48], including the certification and repository services, issuance and revocation of certificates, and issuance of CRLs, is in accordance with this CP. It also ensures its members that the CA will take all necessary measures to ensure that all RAs and Subscribers will follow the requirements of this policy when dealing with any certificates containing this policy's OID or the associated keys. It also assures that all certificates issued in compliance with this CP, and containing this policy's OID are only relevant for authentication and for the protection of integrity of the transactions, within the approval limits of the organization. Any falsification of the transaction would cause only administrative action for correction and may result in a financial loss. In such a case, the CA has no obligations, and disclaims all liability for any use, other than the intended, as identified by this CP, for certificates issued under this CP. In some cases the CA may make a legal claim for loss of its reputation. The CA assumes no liability for the use of HIPPOCRATES-PKI certificates

[10] Can be access online by use of the Online Certificate Status Protocol (OCSP) or LDAP query

or any associated public/private key pairs in relation to cross-certified CAs and their relying parties.

However the CA is responsible for any damages due to the failure of the CA to comply with the terms of this Policy. The CA is also responsible towards Qualified Relying Parties, for any damages caused to any suitable applications or any loss of information due to this failure of compliance with this policy.

The CA does not guarantee 100% availability of the CA services. The CA informs its members that cases such as yearly services, warranty maintenance, system repair or factors outside the control of the CA, may affect such availability.

Finally the Organization of the CA and its employees makes no representations, warranties or conditions, expressed or implied other than those expressly stated in this CP or its CPS. Any disputes, concerning key or certificate management under this policy, are to be resolved by the concerned parties as stated in this policy with the help of the PMAC.

### 1.1.8 Financial Responsibility

Any financial responsibilities for the use of any of the CA services are weighted to the Organizations, individuals, or any other relying parties of the HIPPOCRATES-PKI. Each member can use a contractor to provide (some of) its CA services, with the only obligation for the contractor, the compliance with this Policy. The cost of such use is also reflected on the individual member.

### 1.1.9 Interpretation and Enforcement

#### 1.1.9.1 Governing Law

The enforceability, construction, interpretation, and validity of this Policy and a CA's CPS shall be governed by the laws of the Republic of Cyprus. Any agreements between

the CA and the members of the PKI MODEL [48] must also be constructed and governed under the Law of the Republic of Cyprus.

#### 1.1.9.2 Severity, Survival, Merger, Notice

Any agreements by the CA must ensure that it will contain appropriate provisions governing severity, survival, merger or notice.

#### 1.1.9.3 Dispute Resolution Procedures

Disputes are classified into two categories. The ones, within the organizations, that concerns key and certificate management, and the ones that are between Organizations of the HIPPOCRATES-PKI system. For both situations disputes arising from this Policy or the CA's CPS, unless precluded by governing laws or other agreements, shall be resolved pursuant to binding arbitration, in accordance with the procedure and mechanism the PMAC will establish. If a Relying Party of a Subscriber submits a dispute to the PMAC, the PMAC is obliged to investigate all relevant situations prior to its decision. All disputes should be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved in the Court in accordance with the Laws of the Republic of Cyprus. Prior to resolving of the dispute in the court, the PMAC, being the only committee that can take decisions for the revocation, renewal, or approval of a certificate, can cooperate closely with the organization or individuals in resolving any disputes.

A dispute relating to key and certificate management within an Organization shall be resolved by the appropriate organizational authority in conjunction with the Issuing CA. Each CA must ensure that any agreement it enters into, provides appropriate dispute resolution procedures.

### 1.1.10 Fees

This CP along with the CPS, that supports the CP, will be available on line at no charge.

### 1.1.11 Publication and Repository

According to this policy, and the CA's CPS, each CA must provide an on-line information utility that will be available to Relying Parties and will contain:

- All the CA documents and all other policies related to this PKI model.
- A CA Repository for publishing certificates and CRLs. The CA Repository must comply with all Repository Obligations mentioned previously.
- This CP as a full text version and its CPSs referencing this policy, digitally signed by an authorized representative of the CA. This is needed, first to inform its members or any prospective members, but it will also be necessary for the purposes of any audit, inspection, and accreditation or cross-certification.
- A yearly compliance inspection report that is prepared from the PMAC.
- Irregularities found by the external inspectors.

The on line information will be provided via the RA.

#### 1.1.11.1 Frequency of Publication

Any information available to the CA must be published in the repository within 72 hours. Certificates issued by the CA referencing this Policy, will be published within 48, upon the receiving of the certificate from the Subscriber. Any information related to this policy that affects the operation of the CA, i.e. information regarding revocation of a certificate, obligations, etc., must be available to the Subscriber immediately after the modification or alteration of this policy.

### 1.1.12 Compliance Inspection

External auditors must inspect the CA and RA performance prior to the initiation of their operation. Thereafter external auditors must check and inspect, at least once a year, the compliance of the standards established in its CPS with this CP and all other relevant

policies, as well as the performance of the PKI components. A compliance inspection report must be available on line to all subscribers and must be prepared by the PMAC.

#### 1.1.12.1 Inspector Obligations

- To inspect whether the CPS outlines - in sufficient detail - the technical, procedural and personnel policies and practices of the CA.
- To inspect whether the CPS meets the requirements of all the CPs supported by the CA.
- To check the compliance of the PKI components [48] with this CP.
- To inspect the performance of the CA and the CA compliance with the CP.
- To supply the PMAC with any information that regards the compliance and performance of the PKI components with this policy.
- To specify sufficient reasons to the PMAC why the CA has not complied with its CP at all times and state any periods of non-compliance.

#### 1.1.12.2 Inspectors Identity and Qualifications

External inspectors must have sufficient knowledge of the PKI technology and cryptography techniques. External inspectors must also have knowledge of the operation of the relevant PKI software and the operation of the PKI components [48] in accordance with this policy.

#### 1.1.12.3 Actions Taken as a Result of Inspection

In cases where the CA or any other compartment of the PKI model [48] does not satisfy or comply with this policy or the CPS that is published in accordance with this policy, the PMAC must request immediately the relevant component (CA, RA, etc.) to make the appropriate modifications so that all irregularities may be corrected. However, no PKI component [48] should stop its operation until the next programmed inspection. Operation shall discontinue according to the actions taken in the case of severe irregularities and in previous responses to problems. Any irregularities found must be published so that Subscribers must be aware.

### 1.1.13 Confidentiality Policy

Any information regarding subscribers, which is submitted on applications or after the necessary investigation to identify the submitted applicant information, is confidential and belongs to the Subscriber. This information will be kept confidential by the CA, shall be used only for the purpose collected, and such information shall not be released without the prior written consent of the Subscriber, unless otherwise required by law. With prior consent of subscribers, such information may be published in public directories. Moreover, the private key of each Subject is to be held only by its Subscriber and must be kept confidential by them. Any disclosure by the Subscriber is at the Subscriber's own risk.

Alternatively, CA Certificates, CRLs, and personal or corporate information, appearing on them and in public directories, are not considered sensitive.

## 1.2 Identification and Authentication

### 1.2.1 Initial Registration

Subject to all requirements stated under this security policy, below, the certificate applications will reach the RA

- Via the electronic way, over a secure channel such as that provided by SSL / TLS or other suitably encrypted channels, using the public Internet.
- Or an, in person, application directly to the RA.

#### 1.2.1.1 Types of Names

According with PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [1, 2] the following must be applied:
The subject name (for certificate applicants) must have a distinguishable and unique Distinguish Name (DN) in the certificate subjectName field. The DN must not be blank.

In accordance with the RFC 2459, each Subject may have alternative names in the subjectAltName extension field, only if the CPS states whether an alternative name of a particular form shall be included in the certificate.

Each subjectName field shall include a “CN=” component that specifies designation of the qualifying professional license or credential (e.g. MD The use of professional designations is limited to certificates issued to Independent Practitioners, in which case use of such designation is mandatory. In the case of an organization, the name should reflect the legal name of the organization.

Relying party implementations should be prepared to receive such standard credential designations in subject names.

For certificates issued to members or patients, the subject DN must include an “OU=patient” or “OU=member” designation and include the name of the hospital, clinic, or center in the “O=” component of the DN.

The DN for certificates issued to organizations in order to secure servers, must include the name of the server in the “CN=” component. This name shall be of a form: <machine name>. <Domain name> and the name of the Organization in the “O=” component.

The DN for certificates issued to a Group must include the name of the group in the CN component as follows: “CN= GROUP$ <group name>” and the name of the parent organization in the “O=” component.

**1.2.1.2 Name Meanings**

The contents of each certificate subjectName and issuerName must have a reasonable association with the authenticated name of the Subscriber. It is also recommended that the organizationName component be included in the DN and that it should be the official name of the Organization.

The subject name must be listed in a certificate. In the case of individuals this should be a combination of first name and/or initials and surname.

Where subject private keys are not under the exclusive control of the subject and are managed by an organization, that organization's designation must be included in the "O=" of the Subject DN.

#### 1.2.1.3 Rules for Interpreting Various Name Forms

In the CPS, the CA stipulates how names are to be interpreted.

#### 1.2.1.4 Name Uniqueness

The DN subject listed in a certificate must be unique among all Entities of a CA. For each Entity, the CA may issue additional numbers or letters to the commonName to ensure the uniqueness of the DN. The CA may issue multiple certificates, each with distinct key usage, to a single subscriber.

#### 1.2.1.5 Verification of Key Pair

The identities of both the Subscriber and the issuing certificate must be confirmed before the certificate is issued. The method that proves the possession of their respective private keys, should comply with current standards as stated in the CPS. In the case where the Subscriber is not the certificate subject, the CA, either directly or through its agents (RA), should ensure that the individual or organization has established appropriate security mechanisms, to ensure that the person, group, server or process identified as the certificate subject, controls any private key use identified with the certificate.

#### 1.2.1.6 Authentication of Organization

When an RA receives a certificate application from an organization, it has to be examined via methods that comply with this Certificate Policy. For the application to pass this examination, the RA has to ensure that:

- The organization exists and is qualified as per this Certificate Policy to be a Subscriber of a part of the Health Care CA.
- That the certificate application was signed by an authorized representative of the organization.
- That the information contained in the certificate application is correct.
- Any additional business information such as legal name, type of entity, names of officers, addresses, phone numbers as well as any national payer or provider identifier, are provided.

#### *1.2.1.6.1 Authentication of non Healthcare Organizations acting as agents*

Organizations that do not belong in the Healthcare Sector, but are agents or business partners of healthcare organizations, are not allowed at the moment to receive a certificate. However, any business partner they may have qualifies for a certificate, if it complies with this CP.

### 1.2.1.7 Authentication of Individual -- Independent Practitioner

Licensed healthcare persons may be authenticated by a variety of mechanisms depending upon the relationship between the CA and / or RA and the applicant. However, in every case,

- The measures will be taken by the RA, in order to confirm that the certificate request originated from the Subscriber. These measures will be briefly described at the CPS and will be taken through non-electronic means, such as by contacting the Ministry of Health, the Subscriber, and the National Medical Committee.
- The RA shall verify the currency and good standing of the qualifying license.
- The RA shall also obtain and maintain a physical copy of a certificate application, containing the handwritten signature of the applicant. This application shall include appropriate evidence concerning the accuracy of the provided information and an acknowledgement that a fake application may result in the prosecution of the applicant.

#### 1.2.1.8 Authentication of Groups

As with the case of the authentication of Organizations, the RA has to make the same verifications and measures to confirm that the applicant group complies with this CP However, in order for the RA to proceed with the acceptance of the application, in this case, the subscriber Group has to designate one or more Responsible Individuals, and authorize them to represent the Group. The designated persons will act on behalf of the group and will be the leaders as far as checking, if the group complies with the CP and the CPS, is concerned. They should also be able to verify and confirm all identities of the people of the group, and to manage keys on behalf of the Group.

### 1.2.2 Renewal Applications

Subscribers are obliged to inform the RA, who originally registered them, of the expiration of their Healthcare Certificate two months prior to the scheduled expiration of the operational period of the certificate, provided the original certificate has not been suspended or revoked. A request by subscribers may be made electronically via a digitally signed message generated with the Subscriber's private key, corresponding to the public key contained in the original certificate or by a hand written message signed by the subscriber and containing a copy of the Subscriber ID. Organizations are only obliged to apply for a renewal via the electronic method. Renewal certificates must be issued without re-keying. Renewal with re-keying requires re-authentication of the subscriber by the RA just as with a first time application.

Prior to re-issuance, the RA must once again confirm the accuracy of information contained in the certificate just as with a first time application.

Depending on the Subscriber, the CA and RA may assign different validity periods for their Certifications, which Subscribers must follow. The maximum validity period shall not exceed the remaining validity period of the subscriber’s qualifying license. Finally, the certificate validity period must not extend past the validity period of the CA's signed certificate.

### 1.2.3 Re-key after Revocation

Revoked or expired certificates shall not be renewed. Applicants whose certificates have been revoked due to a compromise of private key or expiration should apply for a certificate just as with a first-time application. In this case, all measures for the validation, examination, and other procedures for the identification and the compliance of the Subscriber with this CP and the CPS will be taken. After revocation a re-keying and a new certificate will be issued.

### 1.2.4 Revocation Request

A revocation request may be submitted electronically in such a way so as to prevent unauthorized revocation requests, but at the same time not compromising how quickly the process can be carried out, in case the need to quickly[11] revoke certificates arises. For Groups, certificates may be revoked upon request by the Responsible Individuals representing the Group.

### 1.2.5 Types of assurance

Types of assurance should be well specified in the CPS.

## 1.3 Operational Requirements

This section specifies the requirements imposed, upon issuing CA, subject CAs, RAs, or end entities with respect to various operational activities.

### 1.3.1 Application for a Certificate

An applicant for a certificate must complete an application form either online from the RA website or by downloading a printed version of the form and completing it in hand writing. Hand Written applications shall be delivered to the RA with all needed information. In the case where the applicant is not the Subscriber, proof of authorization to act on behalf of the prospective Subscriber is required.

[11] In cases that Subscribers have lost their keys

Upon the acceptance of an application from the Subscriber, the CA must proceed with measures and mechanisms to ensure that the application is accompanied by the correct information as stated in the CP and the CPS.

The objectives of the measures should be:

- To prove the identity of the Subscriber in the case of an Independent Practitioner,
- To check if the organization or hospital is qualified for a certificate according to this CP, that a representative of the organization has given written proof of authorization when the applicant is not the Subject, and for proof of authorization that the signature of the Subject is attributable
- To confirm that the applicant group complies with this CP and that designated persons will act on behalf of the group
- To check if the Subscriber has understood the policies as stated in the CP and accepts the obligations as articulated in the Subscriber Agreement. For this reason the CA shall check whether the Subscriber has signed the Subscriber Agreement.

All applications are subject to review, approval and acceptance, by the CA, and the decision of whether to issue a certificate is at the sole discretion of the CA.

### 1.3.2 Application for a Cross-Certificate

Some entities may trust and own certificates from different CAs. In that case Cross certification is used to create the certificate between two CAs, and to minimize the certificate path between two subjects, when both CAs trust each other.

The future need of a Cross Certification must be taken in to account. For this reason, and in addition to all mechanisms and procedures stated above, when a CA encounters a request for cross-certification within the health care CA, this must be accompanied by its CP, the CPS, and a report mentioning the representatives, the managers, and all authorized personnel of the CA. The CA is allowed to hire an external inspector to

validate that the CA satisfies the requirements of its CP. All applications are subject to review, approval and acceptance by the CA and the decision of whether to issue a cross-certificate is at the sole discretion of the CA.

### 1.3.3 Certificate Issuance

Upon successful completion of the Subscriber identification and authentication process, in accordance with this Policy, and the complete and final approval of the certificate application, the CA shall issue the requested certificate.

All Subscribers will be notified of the final approval and the issuing of the certificate and arrangements will be made by the CA so that the certificate will be picked up by the Subscriber or the designated persons of the groups or the organization. The certificate will not be published by the CA until it has been accepted by the applicant. Subscribers should notify the CA when they receive the certificate.

If the Subscriber has not notified the CA for the acceptance of the certificate within 30 days of issuance, the certificate shall be revoked. The CA, in its CPS, may set a lesser time limit.

In the case of an organization or a group the designated responsible person is obliged to deliver the certificates and inform the CA of the delivery. In every circumstance, the Responsible Individual must take steps to assure that the users have accepted responsibility for its use.

### 1.3.4 Certificate Acceptance

The subscriber is required to indicate acceptance or rejection of the certificate to the CA, in accordance with procedures and within a time frame established by the CA and specified in its CPS. If the Subscriber does not indicate acceptance within the maximum time period, then the certificate shall be revoked. Certificate acceptance can be

accomplished through electronic means with a digitally signed document using the issued certificate's related private key.

### 1.3.5 Certificate Suspension and Revocation

A certificate will be revoked by the CA immediately, at any given time, if the CA suspects or realizes that the Subscriber, organization, group, or any member of the group has failed to comply with obligations set out in this CP, the CPS, the Subscriber Agreement, or any applicable policy and law. RAs have a duty to inform the CA if they become aware of inaccuracy of the subject information in the certificate.

Revocation of a certificate will also take place if any of the information in the certificate changes and is no longer true, upon request by the Subscriber[12], If the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS, when the subscriber delays the indication of the acceptance of the certificate, and when the PMAC in its discretion instructs an issuing CA to do so, a certificate will be revoked. Finally, in the event that the CA ceases operations, any certificate issued to and all certificates issued by the CA shall be revoked prior to the date the CA ceases operations.

#### 1.3.5.1 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- The Subscriber in whose name the certificate was issued
- The designated responsible individuals of the group or the organization that are authorized to represent the group and the organization
- The issuing CA or its delegate RA.
- The PMAC

The revocation of a CA-certificate may only be carried out by the CA, on whose behalf the CA-certificate was issued

[12] A Subscriber may request revocation of the Subscriber's certificate at any time for any reason.

#### 1.3.5.2 Required Revocation

A Subscriber or the designated responsible individual of the group or the organization must promptly request revocation of a certificate:

- Whenever any of the information on the certificate changes or becomes obsolete.
- Whenever the Subscriber suspects that someone else is using the certificate or the private key assigned with it.
- Whenever the Subscriber loose his private key.

#### 1.3.5.3 Procedure for Revocation Request

A certificate revocation request should be sent to the issuing CA as soon as possible after recognition of compromise or false subject information. This can be done through the authorized RA electronically and only if it is digitally signed with the private key of the Subscriber, or the Responsible Individual. Alternatively the Subscriber, or Responsible Individuals, may request revocation by contacting the CA or RA authorized personnel and providing adequate proof of identification. The CA must also ensure that these procedures and any additional procedures and requirements with respect to revocation are set out in the CPS. All authenticated revocation requests, and any resulting actions taken by the CA, must be recorded and retained. When a certificate is revoked, full justification for the revocation must also be documented.

#### 1.3.5.4 Certificate Status or CRL Update

After revocation, the CA should update its applicable certificate status databases and should publish the certificate in the next CRL it issues. However, an On-Line Revocation/Status Checking Availability may also be available for the certificate status. In this case such a database shall ordinarily be updated, promptly after revocation or suspension.

#### 1.3.5.5 Revocation Request Grace Period

Requests for revocation should be processed according to the order in which the requests are received. In the case that the Subscriber suspects that someone else is using the certificate or the private key assigned with it or whenever the Subscriber looses his private key requests must be processed immediately. The CA should state in its CPS the maximum time within which it will process certificate revocation requests.

#### 1.3.5.6 Certificate Suspension

Certificates should be suspended by the CA, if the CA suspects unauthorized use of the certificate, and should proceed with further investigations. Also upon notification of a temporary change in employment status of the Subscriber, this may result in the restriction of the Subscriber's rights to access health information for that time.

During suspension, a temporary[13] healthcare certificate may be issued to the Subscriber, if the subscriber is otherwise eligible for new issues of such a certificate. Upon removal of the first certificate from suspension, the interim certificate must be revoked.

Certificate suspension may be supported by including the certificate in the CA's CRL with the CRLReason code specified as certficateHold with hold instruction id-holdinstructon-reject. A certificate is subsequently removed from suspension with a CRLReason entry removeFromCRL.

#### 1.3.5.7 CSS Publishing Frequency

All updates of the CRL should be in accordance with the time specified in the CPS. However, CRLs shall be updated at least every 24 hours to ensure that the most recent CRL is available to Relying Parties.

[13] Temporary means with Limited Valid License Period

### 1.3.6 Computer Security Audit Procedures

All system components activities, i.e. logins, file access, requests, that are accessed by the Subscribers and may influence the outcome of issuing processes for certificates issued in compliance with this CP, the CRL, and any outcome of the Cross certificates, along with all events related to the security of the system, should be automatically recorded in audit trail files. The CA should establish procedures for the regular review of these files, with respect to potential security incidents.

#### 1.3.6.1 Types of Event Recorded

All logs should contain all the action taken by the Subscriber, the date and time of the actions, and the identity of the Subscriber, who caused the action.

#### 1.3.6.2 Frequency of Processing Audit Log

A CA must ensure that CA personnel, as specified in the CPS, review its audit logs and that all significant events are explained and documented in an audit log summary. All actions taken following these reviews must be documented and signed.

#### 1.3.6.3 Retention Period for Audit Log

Recent audit logs must be retained for a time limit specified in the CPS, but no longer than thirty days for external inspection, in case that is needed.

#### 1.3.6.4 Protection of Audit Log

All audit log files must be protected from unauthorized viewing, modifications, and deletions. Manual audit information must be protected from unauthorized viewing, modification and destruction.

#### 1.3.6.5 Audit Log Backup Procedures

Backups at regular times shall be made for all audit logs and audit summaries.

#### 1.3.6.6 Audit Collection System

A CA must ensure that the CPS specifies what information is logged.

#### 1.3.6.7 Vulnerability Assessments

All audits are made to check the future vulnerabilities of the systems. As a result the CA must ensure that vulnerability assessment is performed, reviewed and revised following an examination of these monitored events.

### 1.3.7 Records archival

Retention of records and storage media are often a legal requirement. Therefore, the CA is obliged to maintain a suitable archiving and record retention procedure.

#### 1.3.7.1 Types of Records Archived

The CA must ensure that the archiving of the following records / information is performed at regular time intervals.

- The CP, the CPS, and all other related policies.
- All applications for certificate and all accompanying information with the application regardless if the application was accepted or not.
- All generated certificates and all information stored at the CRLs during regular times, including the status of the certificates.
- All correspondence and contracts between the CA and RAs and the Subscribers.
- Signed certificates and Key histories.
- All computer security audit data.

All this information should be given to all Subscribers and Relying Parties at any given time upon their request. Such requests must be specified with a relevant purpose prior to the delivery of the information. All requests shall be made electronically via the website.

### 1.3.8 Issues of Access Archiving Data

The CA must be aware of some pitfalls posed by obsolete or redundant storage technologies, limiting the ability to access data. For example, the CA must take measures to avoid a situation in which it is not possible to read information stored on "old" media, i.e. old tapes, because of the adoption of more modern techniques and technologies for storage.

However, the CA must ensure that all of its records are safeguarded properly and are not inadequately stored, something which would result in the data being more susceptible to modification, deletion or corruption, thereby destroying the integrity of the contents.

#### 1.3.8.1 Retention Period for Archive

In the health care sector, in general most of the health care organizations retain all patient records for at least 7 years. Accordingly, the Health Care CA must establish mechanisms to ensure the retaining of the audit information, Subscriber Agreements and any inspection, audit, application, identification, authentication, acceptance and revocation information for at least seven years. However, all issued Certificates, and CRL data generated by the CA, must be retained for at least one year after the expiration of the key material.

#### 1.3.8.2 Protection of Archive

The integrity and availability of archive media must be ensured and protected. An extra copy of the retained back up must be stored in a location other than the CA site and must be protected by either physical security alone, or a combination of physical and cryptographic protection. However, if encryption has been used to ensure the protection of sensitive records any future access to the material may be jeopardized, if the CA does not take measures to avoid the reduction of control over the cryptographic Keys.

#### 1.3.8.3 Integrity of the Backups

A CA should establish those mechanisms that periodically verify the integrity of the backups. In the case that any data is found to be corrupted or damaged in any way, it should be replaced with the other copy held in the separate location as soon as possible. The CA should also ensure availability of the archive and that archived information is stored in a readable format during its retention period, even if the CA's operations are interrupted, suspended or terminated. In that case the CA should end notification to all subscribers to ensure the continued availability of the archive.

#### 1.3.8.4 Archiving and CPS

Any further details that subscribers need to know should be referred to them through the CPS.

### 1.3.9 Disaster Recovery Plan

The best way to prepare for a disaster is to avoid the disaster. Today's IT Systems are even more vulnerable to a variety of disruptions, i.e. disk failures, power outage, fire, terrorist actions, etc. For these reasons, the CA must have in place an appropriate disaster recovery and business resumption plan in order to ensure its availability and maintain its uptime as high as possible. This plan must explain step by step the procedures that need to be followed to re-establish the usual operation of the PKI system. However its maximum allowable downtime must be stated in its CPS. Also the selected technological framework should allow provisions that ensure the system's availability. Finally, the disaster recovery plan must be documented by the repository so that all parties will be aware of its procedures.

### 1.3.10 Key Changeover

A Subscriber, the CA, or the RA may initiate the key changeover process. Automated key changeover is permitted. A CA must ensure that the details of this process are indicated in its CPS.

Subscribers without valid keys must be re-authenticated by the CA or RA in the same manner as the initial registration.

When a Subscriber's certificate has been revoked as a result of non-compliance, the CA must verify that any reasons for non-compliance have been addressed to its satisfaction before certificate re-issuance. Keys may not be renewed using an expired digital signature key.

New Policy CA keys shall be generated and a new self-signed CA certificate shall be issued at least three months before the expiration of the old private CA key.

### 1.3.11 Entity Public Certificate Is Revoked

In the case that a revocation of a CA's certificate is needed, the CA, according to this policy, and as briefly described in the CPS, must notify the followings parties;

- The PMAC
- All of its subordinate CAs, if any;
- All CAs with whom it is cross-certified, if any;
- The RAs;
- All Subscribers.

The CA must also publish the certificate serial number to the CRL, revoke all CA-certificates signed with the revoked certificate.

After addressing the factors that led to revocation, the CA may generate a new CA signing key pair, re-issue certificates to all Subjects and ensure all CSS entries are signed using the new key.

#### 1.3.11.1 Entity Key Is Compromised

The CA must request immediate revocation of its certificate, in the event of compromise of its private key. In such a situation, the CA has to revoke all certificates issued, using that key, and provide all Relying Parties with an appropriate notice.

The CA will be eligible to start to re-issuing certificates to all Relying parties only after it has generated a new CA signing key pair and receives the new, requested CA certificate. In the event of the compromise, or suspected compromise, of any other Entity's private key, the Entity must notify the CA immediately.

### 1.3.12 CA Termination

A CA ceases its operations only at the point where all services associated with a logical CA are terminated permanently. In the event that a CA ceases operation, all Subscribers must be notified immediately upon the termination of operations. The issuer of any signed certificates, all its subordinate CAs, all CAs with whom it is cross- certified, and all other known Relying Parties, should also be notified. All certificates issued by the CA that reference this Policy, will be revoked no later than the time of termination and the CA must take all necessary measures to arrange for the continued retention of the CA's keys and information.

#### 1.3.12.1 CA Change of Management

In the event of a change in management of a CA's operations, the CA must notify all Entities for which it has issued certificates, all CAs with whom it has cross-certified, all Subscribers, and the PMAC members.

#### 1.3.12.2 CA transfer of Operation

In the event of a transfer of a CA's operations to another CA, operating at a lower level of assurance, the certificates issued by the CA whose operations are being transferred

must be revoked through a CRL, signed by that CA, prior to the transfer. All archives should be retained for all the time specified in the CPS.

#### 1.3.12.3 Physical, Procedural, and Personnel Security Controls

Due to the importance of information and data, as well as the expenditure of the hardware components that a PKI system is consisted of, both the RA and the CA site must ensure that all security controls concerning aspects such as physical security, Trusted Roles, identification, and personnel training, are in place.

### 1.3.13 Web Server Database Connectivity

The CA will have to connect to the RA's database. Therefore, the technology must support authentication and encrypted data flow from and to the DBMS.

## 1.4 Physical Security -- Access Controls

Both the CA and RA shall implement security controls in order to ensure that access to the sites is limited only to authorized personnel, listed in the access list. For this reason security personnel shall monitor and inspect the site on a 24 hours a day, seven days a week basis. Monitoring shall be done via electronic media and through periodical inspections of the Computer Hardware and Software components of the system, in order to ensure the integrity of the data and the equipment. Electronic monitoring shall be done through a close control monitor system, whereas for periodical inspections a log file shall be used to record the time of the last inspection. The security personnel will be obliged to record the time of login and logoff of all authorized personnel. The security personnel must also escort all visitors and keep a log file with their identifications. The log file shall be inspected periodically and the inspection procedure shall be well defined in the CPS.

In the case of the RA, security access controls may be varied due to the fact that candidates for a certificate as specified in this policy are allowed to deliver Hand Written applications. In this case, and in order for the RA to ensure its integrity and avoid any

contact of the candidate with the machines, different personnel shall be responsible for the acceptance of the application forms.

### 1.4.1. Other Physical Security Aspects

The CA must ensure that

- All removable media and paper containing sensitive plain text information such as keys for signing certificates and CRLs, are stored in a secure container or safe.
- The operation of the RA site provides appropriate security protection of the cryptographic module and the RA Administrator's private key. The CA must conduct a threat and risk assessment. For example, the cryptographic module and the RA Administrator's private key could be stored in a secure container or safe.
- Any software or hardware that supports the functions of Responsible Individuals shall be appropriately protected

### 1.4.2 Procedural Controls

Trusted Roles are assigned to all personnel, who according to this policy and the CPS, have access to or control cryptographic operations, which may affect the global operation of the CA in the matters of CA's issuance, use, revocation of certificates, and any other CA operations i.e. CRL. According to this policy this personnel list may include employees (such as system administration personnel, operators, and engineering personnel), contractors, consultants and executives who are designated to oversee the CA's operations of the CA. Finally, individual Trusted Roles may be assigned by both CA and RA.

#### 1.4.2.1 RA Trusted Roles

All RA personnel must understand their responsibility and their role for the identification and authentication of prospective Subscribers and perform the following functions:

- Acceptance of requests for certificates, certificate change, and revocation;
- Authentication of an applicant's identity;

- Transmission of applicant information to the CA;
- Provision of authorization codes for on-line key exchange and certificate creation.

#### 1.4.2.2 CA Trusted Roles

All CA personnel must understand their responsibility in ensuring the integrity and the high availability of the system. For this purpose a separation of duties for critical CA functions, in order to prevent one person from maliciously using the CA system without detection, is needed. This separation will cover at the minimum the duties of day-to-day operators, system administrators, managements, and auditors of the system. Of course any different arrangements of separation of duties may be acceptable, provided the brief description of the roles in the CPS.

CA Security Managers role includes:

- Assigning security privileges and access controls of CA Operators and System Administrators
- Review of the audit log to detect CA Operators' compliance with system security policy

CA Operator role includes:

- Configuring CA security policies;
- Creation, renewal or revocation of certificates;
- Generating, distributing, and otherwise managing CRLs

CA System Administrator role includes:

- Configuration and maintenance of the CA system hardware and software;
- Creating emergency system restart media to recover from catastrophic system loss;
- Performing system backups, software upgrades and recovery, including the secure storage and distribution of the backups and upgrades to an off-site location.

Only these personnel should have access to the hardware and software that controls the CA operation.

CA Auditors role includes

- Verification of audit logs;
- Verification of CP and CPS compliance;

#### 1.4.2.3 Identification and Authentication for Each Role

Prior to the inclusion of any CA personnel to the Access List, the CA must establish proof of their identity and validity of their information. For the personnel that is included in the Access List the CA must

- Give a Certificate for the performance of their CA role.
- Give them an account on the CA system.
- Notify all Security Personnel for physical access to the CA system.

Certificates and Accounts must:

- Be directly attributable to an individual
- Not be shared
- Be restricted to actions authorized for that role, through the use of CA software, operating systems and procedural controls.

CA operations must be secured. For these reasons mechanisms such as token-based strong authentication and encryption, when accessed across a shared network, may be used.

#### 1.4.2.4 Multiple Roles (Number of Persons Required Per Task)

The need of multiple roles among the different PKI systems is a must, not only to ensure that no single individual may gain access to Subscriber private keys stored by the CA, but also to ensure the high quality of services and proficiency. The CA must ensure that for

operations such as Key Recovery or Key generation a multi user technique, preferably using a split-knowledge technique, such as twin passwords, must be performed.

Multiple Roles are also useful, because of the fact that not only one user is appointed and eligible for one task, but more. This gives flexibility to the user and to the CA not to depend on the knowledge of one person only.

### 1.4.3 Personal Security Controls

A CA must ensure that all personnel that are related with any duties with respect to the operation of a CA or RA must:

- Be appointed in writing;
- Be bound by contract to the terms and conditions of the position they are to fill;
- According to their contract, not disclose any sensitive CA security-relevant information or Subscriber information;
- Have received comprehensive training with respect to the duties they are to perform;
- Not be assigned duties that may cause a conflict of interest with their CA or RA duties.

#### 1.4.3.1 Background and Qualifications

All personnel must be unquestionably loyal, trustworthy and characterized by integrity, and should have demonstrated security consciousness and awareness in his or her daily activities. All personnel should be able to perform its duties with caution and according to this CP and the CPS. The CPS must describe any other different requirements to the above special requirements needed by the CA.

#### 1.4.3.2 Training Requirements

All personnel that are related to any duties, with respect to the operation of a CA or RA, must receive comprehensive training. The training will include:

- The CA/RA security principles and mechanisms;
- This CP and the CPS
- All PKI software versions in use on the CA and RA system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures.

Refresher training and seminars will be held in order to ensure the high quality of knowledge and also to ensure the updateability of the personnel as regards to any changes of the system or this CP.

#### 1.4.3.3 Documentation Supplied to Personnel

This CP and the CPS, along with all relevant documentations regarding the policies of the system, must be made available to the CA and RA personnel. The CA should ensure that all personnel receive all relevant information along with the acceptance of their contract. All personnel should sign a statement, stating that the person identified has been informed and acknowledged their understanding that certificates issued under this Policy should be used to facilitate appropriate access to personal health information and that such data is protected and any inappropriate acquisition and misuse may lead to a criminal penalty.

### 1.4.4 Security and Confidentiality

Due to the nature of the system, security and confidentiality are critical factors affecting the selection of the technological framework. The selected framework must provide the ability to authenticate and encrypt communication and to control access to the system's components and resources.

## 1.5 Technical Security Controls

This section contains provisions of the public/private key pair management policy for CAs, RAs and end entities, and the corresponding technical controls.

### 1.5.1 Key Pair Generation

Subscribers will not be allowed to generate their own key pairs. Keys will be given to them by the CA, using an approved software or hardware component. Hardware and software components must be evaluated and all their capabilities must be checked to see if they meet the technical specifications. However, key pairs for CA and RA must be generated in such a way that use of the private key, at all times, remains under the control of the authorized authority.

#### 1.5.1.1 Subscriber Public Key Delivery to CA

The Subscriber's public key must be transferred to the RA, which will store it to the CRL database. The CA in a way must ensure that:

- The key has not been changed during transit.
- The sender possesses the private key that corresponds to the transferred public key.
- The sender of the public key is the legitimate user claimed in the certificate application.

#### 1.5.1.2 Private Key Delivery to Entity

The private key should be delivered in hand to a physical person after proof of their identity. Guidelines should be given for the protection of the private key. Private keys prior to the delivery should be encrypted with a minimum of an 8-bit password.

#### 1.5.1.3 Public Key Delivery to Certificate Issuer

The public signature verification key must be implemented and delivered to the CA, either via an on-line transaction, i.e. through the web interface, in accordance with the PKIX "Internet X.509 Public Key Infrastructure Certificate Management Protocols" [1,2],

or via an equally secure manner stated in the CPS. This should be done after a request is made.

#### 1.5.1.4 CA Public Key Delivery to Users

The CA's public signature verification key should be available via the CA's Repository. A legitimate user should be allowed to directly access the repository database.

#### 1.5.1.5 Key Sizes

Key sizes should be long enough to provide adequate protection. As a result each CA must ensure that each certified public key is of the type and length stated in this policy. Key sizes are currently specified [61] as 1024 bits for Public Key Cryptosystems (e.g., RSA [9]) and 160 bits for Elliptical Curve Cryptosystems (ECC) [42].

#### 1.5.1.6 Public Key Parameters Generation

Parameters, if any, shall be specified in the CPS.

#### 1.5.1.7 Parameter Quality Checking

Parameters, if any, shall be specified in the CPS

### 1.5.2 Hardware/Software Key Generation

All software and hardware of interest to the CA should be evaluated prior to using. All components chosen will be the ones that comply with the specifications given by this CP.

#### 1.5.2.1 Key Usage Purposes (As per X.509 v3 field)

As per PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [1, 2] the CA signing keys may be used for signing certificates and CRLs, whereas the End Entity signing keys may be used for authentication, non-repudiation and message integrity. Both keys may also be used for session key establishment. The name of the field as per the X. 509 is specified as KeyUsage field.

### 1.5.3 Private Key Protections

The CA should make it clear that it does not have any legal or ethical responsibility and is not liable in the case of a private key being misused.

#### 1.5.3.1 Policy CA Private Signing Key

The private signing key of the CA must be well protected from any disclosure and unauthorized use, especially when not active. In such a case, the key must be stored in an encrypted form. The activation data for the private key may be in the form of a password. Two persons must participate or be present to activate the Policy CA's private signing key. It is recommended that the CA's private key be stored in an isolated machine within a restricted area and under strict control as to who may have access to this machine. Regular backups should be made so as to minimize the recovering time in case of system disaster. For backups the system should provide at least the same level of protection in all situations as stipulated for the regular active private signing key. The procedures used shall be described in the CPS.

#### 1.5.3.2 End Entity Private Signing Key

Guidelines should be given to the Subscriber for the protection of his private keys from disclosure. When not active, the private key must be stored in encrypted form, to protect it from unauthorized use. The activation data for the private key may be in the form of a password. Occasionally backups are also recommended for avoiding the possibility of loses. Subscribers are advised to copy and store their keys in an encrypted form.

#### 1.5.3.3 Private Key Backup

As mentioned earlier the Subscribers are recommended to back up the Subscribers' private key. For this reason, the CA / RA should inform Subscribers of the consequences of the non-availability of the private key, and they should give them guidance for the appropriate method(s) for key backup.

### 1.5.4 Other Aspects of Key Pair Management

#### 1.5.4.1 Public Key Archival

All public keys are archived by the Issuing CA.

#### 1.5.4.2 Usage Periods for the Public and Private Keys

Suggested validity periods for keys are:

- Policy CA public signature verification key (2048 bits) and certificate – ten years;
- Policy CA private signing key (2048 bits) – seven years;
- CA public signature verification key (2048 bits) and certificate – three years;
- CA private signing key (2048 bits) – one year;
- End Entity public signature verification key (1024 bits) and certificate – two years;
- End Entity private signing key (1024 bits) – two years.
- Key lengths must be at least 1024 bits and should be determined in organizational Threat-Risk Assessments.

Key lengths and validity periods shall be stated in the CPS.

However to minimize the risk of key misuse, the keys should be renewed every year.

#### 1.5.4.3 Destroying Private Keys

Upon expiration, revocation of a certificate, or other termination of the use of a private key, used for creating signatures, all copies of the private key should be securely destroyed.

### 1.5.5 Activation Data

Any activation data must be unique, unpredictable, and must have an appropriate level of strength for the keys or data to be protected. Where passwords are used, an Entity must have the capability to change its password at any time.

### 1.5.6 Restrictions on Private Key Use

The CA's signing key shall be used only for signing certificates and revocation lists. Separate Keys are often used for signing certificates and for signing CRL or other revocation information.

The RA's private key should be used only to support the RA function unless specifically authorized by the CA.

### 1.5.7 Specific Computer Security Technical Requirements

All workstations and servers used in the CA system should be configured to provide the minimal functionality required to provide the assigned CA or RA services. Operating systems along with the PKI software must provide access control and trace-ability down to an individual level on all transactions and functions affecting the use of CA's private signing keys as described in the CPS.

Local Security Policies should be well designed in order to provide the best security required for the local personnel, using the PKI CA software. Any initializations of the system, operating a CA's private signing keys can be performed by at least two operators, both of which are securely identified by the system. A detailed log file must be kept to record with all important steps of the initializing process. The CPS shall include a description of significant security measures for the CA system.

### 1.5.8 Life Cycle Technical Controls

#### 1.5.8.1 System Development Controls

All cryptographic modules developed must be tested prior to usage. All modules must have been developed using well-established techniques and methodology.

#### 1.5.8.2 Security Management Controls

Any alterations of the computer hardware or any modifications, upgrades of the system, or any changes of the configurations must be documented and controlled. The PMAC shall be notified of any significant changes.

#### 1.5.8.3 Network Security Controls

The CA server and repository must be protected through application level (proxy) firewalls configured to allow only the protocols and commands required for the CA's services.

The PKI system must be protected from any attacks through any open or general-purpose network with which it is connected, i.e. the Internet. For this purpose the system must be protected through an integrated solution that involves the implementation and configuration of firewalls, intrusion detection, and other spamming equipment. Such protection must be provided, to allow only the protocols and ports that are required for the operation of the CA to pass thru. All required protocols must be defined in the CPS. Finally, Communications over an external network always require the establishment of an encrypted channel of sufficient strength.

### 1.5.9 Web Server Security

The technology must be such that the web server limits user's access to specific resources and folders. An important issue that is often overlooked nowadays during the configuration of a web server, is the ability to retrieve a list with the contents of a directory. The web server must be configured in such a way that users are not allowed to

see a listing with the contents of directories (files and subfolders). More on Web Server Security can be found in Appendix D.

### 1.5.10 Operating System Security

The operating system and its configuration must provide filesystem security; that is, every user account should have limited, predefined access to the system's folders and files. Moreover, the selected operating system should allow the deployment and use of other security techniques such as software firewalls and software intrusion detection systems.

### 1.5.11 Database Security with Discretionary Access Control

The selected DBMS must allow the ability to create, modify and delete user accounts in the database level. The DBMS must support discretionary access control; i.e. it should provide the DBA with the ability to define the tables to which a user has access to, as well as the kind of access (INSERT, UPDATE, DELETE, SELECT).

This kind of control allows the minimization of the chances of a particular user damaging the database. For example, unregistered users who access the system through their web browser, to apply for registration, will logon to the database with a specific, limited capabilities account; this account will be configured in such a way by the DBA so that it restricts the user's ability to manipulate the database. For instance it may allow the user only to INSERT an entry into the application requests table, but not UPDATE it. So even if the user gains the ability to send raw SQL commands to the database, he will not be able to change his request status, delete other users' requests, view other users' requests, steel passwords, access other tables etc.

### 1.5.12 Reliability

The technological framework must provide system reliability; i.e. the system must always produce correct results. In order to achieve this requirement, the use of popular, well-tested and mature software is suggested.

### 1.5.13 Resilience

The technological framework must provide the means to build a resilient system; i.e. the system must prevent data from being damaged in cases of failure. Since the core of the system will be based on databases, the use of a DBMS, which ensures the ACID[14] properties, is critical. No compromise should be made in favor of low cost.

## 1.6 Certificate and CRL Profiles

This section specifies the certificate format and the CRL format. Any further coding conversations or any other specific information regarding the content required, recommended fields, extensions, and CRLs, should be specified in the CPS.

### 1.6.1 Certificate Profile

Public keys shall be contain in the Certificates that reference this Policy and shall be used for authenticating the sender of an electronic message and verifying the integrity of such messages, including public keys used for digital signature verification.

All certificates that reference this Policy must be issued in accordance to the X.509 format. CAs should identify in their CPS, the certificate extensions supported. Such support should be consistent with the Healthcare Certificate Profile detailed in an attachment to this document.

[14] ACID stands for Atomicity, Consistency, Isolation and Durability. These are the attributes any serious DBMS must possess.

### 1.6.1.1 Version Numbers

The CA must issue X.509 Version 3 certificates, in accordance with the PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" RFC2459[2].

The values of the base (non-extension) X.509 fields shall be:

| Field Comment | Content |
|---|---|
| Version | Version of X.509 certificate, version is 3 |
| serialNumber | Unique serial number for certificate |
| Signature | The OID for the algorithm used by the CA to sign the certificate. |
| Issuer | X.501 type distinguished name of CA. |
| Validity | The first and last date in the validity period for the certificate |
| Subject | Distinguished name of the entity to which the certificate is issued. |

**Table 1:The values of the base (non-extension) X.509 fields**

### 1.6.1.2 Certificate Extensions

The following table states extensions that: are required, recommended, not recommended, and not allowed, in certificates complying with this CP. It also states whether each extension should be marked as critical or not:

| Extension | Required | Recommended | Not recommended | Not allowed |
|---|---|---|---|---|
| authorityKeyIdentifier | NC | | | |
| subjectKeyIdentifier | NC | | | |
| keyUsage | C | | | |
| certificatePolicies | | NC | | |
| policyMapping | | | | EE, CA |
| subjectAltName | | NC | | |
| issuerAltName | | NC | | |
| subjectDirectoryAttributes | | | | EE, CA |
| basicConstraints | CA/C | | | EE |
| extKeyUsage | | If applicable: EE, CA / C | | |
| cRLDistributionPoint | | NC | | |
| authorityInformationAccess | | | | EE, CA |
| nameConstrains | | | | EE, CA |
| OCSPNocheck | | | | EE, CA |
| policyConstraints | | | | EE, CA |
| privateKeyUsagePeriod | | | | EE, CA |

C = critical, NC = noncritical, EE = End Entity certificate, CA = CA certificate

**Table 2:Table Extensions Criticallity**

The following table specifies the values of certificate extensions and recommends values for some recommended extensions.

| Extension Comment | Content |
|---|---|
| authorityKeyIdentifier | Can be used to identify a particular public key when a CA has several. Fingerprint of CAs public key, and serial number of CA certificate. |
| subjectKeyIdentifier | Fingerprint of the subjectPublicKey. |
| keyUsage | End Entity certificate – RSA key: digitalSignature, nonRepudiation, keyEncipherment. CA certificate – RSA key: keyCertSign, cRLSign. |
| certificatePolicies | End Entity and cross-certification certificate: OID, URI of CPS and UserNotice CA certificate – OID. |
| subjectAltName | E-mail address is recommended. |
| issuerAltName | E-mail address, and http URI to CA web site are recommended. |
| basicConstraints | CA certificate: true<br>Shall not appear in end End Entity certificates |
| cRLDistributionPoint | URI of CRL. |

**Table 3: The values of required certificate extensions**

### 1.6.1.3 Cryptographic Algorithm Object Identifiers

The following algorithms, for signing and verification, must be supported by the CA and the End Entities:

RSA – {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 };
SHA-1 – sha1WithRSAEncryption, {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }.

In addition, the CA and End Entities must support the algorithms approved by PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [2] for verification.

### 1.6.1.4 Name Forms

Each DN must be in the form of an X.501 UTF8 String.

#### 1.6.1.5 Processing Semantics for Critical Certificate Policy Extension

Critical extensions should be interpreted as defined in PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [2].

### 1.6.2 CRL Profile

All PKI End Entity software must support and correctly process the CRL fields and extensions identified in PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [2]. Any CRL issued by a CA referencing this Policy must include the CRLNumber extension; use of the CRLReason extension is recommended. The CA's public CPS shall identify the CRL extensions supported.

| **CRL Field** | **Comment -Content** |
|---|---|
| version | X.509 CRL, version is 3 |
| signature and signatureAlgorithm | sha-1WithRSAEncryption shall be used by the CA to sign the CRL. OID: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } |
| issuer | |
| thisUpdate | Required |
| nextUpdate | Required |
| **CRL Entry Field** | |
| userCertificate | Serial number of revoked certificate |
| revocationDate | Required |

**Table 4: Supported Extensions**

#### 1.6.2.1 1 CRL and CRL Entry Extensions

All PKI user software must correctly process all CRL extensions and CRL entry extensions identified in PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [2]. The following table lists CRL extensions and CRL entry extensions that are required, recommended, and allowed in CRLs complying with this CP. It also states whether each extension shall be marked critical or not:

| CRL Extension | Required | Recommended | Allowed |
|---|---|---|---|
| authorityKeyIdentifier | NC | | |
| issuerAltName | | NC | |
| **CRL Entry Extension** | | | |
| reasonCode | NC | | |
| invalidityDate | | NC | |

**Table 5: CRL Extension Criticallity**

The following table gives the stipulations for the extensions and entry extensions:

| CRL Extension | Comment – Content |
|---|---|
| authorityKeyIdentifier | Can be used to identify a particular public key when a CA has several. Fingerprint of CAs public key, and serial number of CA certificate. |
| issuerAltName | E-mail address, and http URI to CA web site are recommended. |
| **CRL Entry Extension** | |
| reasonCode | Specified reason codes are strongly recommended. |
| invalidityDate | Date of known or suspected compromise or invalidation. |

**Table 6: Extensions Stipulations**

### 1.7 Specification Administration

### 1.7.1 Changes with Notification

Prior to any changes to this certificate policy, the PMAC will notify all entities including subordinate CAs, and all CAs that are directly cross-certified with the Policy CA.

#### 1.7.1.1 List of Items

All items, except the contact information in this certificate policy, are subject to the notification requirement.

#### 1.7.1.2 Notification Mechanism

The notification will be stated by PMAC and must contain a statement of the proposed changes, the final date of receipt of comments from entities, and the proposed effective date of change. Notification of the changes along with the proposed changes will be available on line at the RA web site. All subordinate CAs will be notified by the PMAC, in writing.

#### 1.7.1.3 Comment Period

The comment period will be maximum 30 days unless otherwise specified in the CPS. The comment period will be defined in the notification. If a proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be published.

#### 1.7.1.4 Mechanism to Handle Comments

Proposed Comments by impacted users must be handed directly to the PMAC within the time limit and no later than the time specified in the CPS. Decisions with respect to the proposed changes are at the sole discretion of the PMA.

#### 1.7.1.5 Period for Final Change Notice

The PMAC will determine the period for final change notice.

#### 1.7.1.6 Items Whose Change Requires a New Policy

If a policy change is determined by the PMAC to warrant the issuance of a new policy, the PMAC may assign a new Object Identifier (OID) for the modified policy. The new assign number will be a under the original root OID.

### 1.7.2 Publication and Notification Policies

This policy definition, digitally signed by an authorized representative of the CA, is (currently) available in electronic form on the Internet at: http://www.hippocrates.org.cy/policies.htm or via email from cp@hippocrates.com.cy. Other CAs issuing certificates that identify this certificate policy shall post copies of this CP on their CA web site.

### 1.7.3 CPS Approval Procedures

CPS contains information, relevant to the security of a CA, and more specific to this CP. CPS must also be available on line for all Subscribers. The subscriber must accept both CP and CPS prior to receiving the Certificate. CPS can be found at http://www.hippocratres.org.cy or via an email from cps@hippocrates.com.cy.

## 1.8 Policy Administration

Any party that registers an OID for this Policy (the Registering Party), will provide notice of any proposed changes to this policy, which may materially impact users of this Policy. The Registering Party will make reasonable attempts to directly notify CAs known to have implemented this Policy, who then are required to notify their Subscribers. Notice can be accomplished either electronically or by mail. The Registering Party will post the proposed changes in electronic form, on the Internet.
If the changes to the Policy will have a material affect upon acceptance by Relying Parties, the new Policy created by the application of the proposed changes should be assigned an OID, distinct from that assigned to this Policy.

### 1.9 Personnel Expertise

The selection of a particular framework should take into account the current personnel's expertise. The use of familiar and easy to learn technology is highly desirable, as it will lead to faster implementation, quicker response when changes are required and less training cost

# Appendix B

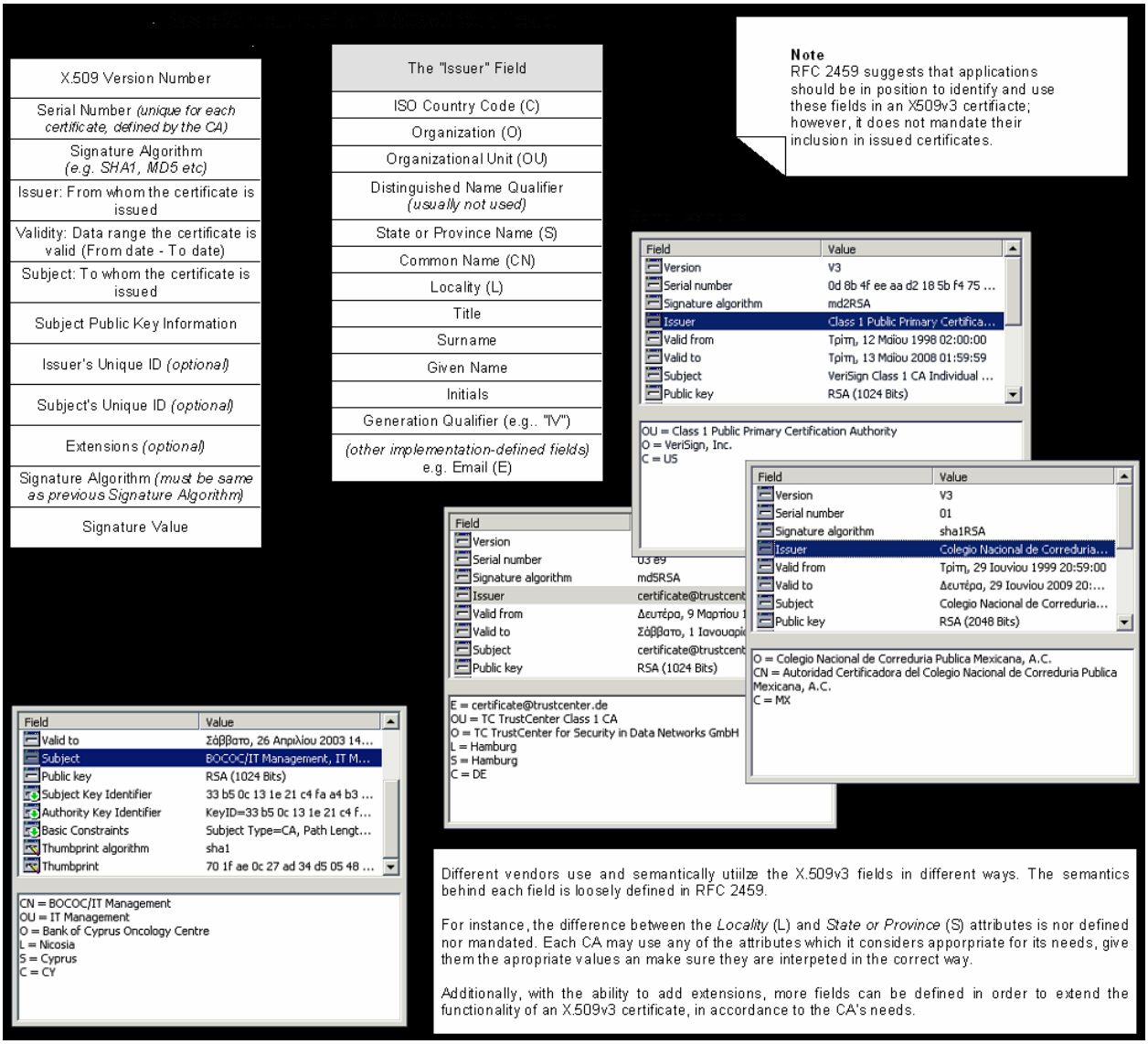


Figure 4: Basic Structure of an X509 v3 Certificate

# Appendix C

## Hippocrates CA/RA Personnel Agreement

Hippocrates Certificate Authority (CA) system has the obligation and responsibility to ensure the trustworthiness of the provided services and protect confidential information processed, at all times. Hippocrates CA system is supported by the job function of appropriate Certificate Authority (CA) and Registration Authority (RA) personnel who must obey to the following rules and procedures:

(1) **Demonstrate integrity and confidentiality.**

All personnel have an obligation to act in a conscious, loyal and secure way in all daily activities regarding the operation of Hippocrates CA system. If for any reason any employee is found revealing any sensitive CA security-relevant information or Subscriber information will be held liable for his/her action and legal measures may be forced against him/her.

2) **Read and Adhere to Hippocrates Agreed Procedures.**

All personnel must understand the guidelines provided in Hippocrates Certificate Policy (CP) and Certificate Practice Statement (CPS) and perform their duties according to them. The CP and CPS must be made available to CA and RA personnel by an appointive officer.

(3) **Willing to receive appropriate training.**

All personnel, according to their duties and in respect to the operation of CA or RA, must be willing to receive comprehensive training on the following areas:

- The CA/RA security principles and mechanisms
- The CP and CPS guidelines and their practical implementation
- All PKI software versions in use on the CA and RA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures

(4) **Acknowledge the proper and legitimate Usage of Hippocrates CA's Public Key Certificates.**

Upon agreeing to subscribe to a certificate, all personnel acknowledge that it should be used to facilitate appropriate access to personal health information and that such data is protected from disclosure or other malicious activity. Any inappropriate acquisition and misuse may lead to a criminal penalty.

---

I acknowledge that I have read, understood and accept the terms of this document and I will comply with the recommended procedures.

Signature _____ Date_____

---

# Hippocrates End User Agreement

A certification authority has the obligation and responsibility to ensure the trustworthiness and security of the certification process. However, the certification authority alone cannot ensure trustworthiness and security; the subscribers and relying parties also have duties, as far as making sure that the certification process is secure and trustworthy is regarded.

The terms “End User” and “Subscriber” hereinafter refer to: (a) an identified individual on behalf of whom the certificate is being issued, and who is managing the private key (b) an identified organization acquiring the certificate and managing the private key on behalf of an identified individual (c) an organization acquiring the certificate and managing the private key on behalf of a group of identified individuals.

Upon requesting a certificate from the Hippocrates Registration Authority, End Users shall:

(1) **Present Accurate Information**: A subscriber has an obligation to present accurate information to the certification authority and the registration authority when the subscriber applies for a certificate.

(2) **Check of Certificate Issuance:** When a certification authority issues a certificate, the subscriber has an obligation to check the descriptive information on the certificate for accuracy and notify the certification authority in case of mistakes or oversights.

(3) **Protect the Private Key**: A subscriber has an obligation to take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including the selection of a passphrase having a minimum of 8 characters.

(4) **Prompt Revocation/Renewal Procedure:** A subscriber has an obligation to take prompt action towards (a) certificate revocation in cases where there is a compromise or leakage of the private key (b) certificate renewal in cases where the information recorded on a certificate has changed.

(5) **Read and Adhere to Hippocrates Agreed Procedures**: Furthermore, in the case where the subscriber is an organization, it should maintain control and ensure that the use of certificates will not be against the rights of any of individual members of the organization.

(6) **Accept that in the Usage of Public Key Certificates Hippocrates CA's Liability is Limited According to What is Specified in the Certificate Policy**.

Upon agreeing to subscribe to a certificate, the End User consents to the formation and conclusion of contracts, delivery of notifications and communications in general, by electronic means, with Hippocrates CA for the purposes of the digital certification services provided in accordance with appropriate policies and that she/he is prepared and has the capability and equipment to do so.

---

I acknowledge that I have read, understood and accept the terms of this document and I will comply with the recommended procedures.

Signature _____ Date_____

---

# Appendix D
# Web Server Security Requirements

## 1.0 Introduction

Since RA users will have the ability to connect and download digital certificates from the RA web server or perform other sorts of sensitive data transactions, it is extremely important to be able to provide a secure communication link between the user's web browser and RA's web server. A secure communication link is imperative, in order to ensure the identity of the participating entities and the confidentiality of the transmitted data. A secure communication link can be established using the SSL protocol.

## 2.0 The Secure Socket Layers (SSL) Protocol

SSL is a protocol layer which is placed between a reliable connection-oriented network layer protocol (TCP) and the application protocol layer (HTTP). SSL provides secure communication between the client and server, in three ways:

1. Allows mutual authentication, using certificates.
2. Allows data integrity check, using digital signatures (message digests).
3. Allows confidentiality, using data encryption.

The protocol begins with a handshake phase that negotiates an encryption algorithm and keys, and authenticates the server to the client. Once the handshake is complete, all data traffic between the two end-hosts is encrypted using the keys negotiated during the handshake phase.

During server authentication, the client (web browser) obtains a certificate from the server (web server) containing the server's public key. The certificate must be issued by a CA listed in the browser's list of trusted CAs. This allows the client to authenticate the server before sending any data to it.

During **client authentication**, the server obtains a certificate from the client containing the client's public key. This certificate must have also been issued by a CA which is included in the server's list of trusted CAs.

### 2.1 Certificates in SSL Transactions

As stated earlier, the certificate which the client obtains from the server must be issued by a CA listed in the browser's list of trusted CAs. If not, then the client's browser will display a warning dialog box (like the one beside) notifying the user that the certificate is not issued by a trusted CA (or other reasons for which the client may choose to refuse the certificate). Still, if the system policies allow it, the certificate may be accepted thereby allowing the communication to continue.


Figure 5: Security Message Alert received from Windows 2000 Advance Server

### 3.0 Do We Need Certificates from A Third Party?

It is not necessary to obtain a certificate from a third party, as long as HCA creates its own, self-signed certificates to be used for SSL transactions. A drawback of this practice is the fact that the client will have to manually accept the certificate (in response to a dialog box like the one shown before). Another drawback is that if the client works for an

organization, the Information Systems Administrator may configure the system so that it does not accept any certificates from non-trusted parties.

### 3.1 Certificates from Verisign

Verisign provides certificates with 128-bit encryption key and one-year lifetime for $895. With two-year lifetime, it costs $1595.
There is also a cheaper, 40-bit encryption certificate which costs $349 and $598 for one-year and two-year lifetime respectively but it is not recommended.

## References


**1.** Carlisle Adams and Stephen Farrell, Internet X.509 Public Key Infrastructure Certificate Management Protocols, March 1999 (RFC 2510)

**2.** Russell Housley, Warwick Ford, Tim Polk and David Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999 (RFC 2459)

**3.** X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999 (FBCA)

**4.** National Computational Science Alliance, Certificate Policy, Version 0.9.1, June 30, 1999 (NCSA)

**5.** Santosh Chokani, Warwick Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999.(RFC 2527)

**6.** Burt Kaliski, The MD2 Message-Digest Algorithm. RSA Laboratories, April 1992.(RFC 1319)

**7.** Ronald Rives, The MD4 Message-Digest Algorithm. RSA Data Security Inc., April 1992. (RFC 1320)

**8.** Ronald Rives, The MD4 Message-Digest Algorithm. RSA Data Security Inc., April 1992. (RFC 1321)

**9.** Ronald L. Rivest , Adi Shamir, and Len Adleman, A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2):120-126, February 1978.

**10.** European Union, "DIRECTIVE 1999/93/EC-Electronic Signatures" The European Parliament And Of The Council. 13 December 1999

**11.** European Union, "Data Protection Act 1988- Keeping personal information on computer:Your responsibilities-Guidelines for Data Controllers issued by the Data Protection" The European Parliament And Of The Council. 13 December 1999

**12.** European Union-The European Parliament, "Data Protection Act 2003",2003

**13.** Evelyn JSHovenga, " Primary Healthcare , e-Health and Internet Access". The world Medical Association,2002.

**14.** European Union, “An Information Society For All”. Communication on a Commission Initiative for the Special European Council. Lisbon, 23 and 24 March 2000.

**15.** Health Summit Working Group, “Criteria for Assessing the Quality of Health Information on the Internet”. Approved by the IEEE-USA Board of Directors (November 1999)

**16.** European Parliament , “Directive 2000/31/EC –Electronic Commerce”, Official Journal L 178 , 17/07/2000 P. 0001 - 0016

**17.** EESSI Conformity Assessment Guidance Issued 2000-11-15 Ref. ESV-54, 1.0

**18.** Policy requirements for certification authorities issuing public key certificates, ETSI TS 102 042 V1.1.1 (2002-04)

**19.** Policy requirements for certification authorities issuing qualified certificates, ETSI TS 101 456 V1.2.1 (2002-04)

**20.** National Bureau of Standards. Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46-3. U.S. Department of Commerce, 1977. Reaffirmed 1988.

**21.** National Bureau of Standards. DES Modes of Operation, Federal Information Processing Standards Publication (FIPS PUB) 81. U.S. Department of Commerce, 1980.

**22.** Whitfield Diffie and Eric S. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976.

**23.** Burt Kaliski, “Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services”. Internet Engineering Task Force, 1993. (RFC 1424)

**24.** Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, “X509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, June 1999. (RFC 2560)

**25.** Paul Wing, Brian O'Higgins, Using public-key infrastructures for security and risk management, IEEE Communications Magazine v. 37 no9 (Sept. 1999) p.71-3

**26.** Ortiz, Sixto, Jr. Will PKI become a key to online security? IEEE Computer v. 33 no12 (Dec. 2000) p.13-15

**27.** Ellison,Carl and Schneier,Bruce. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, Computer Security Journal, Volume XVI, Number 1, 2000

**28.** Ellison,Carl and Schneier,Bruce, Risks of E-commerce. Communications of the ACM v. 43 no2 (Feb.2000) p. 152

**29.** Hunt, Ray. Technological infrastructure for PKI and digital certification. Computer communications. 24, no. 14, (2001): 1460 (12 pages)

**30.** Ellison,Carl M The nature of a useable PKI Computer networks. 31, no. 8, (1999): 823 (8 pages)

**31.** Carlisle Adams, Mike Burmester, Yvo Desmedt, Mike Reiter and Phil Zimmerman, Which PKI (Public Key Infrastructure) is the right one? Proceedings of the 7th ACM conference on Computer and communications security, 2000, Pages 98-101

**32.** David A. Cooper, "A model of certificate revocation", In Proceedings of the Fifteenth Annual Computer Security Applications Conference, December 1999.

**33.** Warwich Ford and Michael S. Baum, "Secure Electronic Commerce", Prentce Hall PTR, 1977

**34.** Bruno,Lee, Certificate authorities: Who do you trust? Data Communications, vol. 27, no. 4, pp. 54-63, 21 Mar 1998

**35.** Carlisle Adams and Steve Lloyd, "Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Consideration", Macmillan Technical Publishing 1999.

**36.** Jean Carlo Binder, European Master in Multimedia Projects, Introduction to PKI - Public Key Infrastructure, Version 1.1, .2002

**37.** Leslie Peckham, A Business Perspective on PKI: Why Many PKI Implementations Fail, and Success Factors To Consider August 2, 2001

**38.** Certificate Policy, Digital Signature, Medium Strength Soft Certificates: "The Public Key Infrastructure for Swedish Universities and University Colleges" Policy Management Authority 2001-02-08 Version 1.0

**39.** Uppsala University, Certificate Practice Statement (CPS), Uppsala University CA 2001-05-28 Version 1.1

**40.** NHS Information Authority, Certification Practices Statement Guidelines For Encryption Certificates, April 2002

**41.** Matt Blaze, Whiteld Die, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, Michael Wiener, Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, January 1996

**42.** Arjen K. Lenstra, Eric R. Verheul, Selecting Cryptographic Key Sizes, October 27, 1999.

**43.** Albert Levi and M. Ufuk Caglayan, An Efficient, Dynamic and Trust Preserving Public Key Infrastructure, IEEE journal, 2000.

**44.** ITU-T Recommendation X.509, ISO/IEC 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, 1997 Edition.

**45.** Utah Becomes First State to Provide For Digital Signatures, The Computer Lawyer, Jan. 1998, at 26

**46.** Charles R. Merrill, What Lawyers Need to Know About the Internet, A Cryptography Primer, 433 PLI/Pat 187, 189-90 (1996).

**47.** Blake Ramsdell, S/MIME Version 3 Certificate Handling, work in progress, Internet Draft, April 1999.

**48.** Shashi Kiran, Patricia Lareau and Steve Lloyd, PKI Basics – A Technical Perspective, http://www.pkiforum.com, November 2002

**49.** Shimshon Berkovits, Santosh Chokhani, Judith A. Furlong, Jisoo A. Geiter, and Jonathan C. Guild, "Public Key Infrastructure Study: Final Report", MITRE Corporation, April 1994.

**50.** Loren M. KohnFelder, "Towords a Practical Public-key Cryptosystem", B.S. Thesis, supervised by Len Adleman, MIT, May 1978.

**51.** U.S. Department of Health and Human Services, HHS IRM Policy for Public Key Infrastructure (PKI) - Certification Authority (CA), 2001, HHS-IRM-2000-0011. Available at: http://www.hhs.gov/read/irmpolicy/0011.html

**52.** Government of Canada, Serving Canadians Better-Government On-Line initiative. Available at: http://www.gol-ged.gc.ca/index_e.asp

**53.** Government of Canada, Policy for Public Key Infrastructure Management in the Government of Canada.
Available at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_e.asp

**54.** Accredited Provider of PKI within the Australian healthcare sector -Health eSignature Authority Pty Ltd, policy documents.
Available at: http://www.hesa.com.au/forms_pubs/policy_docs.htm

**55.** Governing Technical Committee ISO/TC 215 Working Group , http://www.health.nsw.gov.au/iasd/imcs/iso-215/

**56.** NHS Information Authority, Explanatory Guideline To PKI For Health Care Administrators, Version 1.0,28 April 2002

**57.** ISO 17090-1, Health Informatics - Public Key Infrastructure Part 1: Framework and Overview, 2001.

**58**. Erkki Liikanen, Commissioner, "The eEurope Policy Perspective" - The Contribution of ICT to Health-Ministerial Conference and Exhibition. 22-23 May, 2003 – Brussels. (Conferences Presentations)

**59**. Georges De Moor, "Standardization and legal issues in eHealth" - The Contribution of ICT to Health-Ministerial Conference and Exhibition. 22-23 May, 2003 – Brussels. (Conferences Presentations)

**60**. Dorothy E. Denning -Denning. Cryptography and Data Security. Addison-Wesley, Reading, Mass., 1982.

**61**. HCFA Internet Security Policy, Internet Communications Security and Appropriate Use Policy and Guidelines for HCFA Privacy Act-protected and other Sensitive HCFA Information, 1998.