

This is an HTML working draft that led to an article publication. A reference to this work should always be done using the following citation:

(C4) [Dimitrios Lekkas](#), [Stefanos Gritzalis](#), [Socrates Katsikas](#), "[Deploying quality management in Trusted Third Parties within a medical environment. Towards ISO9000 compliance](#)", In *Proceedings of 6th International Symposium on Health Information Management Research – ISHIMR 2001*, Halkidiki, Greece, Sheffield Academic Press, (May 2001)

This material is presented to ensure timely dissemination of research and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by all the copyright holders. In most cases, these works may not be reposted or distributed without the explicit permission of the copyright holders.

DEPLOYING QUALITY MANAGEMENT IN TRUSTED THIRD PARTIES WITHIN A MEDICAL ENVIRONMENT. TOWARDS ISO9000 COMPLIANCE

D. Lekkas ^a, S. Gritzalis ^{a,b}, S. Katsikas ^a

^a Department of Information & Communication Systems,
University of the Aegean,
30 Voulgaroktonou St., Athens, GR-11472, GREECE
e-mail: (dlek, sgritz, ska)@aegean.gr

^b Department of Informatics,
Technological Educational Institute (T.E.I.) of Athens
Ag. Spiridonos St., Aegaleo GR-12210, GREECE

e-mail: sgritz@teiath.gr

ABSTRACT

In this paper we present a complete reference framework for the operation of a Trusted Third Party (TTP) as an organisation within a medical environment. The objective is to form an intermediate reference model, to which the TTPs will conform, towards the full compliance to the ISO-9000 quality standard. There are two dimensions of quality in respect of a TTP, which are related to specific medical environment issues: The first quality dimension regards the value added security services and products it provides, which must fulfil the user requirements and be characterised by efficiency, reliability, security, credibility and trust. The second quality dimension refers to the internal organisation, which must maximise its effectiveness by achieving efficient management, have a clear and strict structure and comply with the registered internal procedures. The guidelines for achieving the above mentioned quality objectives are reflected within the published Quality Policy Statement and the Certification Practice Statement (CPS).

Keywords: Quality, Trust, ISO-9000 quality standard, Security, Public Key Infrastructure, Health Information System

1. INTRODUCTION

The Public Key Infrastructure (PKI) becomes more important within the healthcare society as the need for secure communications and data protection grows. A Trusted Third Party (TTP) may exist within the PKI as a governmental institution, as a private business or as a non-profit research organisation. The scope of a TTP within a Health Information System (HIS) is to provide end-to-end security services, which are scalable, based on standards and are usable across different domains, geographical areas and specialisation sectors. The user requirements for various medical perspectives have to be extracted and satisfied.

Hereinafter the TTP will be referred also as '**organisation**' and the users of the TTP services as '**customers**'. Customers may be, but not limited to, patients, healthcare personnel, hospitals or other TTPs.

The aim of a TTP to provide acceptable and effective services will only be achieved when the organisation gains *enhanced level of trust* from its customers. Global trust is essential in a sensitive environment such as HIS. The objective towards this achievement is to form a reference framework for the operation of a TTP, which conforms to the requirements of the ISO-9000 quality standards. It is a management responsibility to ensure that the quality objectives are met. Failure to meet these requirements may have consequences in the trustworthiness that will adversely affect the customer, the organisation and the society.

The term "quality" in respect of a TTP has to be examined under two perspectives: The first is the *Quality of Service*, which regards the features and characteristics of the value added services provided that enable them to satisfy the customer needs. The second perspective is the *Quality Management*, which administers efficiently the internal organisation and structure, implements the stated quality policy and activates the

Quality System, handling responsibilities, procedures, processes, human and material resources.

The main objective of this paper is to provide all the basic guidelines towards the development of a quality system for a TTP, according to ISO-9001 [1] and ISO-9004-2 [2]. The requirements of the standard will be examined and their mapping to the TTP business, products and services will be attempted. The principle elements of the standards that will be examined in detail include the management responsibility, the quality system, contract review, design and document control, subcontracting, verification, inspection and quality records. These elements will be analysed in association with the user requirements for security, the TTP services provided to the healthcare society, the internal processes and control functions, and the published Certificate Policy and Certification Practice Statements (CPS) [3] [4] [5].

2. BACKGROUND: THE ROLE OF A TTP IN SECURE ENVIRONMENTS

Trusted Third Parties supply technically and legally reliable means for producing objective evidence concerning an electronic transaction and for data protection. TTP services are provided and underwritten not only by technical, but also by legal, financial, and structural means [6] [7]. TTPs are operationally connected through chains of trust (usually called *certificate paths*) in order to provide a web of trust forming the notion of a Public Key Infrastructure. A PKI consists of one or several TTPs that issue and revoke certificates for users and other TTPs. The TTPs may be organised in many ways, including, for example, a hierarchy or a decentralised web of trust. In general, the following entities are involved within a TTP solution:

- **Certificates:** The term certificate was, first, used to refer to a digitally signed record holding a name and a public-key [8]. Today a certificate binds a public-

key value to a set of information that fully identifies the entity (such as person, organisation or site) which possesses and uses the corresponding private key. Numerous additional attributes are included in a certificate, related to its usage (e.g. allowed usage, expiration, issuing authority, algorithms and key length).

- **Certificate owners:** This entity is the identified party bind to a certificate. It is known as the 'subject' of the certificate.
- **Certificate users** or 'relying parties' are the entities that need to use, and rely upon the accuracy of the public key distributed via a certificate. Typically a certificate user verifies a digital signature originating from the certificate's subject or sends encrypted data to the subject.
- **Registration Authorities (RAs)** which handle identity verification material in order for a certificate to be issued by the CA to a user. The RA also issues a certificate request on behalf of the user, among other related tasks.
- **Certificate Authorities (CAs)**, which can manage (i.e. issue and revoke) a certificate (sometimes we use the term CA instead of TTP). The degree to which a certificate user can trust the binding embodied in a certificate depends on several factors. These factors include the practices followed by the RA in authenticating the subject; the CA's operating policy, procedures and controls; the subject obligations (e.g. in protecting the private key); and the stated undertakings and legal obligations of the CA, such as warranties and limitations on liability.
- **Directories** that serve as a repository for certificates issued, and also for publishing Certificate Status Information - CSI (e.g. Certificate Revocation Lists - CRLs, delta CRLs etc.)
- **Software** development kits and application program interfaces to TTP-enabled

applications.

- **Mechanisms** to establish and operationally maintain hierarchical and cross-certification trust relationships among different TTPs.
- **Policies** that have been developed and govern the operation and the procedures of the TTPs.

3. MEDICAL ENVIRONMENT SECURITY ISSUES

Healthcare Information Systems (HISs) are regarded as highly sensitive systems due to the particularly sensitive nature of healthcare information. While the benefits that come with the advent of Information Technology are by no means disregarded, the introduction of automated HISs is welcome only when the trust in the information they provide can be preserved.

In a medical environment the following security characteristics of the healthcare information must be preserved:

- integrity (prevention of unauthorised modification)
- availability (prevention of unauthorised withholding or system failure)
- confidentiality (prevention of unauthorised disclosure) and
- authenticity (proof of the owner or the origin of the data)

Healthcare information is a valuable asset that several parties may have interest in getting access to, due to a variety of personal reasons **Error! Reference source not found.** The most influential of the stakeholders are medical researchers, healthcare professionals, patients, the pharmaceutical industry, insurance organisations, healthcare information systems vendors and law enforcement authorities.

The interconnection of HISs with other HISs and the Internet raises new security problems. A TTP and its services contribute to the effort of preserving the constituent elements of a HIS (namely data, equipment, software, procedures and the

aforementioned security attributes) as well as controlling the access of the stakeholders. An ISO-certified TTP will inspire the global trustworthiness needed in a medical environment and thus will provide the means to apply global and strict security policies.

4. QUALITY OF SERVICE

A service is defined as the results generated by activities at the interface between the TTP and the customer and by the internal activities of the TTP, to meet customer needs. A complete set of TTP services as described in Keystone project [10] are: Registration, Digital signatures, Encryption, Time-stamping, Non-repudiation, Key management, Certificate management, Information repository, Directory services, Authorisation, Audit, Quality assurance and Trust services, Customer oriented services and TTP-to-TTP interoperability.

Specifically for a medical environment, the ‘Swedish Medical Association’ in [11] identifies the following topics as a set of security services:

- Access to health-related personal files
- Network security and coding of transmitted patient information
- Physicians roles and integrity
- Education and awareness
- Quality improvement and organisational monitoring
- Use of anonymous data in research
- New technology, standardisation and future trends

The Quality of Service (QoS) is described in terms of a set of features and characteristics that are observable and subject to customer evaluation. They are expressed in common language that can be understood by the user and as a number of parameters. These parameters are either quantitative or qualitative, in other words they

may have absolute value limits or they may be comparable. The service delivery characteristics also need to be defined in terms of characteristics that are not always be observable by the customer, but directly affect service performance [12].

The overall assessment of the QoS is always performed by the users, since the efficiency of the services depends on the fulfilment of user requirements. The feedback from the customers may be obtained through questionnaires, frequently asked questions, complaints and problem reporting. Examples of service characteristics that are subject to user evaluation are:

- Comprehensiveness of the service description
- Waiting times for delivery and processing
- Communication effectiveness and security
- Comprehensiveness and completeness of the Certificate Practice Statement [4] [5]
[3]
- Accessibility and availability of service
- State-of-the-art and standard conformance
- Dependability of service in terms of confidentiality, reliability and integrity
- Help-Desk response
- Trustworthiness
- Certificates usability
- Registration accuracy and authenticity
- Strength of keys
- Accuracy and accessibility of Directory and Information Repository
- Network performance
- Ease of use
- Credibility and frequency of audits.

The control of service quality characteristics can be achieved by controlling the processes that deliver the service. The quality system that embraces all the processes needed to provide an effective service is therefore essential for achieving and maintaining the desired quality. The delivery process of the TTP services is highly automated with minimum human intervention. Therefore, the more definable and documented the processes, the easier to apply structured and disciplined quality system principles.

5. MANAGEMENT RESPONSIBILITY

5.1 Quality Policy Statement

The organisation's quality policy may declare the intention to satisfy customers, the way the customers, employees and suppliers are treated, the intention for investment in training, new technology and continuous improvement and the intentions regarding the law, the standards, the practices, the reliability, the environment and others. This statement should not include any quantitative targets or any exemptions for deviating from the policy, as this will reduce the original intent.

The standard requires that the quality policy shall be relevant to the provider's organisational goals and the expectations and needs of its customers. Furthermore it requires ensuring that this policy is communicated, understood, implemented and maintained at all levels of the organisation [12]. An example of quality policy statement follows:

Our TTP will provide services and products to our customers that will meet or exceed their expectations. Customers are those who make use of our services, our staff, other parent or subordinate TTPs, Local RAs (LRAs) and all people with whom we have contact. We will be carrying out quality assurance activities in all stages of certification processes as they are described in our CPS, in order to achieve total customer

satisfaction. We will be continuously investing in new technology and training, aiming to continuous improvement and best practice. We will thereby provide complete services to the medical society with respect to the national and international laws and ethical principles, to the highest standards, security, safety, reliability and availability.

5.2 Quality objectives

ISO-9004 [2] requires from the management to define and document its objectives for quality. Although these objectives are not explicitly stated, they are aiming to improve the ability of the organisation to satisfy customer needs, to reduce errors in processes and to maintain the standards. These objectives are referring to the performance of the services, the business and the staff; the addressing environment; the impacts on society; the customer needs; the capability, efficiency and controllability of the processes; the working environment; the personnel skills, knowledge, ability, motivation, development and training.

In general terms the quality objectives of a TTP could be summarised as follows:

The Public Certification Services of the TTP must be designed to support secure electronic communications within a Health Information System, to satisfy users' needs for data integrity, confidentiality, authenticity, availability and trust in their personal correspondence, business or research. It will support the ethical principle of medical confidentiality and the patients right for no-disclosure of any personal information unless they agree [13]. It will however support the availability of data necessary for diagnosis, research and knowledge spreading. The security functions of the TTP are addressed to a large, public, geographically dispersed medical community and they are enhancing users' trust against the TTP.

The main objective of the TTP is to confirm or prove the relationship between a named physical or logical entity with its public key. In order to be trusted for this operation it

has to prove its capability, efficiency and controllability of a series of certification processes such as entity registration, naming, authentication, certificate issuance, identity confirmation, revocation, suspension, key management, logging, auditing and legal compliance [14]. The organisation will be offering any necessary resources in order to facilitate a quick and reliable certification process and therefore it will be employing contemporary technology and properly skilled support personnel.

5.3 Commitment

The ISO-9001 [1] standard requires that the commitment of the management to quality is defined and documented. Commitment can be defined either within the policy statement or separately and it should explicitly state that:

- The management of the TTP is really doing at least what it states in the Quality Policy and in the CPS
- It will not distribute any products or services below standard
- It will be listening to the staff and to the customers needs, requirements and suggestions
- It motivates the staff to resolve problems and to achieve the targets.

5.4 Personnel responsibility and authority

The responsibility, authority and interrelation of personnel, who manage, perform and verify work-affecting quality has to be defined and documented. Responsibilities and authorities can be documented using organisational structure diagrams describing the interrelation and the hierarchy of the various roles, job descriptions containing the objectives of each job and procedures specifying individual actions and tasks.

Within a TTP / CA the basic roles that require assignment of responsibility to persons are:

- Defining the quality policy and objectives

- Assigning trained and experienced personnel
- Access to sensitive data and private key store

5.5 Resources

Another requirement of the standard is that the resource requirements for management, performance of work and verification activities must be identified and adequately provided. Within a TTP quality system the necessary resources include technical, human, finance, material and telecommunication resources.

6. QUALITY SYSTEM

One of the most important requirements of ISO-9001 [1] is the establishment and maintenance of a quality system. The quality system is a tool that enables the organisation to achieve its quality objectives either for control or for improvement. A quality system includes the corporate quality policy, a quality manual, the control procedures needed and the support documentation such as standards, guides, and operating procedures.

The contents of the quality manual of a TTP may include:

- *The purpose:* to describe the services offered by the TTP for undertaking CA services and to provide evidence of the methods used in order to exhibit trust.
- *The scope:* practices and procedures employed by the TTP to perform CA services
- *The applicability of a TTP,* such as protection of communication, personal medical records and information assets, secure e-mail, time-stamping and key management.
- *Nature of business:* A trusted third party issuing, managing, verifying and suspending digital certificates and other related services such as time-stamping, archiving and key management in accordance with published CPS.

- *The corporate policy* (example given in the previous section) describing the mission, vision, values and objectives of the organisation.
- *Management control* including the quality system management, audit trailing, trustworthiness exhibition, reviews, planning and continuous improvement.
- *Operational policies and the relative implementing procedures*, from receipt of customer inquiry through to delivery of service. The purpose of the documentation of the operational policies is to translate and extend the corporate policy into practical terms that can be implemented through procedures, as well as to limit the choices whenever choice is available. Some examples of operational policies are given in the next paragraph.

6.1 Operational policies examples

On personnel practices: The TTP shall provide the minimum required practices to assure the trustworthiness and competence of its employees and the satisfactory performance of their duties. Any employees that have access to medical or key repositories and cryptographic operations that may affect the issuance, usage, verification and revocation of certificates will be considered as serving sensitive positions. The management shall conduct periodic assessment of these personnel to verify their continued trustworthiness and effectiveness. Failure to verify this will lead to the removal of the employee(s) from the sensitive position(s).

On resources: The organisation shall provide all the necessary network, communications, manpower and knowledge resources needed to serve any offered service which is included in its CPS. The workload of any additional action to be carried out will be estimated and agreed with the management prior to any commitment to it.

On product identification: The TTP supports the provision of different certificate

classes for different purposes and levels of trust. For each certificate class a clear description shall be given, which includes its applicability, to whom it is addressed, its level of assurance, key protection functionality and required information for its issuance. The applicability of each class of certificates is only a recommendation and the users must independently assess and determine the appropriateness of each class for any particular purpose.

On servicing procedures: These policies should refer to the classes of the certificates provided, the hierarchy within the PKI, the requesting, naming and issuance of certificates, the verification procedures, the applicability and usage of certificates, the suspension expiration and revocation of the certificates and other supplementary services that may be provided.

7. MAINTAINING A QUALITY SYSTEM

The quality system shall be periodically maintained and updated to reflect any business changes and procedural amendments. Another important issue is the constant awareness in the developments of the state-of-the-art technology relevant to information security issues. The policies and procedures of the TTP must be up to date with the latest technological evolution and the generic security policies of the HISs.

7.1 Quality system procedures

According to the standard it is required to prepare documented procedures, which prescribe specific ways to perform the organisation's tasks. Within a TTP, documented practices shall be implemented for the following areas:

- *Control procedures* that regulate the workflow as it passes between departments or processes. Examples of such procedures include the way of communication for the issuance of a certificate, starting from the Local RAs passing through the issuance authority and ending at the Repository.

- *Operational procedures*, which describe how specific tasks are to be performed, such as certificate issuance, verification, revocation, expiration and renewal, naming procedures, certificate and CRL distribution.
- *Inter-operation activities*, that regulate common activities or preserve the hierarchy or control the data flow between divisions of the organisation (such as CAs, RAs, LRAs, Subordinate TTPs and Repositories), with other TTP hierarchies or with a Health Information System. The TTP will regulate the global access to medical data for users of different HISs (even if they are certified by different TTPs) by providing cross-authentication mechanisms. An important issue for a TTP is to ensure the transition of trustworthiness between the various levels of the PKI hierarchy and the effectiveness of the certification chain [10].
- *Standards* that refer to the control or operational procedures are also part of the quality system. Standards determine which is the acceptance level of the quality of a product or a service. For example a TTP may explicitly state in its CPS that the issued certificates conform with the X.509 v.3 standard and that the exchange and verification of digital signatures is performed according to cryptographic message syntax standard PKCS#7 [16]. Standards are not only national or international. The organisation itself may implement its own internal standards as a tool for judging the quality of its activities.
- *Manuals and guides*, containing documented experience, examples and hints to help staff perform their work.

8. CONTRACT REVIEW

Each time a member of the medical community applies for a certificate and after the acceptance of the request by the TTP and the issuance of the certificate, there is

automatically initiated a binding agreement between the customer and the organisation [15]. It is rather an undertaking of obligations by the TTP for the provision of products and services against its customers, according to its CPS. The standard requires that the supplier establishes maintains and co-ordinates documented procedures for contract review. Before accepting an order the contract must be reviewed to ensure that the requirements are adequately defined and documented. Specifically for a TTP the following issues must be clearly defined, in order to be able to perform contract review:

- The classes of certificates provided, their purpose and the related services. Examples of intended certificate usage within a HIS are:
 - Data encryption
 - Digital signatures
 - Secure e-mail
 - Secure Web-server
 - Authentication
 - Subscription services
 - Data integrity
 - Time-stamping
- The conditions of use of a certificate and the security implications of misuse, such as the storage and the protection of the private key, the reliance upon an expired certificate or the possible reasons for revoking a certificate.
- A list of typical features and characteristics that will make the TTP services to fit for its intended purposes within a medical environment. Such features may include at least the following, ordered according to their importance:
 - Trustworthiness
 - Reliability
 - Accessibility
 - Security
 - Efficiency
 - Credibility.
- The delivery of the products and the accessibility to the services, shall include:
 - Key generation and out-of-band exchanges
 - The delivery of certificates (e.g. files, smart cards) and their format (e.g. DER,

X.509)

- The URLs for retrieving the public key of the CA and the CRLs, as well as any other information for certificate verification.
- The contractual requirements such as:
 - Warranty and disclaimers
 - Any financial obligations and conditions
 - Legal issues and TTP liability
 - Subcontracting terms in case of registering a subordinate TTP
 - Customer prerequisites like equipment, material and skills.
- The management requirements, such as points of contact, plans for dealing with breakdowns, plans in case of cease of TTP operation, progress and changes reporting.

9. DESIGN CONTROL

According to the standard it is required to establish and maintain documented procedures to control the design of the products in order to ensure that the specified requirements are met. The first step in this procedure is the establishment of the customer needs. These needs are then converted into specific user requirements (user requirements capture process) [10] [14].

9.1 Design input

Specifically for a TTP, in order to collect the minimal requirements that will constitute the input for the design process, the following items must be identified:

- The purpose of the TTP and its services is to serve the medical IT community as a trusted entity, who will, upon request, bind legally and indisputably a user, company or computer with their digital identity or certificate.
- The environment, the conditions and the interfaces for the usage and distribution of the products and services must be identified. The environment for a TTP is the Internet or an

Intranet or an interface embodied in the HIS. International standards, national laws and IT industry practices should be taken into account.

- The minimum specifications of the users' equipment must be defined as well as the necessary skills they must have in order to use the TTP products efficiently and trustworthy. Whether the TTP services are addressed to the international medical community, to a national medical system or to a specific organisation.
- Any special requirements by the customer, such as security, reliability, accessibility, legal and ethical conformance and promptness.
- Any constraints that may affect the services provided, such as cost of equipment, proprietary technology used bandwidth, key export policies and any national statutory or regulatory requirements.
- The technological standards with which the TTP products and services need to comply. A summary of standards that could be used by a TTP include [10]: PKCS#10 for certificate request [RSA, 1993]; X.509v3 for certificate format; PKCS#7 [16] for certificate distribution; RSA for encryption keys; LDAP for CRL and certificate retrieval; HTTP for enrolment; SSL for secure Web-based communication; MD5 or SHA-1 or RIPEMD-160 signing algorithms for TTP-user or TTP-TTP secure communication and key exchanging; smart-card technology for private key storage.
- The characteristics of the various interfaces to be implemented. For example, the ease-of-use and the completeness shall characterise the end-user interface, while the security and the high availability shall be characteristics of the TTP-to-TTP or TTP-to-HIS interoperability interfaces.

9.2 Design output

The form of the design output must contain readable information suitable to produce,

inspect, test, install and operate the TTP products and services. This information will probably include a hierarchy of documents starting from the specifications of the hardware and the operating system, schematic diagrams of the software used and the network, down to the component installation, like an encryption algorithm or a key generator.

10. DOCUMENT AND DATA CONTROL

It is required to control any information, data and document related to one or more requirements of the standard. The controlled documents are these that are essential to the achievement of quality, as it is described in the quality system. Any documents that are not traceable to the published policies and procedures are identified as uncontrolled. Controlling either a new or an existing document means planning, preparing, approving, reviewing, formatting, controlling versions and dates, publishing and distributing, authorising usage, revising, publishing changes and amendments, indexing, applying security and archiving.

As illustrated in [Figure 1], there are three basic types of controlled documents: The policies and practices of the organisation, the documents deriving from these policies, such as specifications and procedures and the documents that consist a reference in either of the above documents.

11. PRODUCT IDENTIFICATION

The TTP products – typically the certificates of various classes – must be clearly identified and labelled in order to avoid misunderstandings and misuse and to facilitate the matching of the products with the documents that describe them. Each class of certificates provides a designated level of trust and is intended to be used for specific purposes. It is therefore necessary to be identified during all stages of production, delivery, installation, usage, verification and renewal.

Examples of certificate classes with particular usage and trust in a medical environment are:

- Patient certificate (medium trust): authentication, decryption, signing
- Doctor certificate (medium trust): authentication, encryption, decryption, signing, time-stamping
- Hospital certificate (high trust): authentication, non-repudiation, signing, secure web server
- Subordinate TTP (high trust): certificate signing, CRL signing
- Public access certificate (aggregate data, researchers, insurance agents, drug companies) (low trust): authentication

12. PROCESS CONTROL

The subject here is the process followed to implement the design and generate the final product. Such a process is cycled repeatedly and in the same predefined way to deliver products or services to the same standards every time. In order to control and maintain the quality of a product, either the elements that drive the process must be controlled or the product itself must be controlled and verified against quality standards.

In the case of TTP, the implementation of process quality control has direct interaction with the user requirements and with the specifications and the features that have to be achieved, as well as with the other elements of the quality system. A simplified process flow example for Certificate issuance is shown in [Figure 2].

13. VERIFICATION AND INSPECTION OF SERVICES

13.1 Testing

The standard requires that the TTP must establish and maintain documented procedures for inspection and testing activities in order to verify that the specified requirements for the services are met. These procedures can be summarised in the following actions:

- Identify the authority for inspecting and releasing products and services
- Ensure that trustworthiness is kept through out the process of certificate issuance, certificate verification
- Ensure that communicated data is incorruptible and keeps its integrity until it reaches its destination.
- Ensure the accuracy on supplying critical information such as time-stamps. Identify the necessary tools for testing them (e.g. NTP servers, Global Positioning System - GPS)
- Record and document any non-conformities
- Verify that no information is dispatched until verified that it conforms to the specified requirements

13.2 Corrective and preventing action

It is necessary to establish and maintain documented procedures for implementing corrective and preventive action in order to eliminate the causes of an actual or a potential failure or nonconformity. The corrective actions are applied to face an actual nonconformity such as servicing failures, customer complaints, specification changes, quality system changes and maintenance. The preventing actions are taken to minimise potential non-conformities and may be embodied to design reviews, performance analysis procedures, management review procedures and improvement processes.

Specifically for a TTP we can identify four types of corrective or preventing actions:

1. Actions related to the preservation and the improvement of the trustworthiness of the TTP, its services and its processes. They must prevent or correct any factor that could affect the strict internal organisation of the TTP and its efficiency. Furthermore they must be applied against any factor that could deteriorate the level of trust of the value-

added services of the TTP, such as the security aspects of the telecommunication technology used.

2. Actions related directly with the products and the services of the TTP (e.g. certificates and certification process). The corrective and preventing actions of this type must focus on the product conformance to the standards and the user requirements, its delivery, its availability, its security, as well as any design weaknesses.
3. Actions related to the processes. They include reviews of the CPS, actions aiming to the improvement of the efficiency of the processes and the improvement of the personnel skills.
4. The fourth type of actions is related to the system. They are directly connected with the hardware and software used and the telecommunications technology, regarding their performance and reliability.

14. CONCLUSIONS

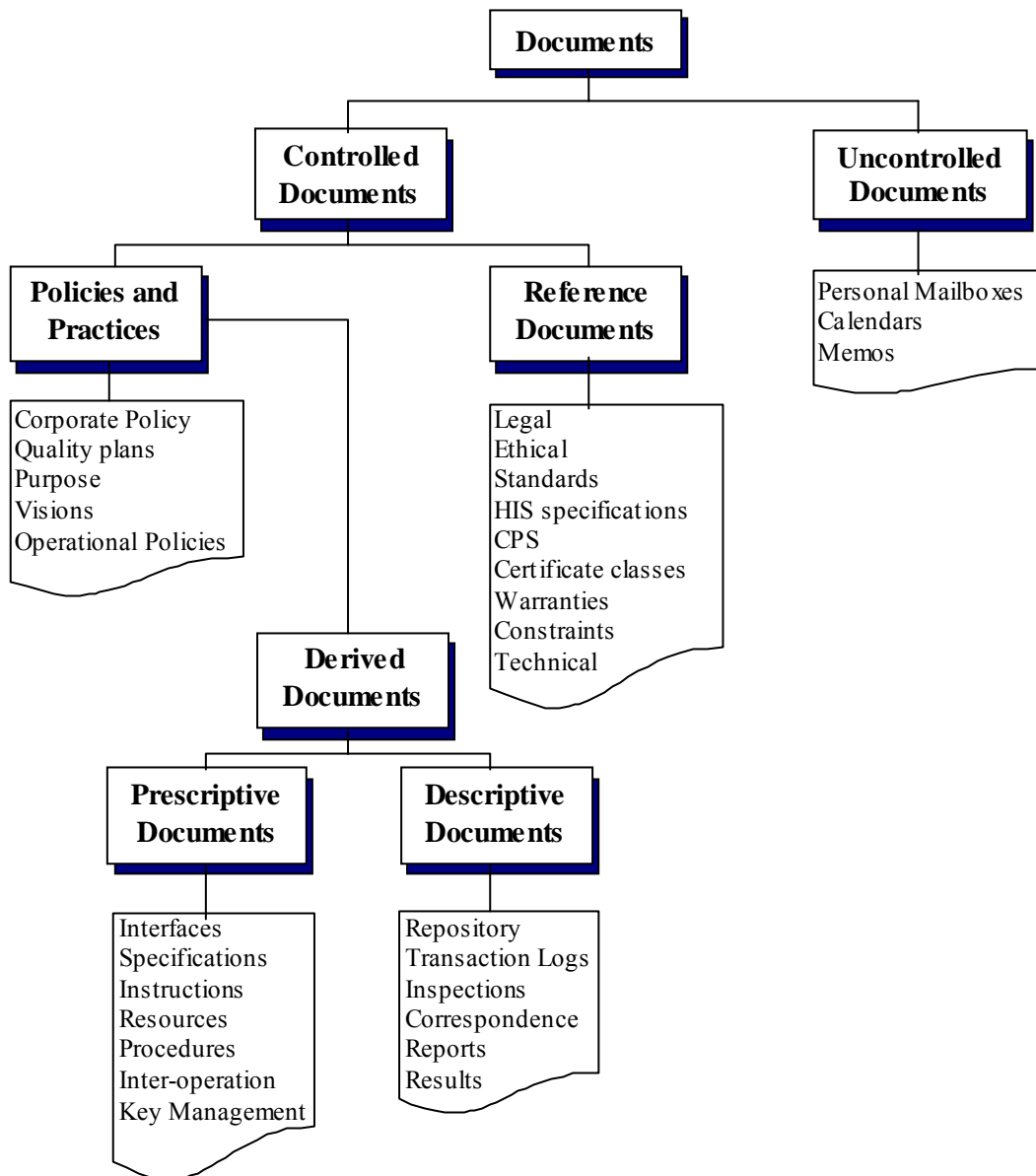
Healthcare establishments invest in Information Technology and aim at improving the quality of health services they offer, while diminishing cost. The information systems they build are characterised as sensitive, high-risk systems since they are handling health-related personal information. The PKI has already presented many solutions towards the secure electronic communications and data storage protection. In the foregoing we have described a framework for the provision of quality PKI services by the TTPs, that will enable the Health Information Systems to be developed more securely and robustly without compromising individual privacy rights. The main objective of this paper is to provide all the basic guidelines towards the development of quality system for a TTP in a medical environment, according to ISO-9001 [1] and ISO-9004-2 [2]. The introduction of a quality system and the certification of a TTP according to the ISO-9000 standards are a necessity, since the demand

for more efficient and reliable security services grow. This compliance will be reflected in the CPS [17] and it will further promote the global trustworthiness of TTPs within the healthcare community. The medical TTPs/CAs will further develop this framework in the future, towards the full compliance with the requirements of the standards.

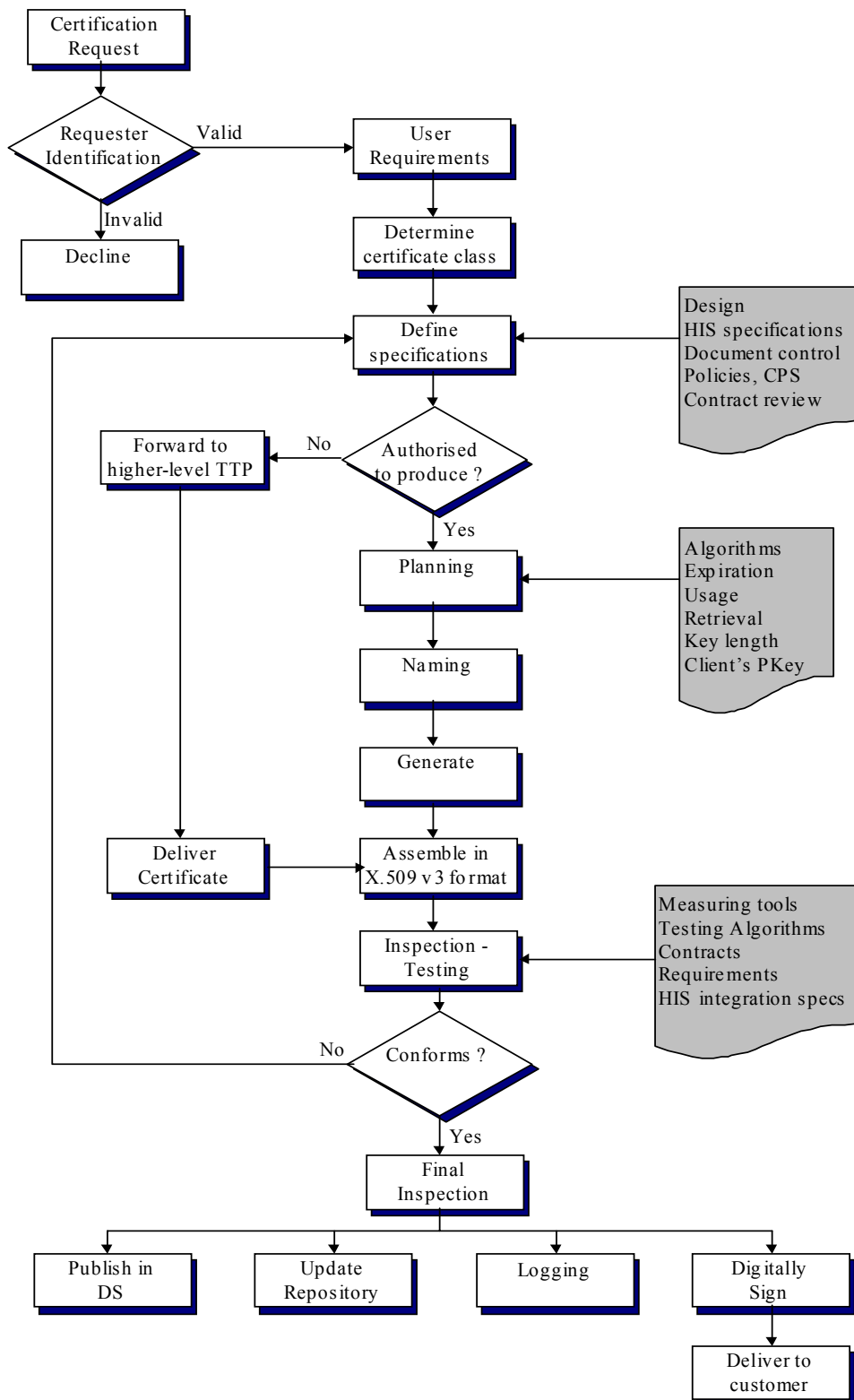
15. REFERENCES

- [1] ISO 9001 “Quality systems – Model for quality assurance in design, development, production, installation and servicing” 1994
- [2] ISO 9004-2 “Quality management and quality system elements – Part2: Guidelines for services” 1991
- [3] VeriSign, “Certification Practice Statement”, 1999, <http://www.verisign.com>
- [4] Entrust, “Certification Practice Statement”, 1999, <http://www.entrust.net>
- [5] Viacode, “Certification Practice Statement”, 1999, <http://www.viacode.com>
- [6] Castell, S. “Code of Practice and Management Guidelines for Trusted Third Party Services”, European Commission, INFOSEC S-2101 project, report no. 2, 1993
- [7] Commission of the European Community, “Green Paper on the Security of Information Systems”, ver.4.2.1, 1994
- [8] Kohnfelder, L. M. Towards a Practical Public-Key Cryptosystem, Ph.D. Thesis, 1978, M.I.T.
- [9] Kokolakis S., Gritzalis D., Katsikas S., "Generic Security Policies for Healthcare Information Systems", Health Informatics journal, Vol.4, No.3, pp.184-195, 1999, Sheffield Academic Press
- [10] KEYSTONE, Gritzalis, S. Katsikas, S. Lekkas, D. Moulinos, K. Polydorou, H. Patel, A. Gladyshev, P. “A European Cross-Domain PKI Architecture KEYSTONE ”, CEC DGXIII ETS-II ‘98 23187 project, EU, 1998

- [11] Swedish Medical Association “Information Technology: The Physician and the Patient” Stockholm, SMA, 1995
- [12] Hoyle, D. ISO-9000 Quality Systems Handbook – Third edition, BH, 1998
- [13] MEDSEC, Spyros Kokolakis, Dimitris Gritzalis, Sokratis Katsikas “Health Care Security and Privacy in the Information Society”, ISIS programme, EU, 1997
- [14] OPARATE, “Operational and Architectural Aspects of TTPs for Europe”, CEC DGXIII ETS-II ‘98 project, EU, 1998
- [15] D. Spinellis, D. Kokolakis, S. Gritzalis, S. “Security requirements, risks and recommendations for small enterprise and home-office environment”, Information Management and Computer Security, Vol.7, No.3, pp.121-128, MCB University Press, 1998
- [16] “An Overview of the PKCS Standards”, RSA Laboratories, 1993
- [17] RFC-2527, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, IETF, 1999



[Figure 1] : Classification and hierarchy of documents



[Figure 2] : Simplified process flow example for Certificate issuance