

Quality assured trusted third parties for deploying secure internet-based healthcare applications

Dimitrios Lekkas, Stefanos Gritzalis *, Sokratis Katsikas

Research Unit, Department of Information & Communication Systems, University of the Aegean, 30 Voulgaroktonou Str., Athens GR-11472, Greece

Received 10 July 2001; received in revised form 31 December 2001; accepted 9 January 2002

Abstract

In this paper we present a complete reference framework for the provision of quality assured Trusted Third Party (TTP) services within a medical environment. The main objective is to provide all the basic guidelines towards the development of a quality system for a TTP as an organisation, which could be mapped directly to the requirements of ISO-9000 standards. The important results of the implementation of a quality system, are the enhanced trustworthiness of the TTP and the confidence of the medical society in the provided services. Furthermore, the value added certification services conform to customer requirements and are characterised by efficiency, reliability, security, credibility and trust. The internal organisation acquires a clear and strict structure and maximises its effectiveness by establishing quality management, committed to control, assure and improve quality. The TTP requirements for quality are identified and the various elements of the quality system are described illustratively. © 2002 Elsevier Science Ireland Ltd. All rights reserved.

Keywords: Quality; Trust; Security; Public key infrastructure; Trusted third party; Health information systems

Abbreviations: CA, certification authority; CPS, certification practice statement; CRL, certificate revocation list; CSI, certificate status information; HIS, health information system; LRA, local registration authority; PKI, public key infrastructure; QoS, quality of service; TTP, trusted third party; URL, universal resource locator.

* Corresponding author. Tel.: +30-1-6492-112; fax: +30-1-6492-299.

E-mail addresses: dlek@aegean.gr (D. Lekkas), sgritz@aegean.gr (S. Gritzalis), ska@aegean.gr (S. Katsikas).

1. Introduction

Public Key Infrastructure (PKI) and digital certificates are emerging as one of the foundation technologies in the new economy and specifically in secure network-based medical environments. The set of public key certification services provided by a Trusted Third Party (TTP) are increasingly gaining momentum, as the Internet is becoming a primary media for healthcare communication-based applications.

A TTP may exist within the PKI as a governmental institution, as a private business or as a non-profit organisation. The scope of a TTP within Healthcare Information Systems (HIS) is to provide end-to-end security services, which are scalable, based on standards and useful 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 for quality. 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 two perspectives: The first is the Quality of Service (QoS), 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, which could be mapped directly to the requirements of ISO-9001 [1] and ISO-9004-2 [2]. The TTP requirements for quality will be identified and the various elements of the quality system will be described. They include QoS, management commitment, personnel responsibility, contract review, design, process and document control, verification, inspection and product identification. These elements will be analysed in association with the stated quality policy, the quality objectives and the Certification Practice Statement (CPS) [3].

1.1. The role of a TTP in secure environments

TTP 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 [4]. 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 PKI. 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, at least the following entities are involved within a TTP solution:

- **Certificate:** The term certificate was, first, used to refer to a digitally signed record holding a name and a public-key [5]. 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 owner:** This entity is the identified party bind to a certificate and the holder of the private key that corresponds to this certificate. It is known as the ‘subject’ of the certificate.
- **Certificate user** or ‘relying party’ is the entity that needs 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.
- **Certification Authority (CA)** is a functionally independent unit of a TTP, which manages (i.e. issues and revokes) a certificate. Due to the crucial role of these functions, the term CA is frequently used instead of the term 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 registration procedure 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.
- **Local Registration Authority (LRA)**, which handles identity verification material before the CA can issue a certificate to a user. The LRA also issues a certificate request on behalf of the user, among other related tasks. LRAs are appointed by CAs but may not delegate the authority to approve certificate applications.
- **CPS** which is a published declaration presenting the practices of the TTP in the provision of certification services. It details and controls the certification process from

establishing a CA to enrolling subscribers and managing certificates, as well as disclaimers, liabilities and limitations [6].

- **Directories** that serve as a repository for certificates issued, and also for publishing Certificate Status Information (CSI) such as Certificate Revocation Lists (CRLs) and delta CRLs [7].
- **Software** development kits and application program interfaces to TTP-enabled applications.
- **Interoperability 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.

1.2. 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 [8].

People involved in a medical environment need to be convinced that the following security characteristics of the healthcare information are preserved [9]:

- 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 get-

ting access to, due to a variety of personal reasons. The most influential of the stakeholders are healthcare establishments, healthcare professionals, medical researchers, 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 more complex 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. A quality-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.

2. Quality

According to [10] quality is defined as the totality of characteristics of the organisation, its services and its processes that bear on their ability to satisfy stated and implied needs. A service is the result generated by activities at the interface between the supplier and the customer and by supplier internal activities to meet the customer needs, while a process is a set of inter-related resources and activities, which transform inputs into outputs according to specified ways called procedures.

2.1. *The need for quality*

The biggest stimulation for the growth of PKI security services in fields such as healthcare or e-commerce, may not be technical expertise. It is the trust built between the Certification Service Provider and its part-

ners, customers, employees and other stakeholders. Indeed, trust has been the basis for commercial and social relationships through the ages. Within the new online economy the identities are more flexible, they may be mobile in destination and in origin and freed from the need of physical presence. This fact draws up new notions of trust, especially for a TTP whose operations are based by default on trust [11].

A TTP is by definition ‘Trusted’ for its operations and this is the key of its existence. In general terms a TTP is trusted by its clients for the accuracy of the binding between a digital certificate and a physical entity. It is also trusted for the accuracy, the integrity and the availability of any data provided to support secure communications, such as time-stamps, CRL and Directories. Finally it must be trusted for its commitment and its capability to perform the procedures described in its CPS.

The question raised is how this concept of trust will be established for a TTP as an enterprise or as an organisation. The keyword in the answer to the above speculation is ‘quality’. Quality may be perceived differently in the following basic business models, but it will enhance trustworthiness in both cases:

- **Business-to-consumer**

It is more likely that customers will have a greater sense of confidence against the value added security services provided by a TTP, that satisfy the user requirements and are efficient, reliable, secure and credible. Furthermore they want comfort that proper controls are in place within the security-related business processes.

- **Business-to-business**

The business partners such as other TTPs or e-enterprises that rely upon the security services provided, demand assurances that the TTP business processes and supporting

systems are well controlled and secured. In addition, they may require independent verification for the soundness of the internal procedures, such as an ISO-9000 certification.

There are numerous benefits, besides trustworthiness, that a TTP gains after deploying quality assurance procedures. The business partners, customers, employees and other stakeholders increase their confidence against the certification services provision. The quality services offered may lead to an advantage over the competition in terms of market share, revenues and customer satisfaction. As a result the name brand and image of the organisation will be strengthened. The development of control procedures will identify ways to improve the effectiveness and efficiency of security, controls, cost and other key capabilities during the service delivery process. Finally the establishment of a quality system proves that the management of the TTP is committed to the registered internal procedures and will not deliver any services below standards [12].

2.2. TTP requirements for quality

A TTP is an enterprise or organisation whose main activity is the provision of information security services [13]. As a service provider, the term ‘quality’ for a TTP has both technical and human dimensions. The requirements for quality are an expression of the needs or their translation into a set of quantitatively or qualitatively stated requirements that reflect customer needs and enable the realisation and examination of the services and the processes. The basic requirements for quality may be identified and categorised as follows.

Quantitative requirements including communication reliability, accessibility and availability of services and interfaces, promptness, responsiveness and cost. All of

them can be described in terms of measurable values such as bandwidth, failure percentage and absolute times, given also nominal values and tolerances.

Qualitative requirements such as dependability, efficiency, flexibility, robustness, usability, mobility, interoperability and ease of use. These requirements are not expressed in absolute values but they are comparable and subject to user perception and evaluation.

Requirements of society include obligations resulting from national and international laws and practices, technological standards and other considerations such as ethical principles, especially within medical environments. The accreditation and auditing of the TTP by an independent party must be also mentioned here.

Security requirements refer to specific functional characteristics of the services provided that will enable the customers to establish secure communications. A set of these requirements [14] is authentication, data integrity, confidentiality, non-repudiation, anonymity, key management, time-stamping and the publication of the CPS.

The totality of the above mentioned requirements have to be fulfilled in order to achieve the major goal, which is the customer satisfaction. The desired result of the achievement of this goal is the enhanced trustworthiness of the TTP and the customer confidence in the provided services. The mean for this achievement is the development of a quality system and the establishment of quality management aiming to control, assure and improve quality. Quality improvement is a continuous process affecting the life cycle of a service, known as quality loop. This concept is illustrated in [Fig. 1].

The TTP shall, therefore, implement, document and maintain a quality system that will provide confidence to both its own manage-

ment and the customer that the intended quality of its services is being achieved and which will ensure that the services provided conform to customer requirements. The basic elements of this quality system will be described in the next sections. The description will be illustrative rather than extensive and will have the form of guidelines, which could be mapped directly to the requirements of ISO 9000 standards.

3. Quality system

The quality system is a tool that enables the organisation to achieve its quality objectives either for control or for improvement. The first step for the establishment of a quality system is to define the quality policy of the TTP. The quality policy is defined [2] as ‘the overall intentions and direction of the organisation with regard to quality, as formally expressed by top management’. The quality system details the organisational structure, procedures, processes and re-

sources needed to implement quality management, which means to implement the objectives and responsibilities determined by the quality policy.

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.

The quality system of the organisation must be designed primarily to meet the internal managerial needs and it is broader than the requirements of the customers. A quality system includes the corporate quality policy, the quality objectives, a quality manual, the description of control procedures and the support documentation such as standards, guides, and operating procedures [15]. These elements will be described illustratively in the next paragraphs.

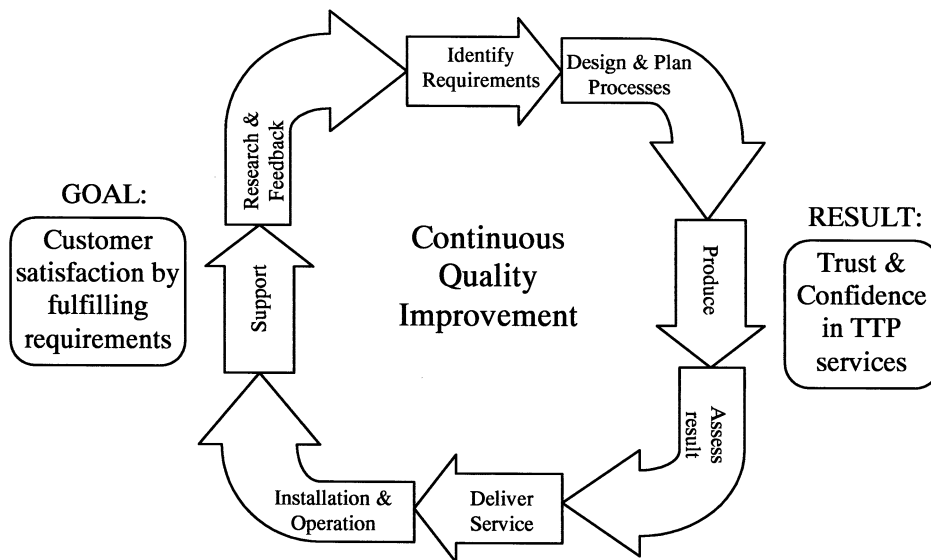


Fig. 1. TTP quality loop.

3.1. *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 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 [15]. 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 Registration Authorities 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 are thereby committed to 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.”

3.2. *Quality objectives*

Within a quality system the management has 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 within a medical environment could be summarised as follows:

‘The Public Certification Services of the TTP must be designed to support secure electronic communications within a HIS, 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 [16,15]. 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 [17]. The organisation will be offering any necessary resources in order to facilitate quick and reliable certification process and, therefore, it will be employing contemporary technology and properly skilled support personnel.'

3.3. Commitment

One of the values that the organisation should exhibit is its commitment to quality. The management shall be committed to the quality policy and objectives, to the internal procedures and to meeting its obligations to its customers and to society. Commitment can be defined either within the policy statement or stated separately and it should explicitly state that the management of the TTP:

- Is really doing at least what it states in the Quality Policy, in the CPS and in the procedures described by the quality system.
- Will perform quality assurance and quality improvement functions and will not distribute any products or services below standard.
- 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.

3.4. Personnel responsibility and authority

The responsibility, authority and interre-

lation 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 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 key stores.

3.5. Quality manual

The quality manual is a document stating the quality policy and describing the quality system of the organisation. The minimum contents of the quality manual of a TTP are:

- *The corporate policy* describing the mission, vision, values and objectives of the organisation, as already described.
- *Nature of business*: A TTP issuing, managing, verifying and suspending digital certificates and other related services such as time-stamping, archiving and key management in accordance with published CPS.
- *Procedures and instructions* of the quality system: description of practices and procedures employed by the TTP to perform CA services and evidence of the methods used in order to exhibit trust
- *The applicability of TTP services*, such as protection of communication, personal medical records and information assets, secure e-mail and time-stamping.
- *Responsibilities*, authorities and inter-relationships of personnel who manage, perform or verify work that affects quality.

- *Operational policies and the relative implementing procedures*, from receipt of customer inquiry through to delivery of service.

3.6. Operational policies

The operational policies defined within a quality system are reflected directly on the published CPS [6] of the TTP. 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. A set of TTP operational policies is given below.

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 which 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 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.

3.7. Quality system procedures

Procedures prescribe specific ways to perform the organisation's processes and activities, which transform inputs into outputs. 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 public directory.
- *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,

LRAs, Subordinate TTPs and Repositories), with other TTP hierarchies or with a HIS. 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 [12].

- *Standards* that refer to the control or operational procedures are also part of the quality system. Standards in most cases determine a measure for the quantitative characteristics of quality. For example a TTP may explicitly state in its CPS that the issued certificates conform with the X.509 [18] standard and that the exchange and verification of digital signatures is performed according to cryptographic message syntax standard PKCS # 7 [19]. 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.

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 [13], 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 [16] iden-

tifies the following topics as a set of security requirements, which the TTP services must fulfil:

- authorised access to health-related personal files;
- confidentiality and integrity of stored medical data;
- network security and confidentiality of transmitted patient information;
- determination of physicians roles and authorisation;
- education and awareness of users in security issues;
- 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 observable by the customer, but directly affect service performance [15].

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. The collected information contains valuable user judgements on various quality characteristics. This information is given as input to the design process, it contributes to the quality improvement and is part of the quality loop.

There are numerous quality characteristics of the TTP services that are subject to user

evaluation. Part of them is communicational, like the comprehensiveness and completeness of the Certificate Practice Statement [3] and the comprehensiveness of the service descriptions. Some others have to do with the general image of the service provider, such as the perception of its trustworthiness and the conformance with standards and state-of-the-art technology. The interaction with the service interfaces is another criterion and we may identify here the effectiveness and security of communication and the ease of use. Other measures are quantitative, such as the waiting times for delivery and processing, the helpdesk response, the strength of security keys, the network performance and the credibility and frequency of audits. Finally, we may identify the following additional qualitative characteristics subject to users evaluation [20]: Accessibility and availability of service; dependability of service in terms of confidentiality, reliability and integrity; certificates usability; registration accuracy and authenticity; accuracy and accessibility of directory and information repository.

The control of service quality characteristics can be achieved by controlling the design and 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. 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 [21]. It is rather an undertaking of obligations by the TTP for the provision of products and services against its customers, according to its CPS. It is required that the organisation establishes and maintains documented procedures for contract review.

Contracts and agreements must be reviewed for two important reasons. First, to ensure that the customer requirements are adequately defined and documented. Second, to assure that the organisation can cope with the undertaken obligations and to express limitations and liabilities. The starting point for the composition of a contract is the CPS. However, the following issues must be reviewed for every different case, according to requirements, conditions and obligations:

- The classes of certificates provided, their purpose and trust level. Examples of intended certificate usage within a HIS are [22]:
 - 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 or revoked certificate and 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 trustworthiness, reliability, accessibility, security, efficiency and credibility.

- The delivery of the products and the accessibility to the services, shall include:
 - key generation procedures and out-of-band exchanges;
 - the delivery of certificates (e.g. files, smart cards) and their format (e.g. DER, X.509);
 - the Universal Resource Locators (URLs) for retrieving the public key of the CA and the CRLs, as well as any information needed for certificate verification.
- The contractual requirements such as:
 - warranty and disclaimers;
 - any financial obligations and conditions;
 - legal issues, TTP liability and limitations;
 - subcontracting terms in case of registering a subordinate TTP;
 - customer prerequisites like equipment, material and skills.
- The managerial requirements, such as points of contact, plans for dealing with breakdowns, plans in case of cease of TTP operation and reports of progress and changes.

6. Design control

The TTP services have some tangible outcome that can be evaluated, whether it is a certificate, a time-stamp a digital signature or simply a document, and, therefore, they need to be properly designed to meet a given need. The establishment and maintenance of documented procedures to control the design of the products and services is part of the quality loop. Design control also applies to the design of items that support the core business, such as internal procedures, equipment, software and networks. It contributes significantly towards the quality improvement and ensures that the specified requirements are

met. The user requirements capture process is the first step, which provides the input for the design process [13] [17].

6.1. Design input

The collection of the minimal requirements that will constitute the input for the design process is performed either by customer feedback or by research. The first input derives from the general mission and the quality policy statement of the TTP. Design will never neglect that 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 patient, a physician or a hospital 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 HIS. International standards, national laws and IT industry practices should be taken into account as well as whether the TTP services are addressed to the international medical community, to a national medical system or to a specific organisation.

From the customer perspective, various parameters such as security, reliability, accessibility, cost, legal and ethical conformance, provide design input. The minimum specifications of the users' equipment must also be defined as well as the necessary skills they must have in order to use the TTP products efficiently and trustworthily.

The technological standards with which the TTP products and services need to comply are obviously basic design inputs. A sample summary of standards that could be used by a TTP includes: PKCS # 10 for certificate request [19]; X.509v3 for certificate format [18]; PKCS # 7 for certificate distribution;

RSA for encryption keys [19]; Lightweight Directory Access Protocol (LDAP) for CRL and certificate retrieval [7]; HTTP for enrolment; Secure Socket Layer (SSL) for secure Web-based communication; MD5 or SHA-1 or RIPEMD-160 hash functions for TTP-user or TTP–TTP secure communication and key exchanging [7]; Smart-card technology for private key storage [23].

The characteristics of the various interfaces to be implemented constitute another input. For example, the ease-of-use and the completeness shall characterise the end-user interface, while the standardisation, the security and the high availability shall be characteristics of the TTP-to-TTP or TTP-to-HIS interoperability interfaces.

Finally, any constraints that may affect the services provided, such as cost of equipment, proprietary technology, bandwidth usage, key export policies and any national statutory or regulatory requirements, must be considered.

6.2. Design output

Since services are delivered through processes, the service design is a matter of process design. The output of service design is a series of process descriptions and associated procedures. The form of the design output must contain readable information suitable to produce, inspect, test, install and operate the TTP services.

This information will probably include a hierarchy of documents starting from the human and material resources required down to hardware and software specifications. It must describe the flow of the processes from input to output, including all the interfaces with other ancillary processes. It may also include the measures needed to obtain customer feedback and to initiate service quality improvements.

The design output must be verified against its input, namely the customer needs. This is achieved by exploiting the customer feedback within the quality loop. Especially for new services, a grace period for ‘beta’ testing should follow the service design. During this period every aspect of the service will be examined closely to validate its design effectiveness and potential for delivering customer satisfaction.

7. Document and data control

Any information and data related to one or more requirements of the TTP for quality must be documented and this documentation must be controlled. 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.

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 consisting a reference in either of the above documents. A proposed document classification is illustrated in [Fig. 2].

8. Product identification

The TTP products—typically the certificates of various classes—must be clearly

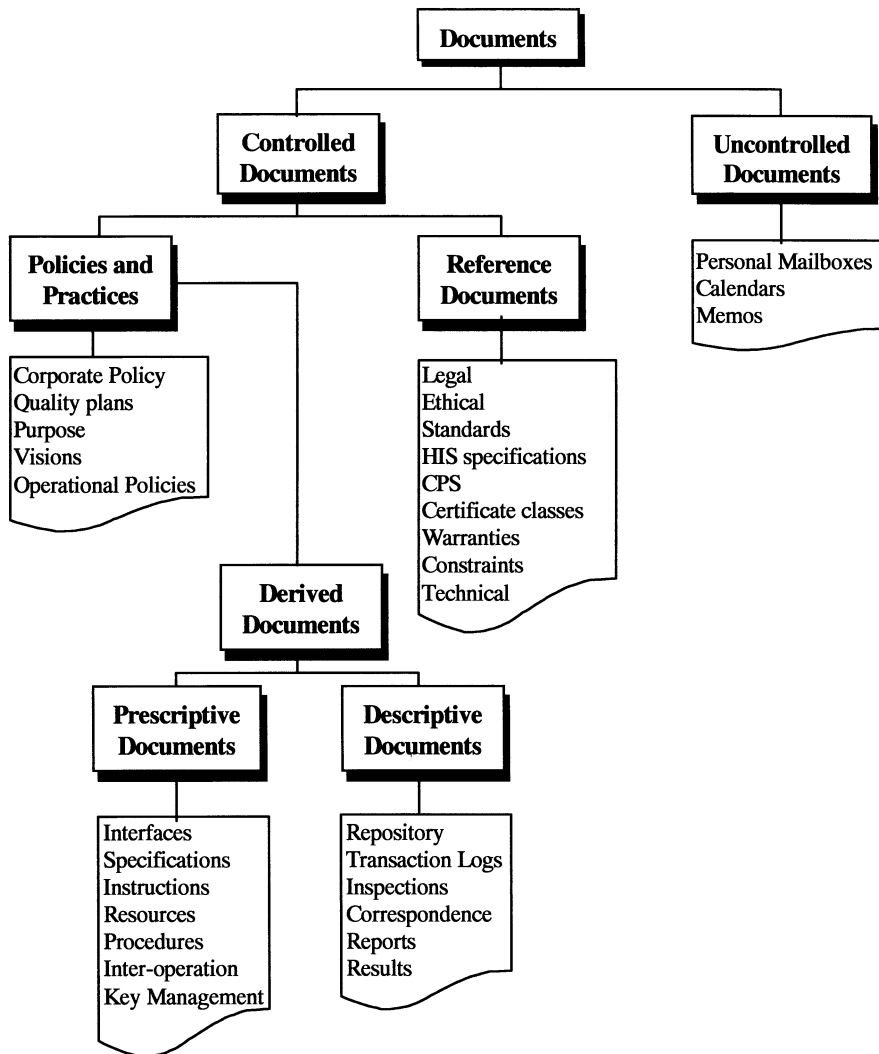


Fig. 2. Classification and hierarchy of documents.

identified and labelled in order to avoid misunderstandings and misuse and to facilitate the matching of the certificates 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 [21]. It is, therefore, necessary to be identified during all stages of production, delivery, installation, usage, verification and renewal.

Five certificate classes with particular usage

and trust in a medical environment are identified:

- Patient certificate (medium trust): for authentication, decryption and signing.
- Physician certificate (medium trust): for authentication, encryption, decryption, signing and time-stamping.
- Hospital certificate (high trust): for authentication, non-repudiation, signing and secure web servers.

- Subordinate TTP (high trust): for certificate signing and CRL signing.
- Public access certificate (low trust): for authentication only. Typically used for aggregate data retrieval by researchers, insurance agents and drug companies.

9. Process control

A process is defined [10] as ‘a set of inter-related resources and activities, which transform inputs into outputs’. A process within a TTP is a series of actions followed to implement the design and generate a final service. Such a process is cycled repeatedly, 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 service, the elements that drive the processes must be controlled and the results must be verified against quality standards.

In order to identify the production processes required to deliver a particular service, the service specifications are needed, which define the features and characteristics that are to be achieved. There are numerous other parameters that affect the design and implementation of processes, such as the specifications of the interacting HIS, the CPS and the quality policy, the contracts and other reference documents. An example of this concept is shown in [Fig. 3], where a simplified process flow example for certificate issuance is described.

10. Verification and Inspection of services

10.1. Testing

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. The organisation identifies the authority for inspecting and releasing products and services which in turn performs a set of actions to assure that the service to be delivered conforms to the stated and implied requirements. The activities of the testing authority are summarised as follows:

- Ensures that trustworthiness is kept through out the process of certificate issuance till certificate verification.
- Ensures that communicated data is incorruptible and keeps its integrity until it reaches its destination.
- Ensures the accuracy on supplying critical information, such as time-stamps and Identifies the necessary tools for testing them (e.g. Global Positioning System).
- Records and documents any non-conformities.
- Verifies that no information is dispatched unless it conforms to the specified requirements.

10.2. Corrective and preventing action

It is necessary to establish and maintain documented procedures for implementing corrective and preventive actions 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

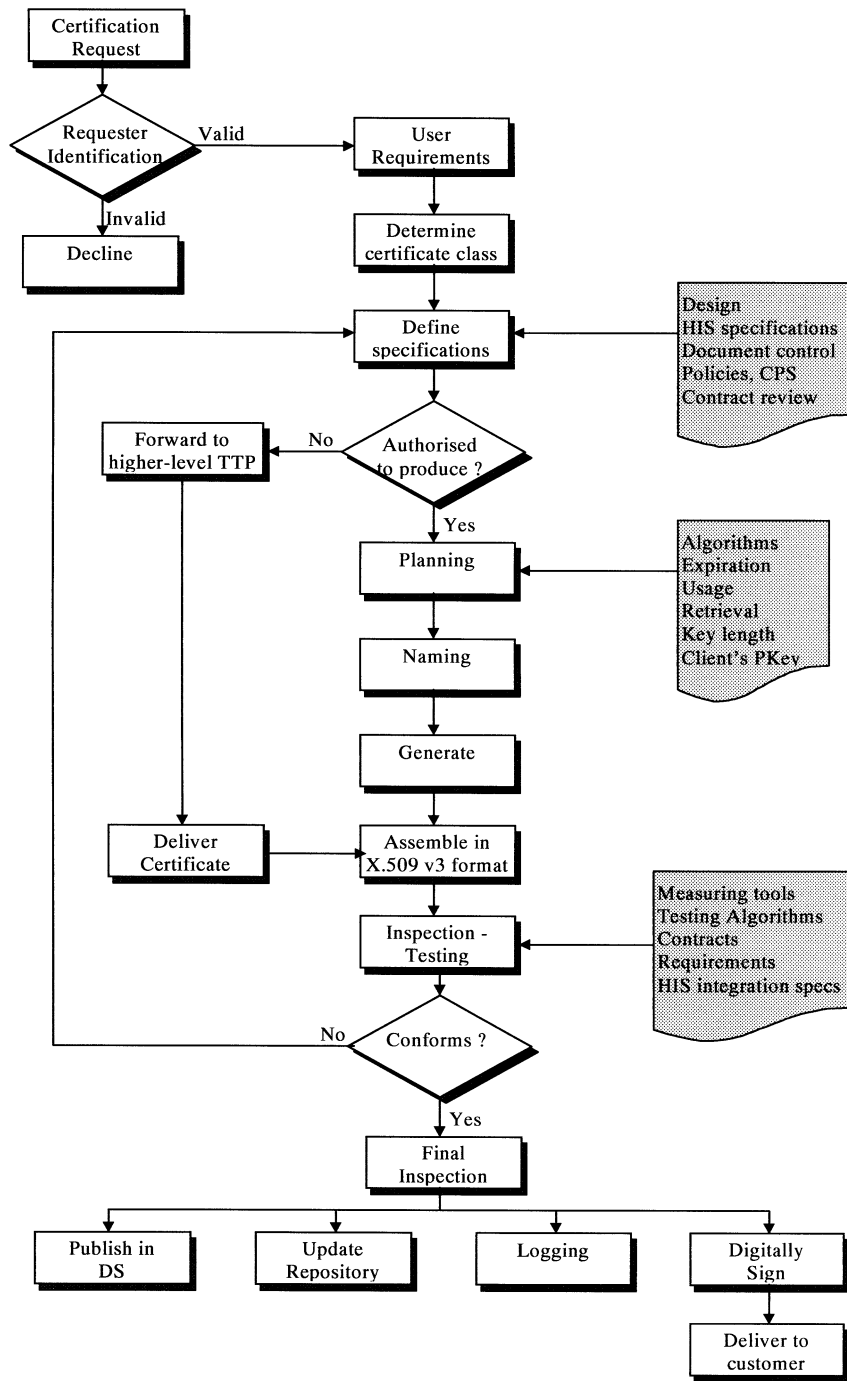


Fig. 3. Simplified process flow example for certificate issuance.

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 on 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.

11. 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 HISs 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 the identified requirements for quality. The introduction of a quality system and even the certification of a TTP according to the ISO-9000 standards [1,2] are a necessity, since the demand for more efficient and reliable security services grow. This quality compliance will be reflected in the CPS [6] and it will further promote the fundamental notion of 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.

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] Entrust Inc., 'Certification Practice Statement', available at <http://www.entrust.net>, 2000.
- [4] S. Castell, 'Code of Practice and Management Guidelines for Trusted Third Party Services', INFOSEC Project Report S2101/02, CEC/DG XIII/B6, 1993.
- [5] L.M. Kohnfelder 'Towards a Practical Public-Key Cryptosystem., MSc. Thesis, M.I.T., 1978.
- [6] S. Chokhani, W. Ford, 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework', Request For Comments 2527, IETF, 1999.
- [7] R. Oppliger, Security Technologies for the World Wide Web, Artech House Publishers, USA, 2000.
- [8] Commission of the European Community, 'Green Paper on the Security of Information Systems', ver.4.2.1, 1994.

- [9] S. Kokolakis, D. Gritzalis, S. Katsikas, Generic security policies for healthcare information systems, in: *Health Informatics Journal*, vol. 4, Sheffield Academic Press, 1999, pp. 184–195.
- [10] ISO 8402 ‘Quality management and quality assurance—Vocabulary’ 1994.
- [11] Ernst & Young “Cyberprocess certification and 3rd party reporting” Assurance and advisory business services brochure, 2001.
- [12] D.H. Besterfield, C. Besterfield-Michna, G. Besterfield, M. Besterfield-Sacre, *Total Quality Management*, Prentice Hall, 1995.
- [13] S. Gritzalis, S. Katsikas, D. Lekkas, K. Moulinos, H. Polydorou, A. Patel, P. Gladyshev, “KEYSTONE: A European Cross-Domain PKI Architecture”, EU DGXIII ETS-II project, 1998.
- [14] D. Lekkas, S. Katsikas, D. Spinellis, P. Gladyshev, A. Patel, User requirements of Trusted Third Parties in Europe, in: *Proceedings of the UIPP’99 IFIP International joint Working Conference on User Identification and Privacy Protection*, Kluwer Academic Publisher, Stockholm, 1999, pp. 229–242.
- [15] D. Hoyle, *ISO-9000 Quality Systems Handbook*, Third ed., Butterworth-Heinemann, Oxford, UK, 1998.
- [16] Swedish Medical Association “Information Technology: The Physician and the Patient” Stockholm, SMA, 1995.
- [17] OPARATE, “Operational and Architectural Aspects of TTPs for Europe”, EU DGXIII ETS-II project, 1998.
- [18] International Telecommunication Union, X-509 | ISO/IEC 9594-8, “The directory: Public-key and attribute certificate frameworks”, ITU, X-Series, Available at <http://www.itu.int>, 2001.
- [19] B. Kaliski, “An Overview of the PKCS Standards”, RSA Laboratories, Technical note, available at <http://www.rsa.com/standards>, 1993.
- [20] S. Gritzalis, J. Iliadis, D. Gritzalis, D. Spinellis, S. Katsikas, *Developing Secure Web-based Medical Applications*, in: *Medical Informatics*, vol. 24, Cambridge University Press/Taylor and Francis, 1999, pp. 75–90.
- [21] D. Spinellis, S. Kokolakis, S. Gritzalis, Security requirements, risks and recommendations for small enterprise and home–office environment, in: *Information Management and Computer Security*, vol. 7, MCB University Press, 1998, pp. 121–128.
- [22] D. Polemi, Trusted third party services for health care in Europe, in: *Future Generation Computer Systems*, vol. 14, Elsevier Science, 1998, pp. 51–59.
- [23] C. Lambrinouidakis, S. Gritzalis, Managing medical and insurance information through a smart card based information system, in: *Journal of Medical Systems*, vol. 24, Kluwer Academic Publishers, 2000, pp. 213–234.