

Towards an ISO-9000 compliant Certification Service Provider

D. Lekkas, S. Gritzalis, S. Katsikas

Abstract-- In this paper we present a complete reference framework for the operation of Certification Service Provider as an organisation. The objective is to form an intermediate reference model, to which the CSPs will conform, towards the full compliance to the ISO-9000 quality standards. There are two dimensions of quality in respect of a CSP: 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.

Index Terms-- Quality, Trust, ISO-9000 quality standard, Security, Certification Service Providers, Trusted Third Parties, Certification Authorities and Public Key Infrastructure

I. 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 environments. The public key certification services are increasingly gaining momentum, as the Internet is becoming a primary media for secure applications such as e-commerce and healthcare communication-based applications.

A Certification Service Provider (CSP) may exist within the PKI as a governmental institution, as a private business or as a non-profit research organisation and may appear by the more general term ‘Trusted Third Party’. The scope of a CSP is to provide end-to-end security services, which are scaleable, based on standards and are useful across different domains, geographical areas and specialisation sectors. The user requirements for various perspectives have to be extracted and satisfied.

Hereinafter the CSP will be referred also as ‘**organisation**’ and the users of the CSP services as ‘**customers**’.

Customers may be, but not limited to, individuals, enterprises, governmental organisations or other CSPs. The aim of a CSP 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 sensitive environments such as Health Information Systems and e-commerce. The objective towards this achievement is to form a reference framework for the operation of a CSP, 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 CSP 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 CSP, according to ISO-9001 [1] and ISO-9004-2 [2]. The requirements of the standard will be examined and their mapping to the CSP 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 CSP services provided to the society, the internal processes and control functions, and the published Certificate Policy and Certification Practice Statements (CPS) [3] [4].

II. THE ROLE OF A CSP IN SECURE ENVIRONMENTS

Certification Service Providers supply technically and legally reliable means for producing objective evidence concerning an electronic transaction and for data protection. Certification services are provided and underwritten not only by technical, but also by legal, financial, and structural means [5] [6]. CSPs 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 CSPs that issue and revoke certificates for users and other CSPs. The CSPs 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 CSP 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 CSP or 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.

Certification Practice Statement, which is a published declaration presenting the practices of the CSP 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.

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 CSP-enabled applications.

Interoperability mechanisms to establish and operationally maintain hierarchical and cross-certification trust relationships among different CSPs.

Policies that have been developed and govern the operation and the procedures of the CSPs.

III. QUALITY

According to [7] 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.

A. 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 partners, 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 CSP whose operations are based by default on trust.

A Certification Service Provider is by definition “Trusted” for its operations and this is the key of its existence. In general terms a CSP 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, Certificate Revocation Lists and directories. Finally it must be trusted for its commitment and its capability to perform the procedures described in its Certification Practice Statement. The question raised is how this concept of trust will be established for a CSP 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 CSP, 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 CSPs or e-enterprises that rely upon the security services provided, demand assurances that the CSP 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 CSP 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 CSP is committed to the registered internal procedures and will not deliver any services below standards.

B. CSP requirements for quality

A Certification Service Provider is an enterprise or organisation whose main activity is the provision of information security services. As a service provider, the term “quality” for a CSP has both technical and human dimensions. The requirements for quality is 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:

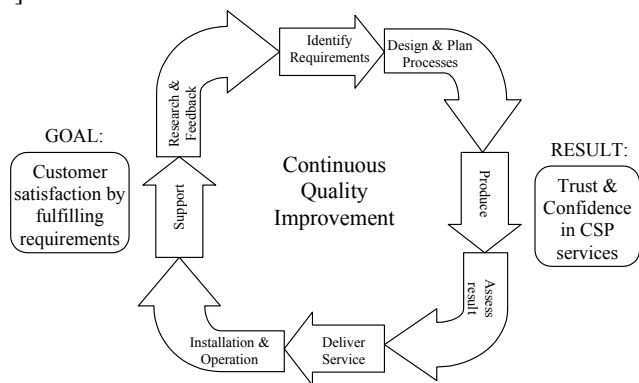
Quantitative requirements including communication reliability, accessibility and availability of services and interfaces, promptness, responsiveness and cost. All of them can be described in terms of measurable values such as bandwidth, failure percentage and absolute times, given also nominal values 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 CSP 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 [12] is authentication, data integrity, confidentiality, non-repudiation, anonymity, key management, time-stamping and the publication of the Certification Practice Statement.

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 CSP 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 [Figure 1].



[Figure 1] : CSP Quality Loop

The CSP shall therefore implement, document and maintain a quality system which will provide confidence to both its own management 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 ISO9000 standards.

IV. QUALITY OF SERVICE

A service is defined as the results generated by activities at the interface between the CSP and the customer and by the internal activities of the CSP, to meet customer needs. A complete set of CSP 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 CSP-to-CSP interoperability.

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 [13]. 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 CSP services that are subject to user evaluation. Part of them is communicational, like the Comprehensiveness and completeness of the Certificate Practice Statement [3] [4] 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 help-desk 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: 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 CSP 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.

V. MANAGEMENT RESPONSIBILITY

A. 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 [13]. An example of quality policy statement follows:

Our CSP 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 CSPs, 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 society with respect to the national and international laws and ethical principles, to the highest standards, security, safety, reliability and availability.

B. 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 CSP could be summarised as follows:

The Public Certification Services of the CSP must be designed to support secure electronic communications, to satisfy users' needs for data integrity, confidentiality, authenticity, availability and trust in their personal correspondence, business or research. It will support ethical principles of confidentiality and the citizens right for no-disclosure of any personal information unless they agree [14]. It will however support the availability of data necessary for research and knowledge spreading. The security functions of the CSP are addressed to a large, public, geographically dispersed community and they are enhancing users' trust against the CSP.

The main objective of the CSP 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 [15]. 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.

C. 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 CSP:

- 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.

D. 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 CSP 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

E. 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 CSP quality system the necessary resources include technical, human, finance, material and telecommunication resources.

VI. 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.

A. 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 CSP are:

- *The corporate policy* declaring the mission, vision, values and objectives of the organisation, as already described.
- *Nature of business*: A certification service provider 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 CSP to perform certification services and evidence of the methods used in order to exhibit trust
- *The applicability of a CSP services*, such as protection of communication, personal 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.

B. Operational policies examples

On personnel practices: The CSP 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 personal data or key repositories and to 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 CSP 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.

C. 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 CSP must be up to date with the latest technological evolution and the generic security policies of the HISSs.

D. 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 CSP, 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 CSPs and Repositories) or with other CSP hierarchies. The CSP will regulate the global access to data for users of different domains (even if they are certified by different CSPs) by providing cross-authentication mechanisms. An important issue for a CSP 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 CSP 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 [17]. 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.

VII. CONTRACT REVIEW

Each time the CSP receives a certification request and after the acceptance and the issuance of the, there is automatically initiated a binding agreement between the customer and the organisation [16]. It is rather an undertaking of obligations by the CSP 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:
 - 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 CSP services to fit for its intended purposes within a specific business 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 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, CSP liability and limitations
 - Subcontracting terms in case of registering a subordinate CSP
- 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 CSP operation and reports of progress and changes.

VIII. DESIGN CONTROL

The CSP 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 [10] [15].

A. 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 CSP. Design will never neglect that the purpose of the CSP and its services is to serve the 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 CSP 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 CSP services are addressed to the international community, to a national information 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 CSP products efficiently and trustworthily.

The technological standards with which the CSP products and services need to comply are obviously basic design inputs. A sample summary of standards that could be used by a CSP includes [10]: PKCS#10 for certificate request [RSA, 1993]; X.509v3 for certificate format; PKCS#7 [17] 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 CSP-user or CSP-CSP secure communication and key exchanging; Smart-card technology for private key storage.

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 CSP-to-CSP or CSP-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.

B. 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 CSP 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.

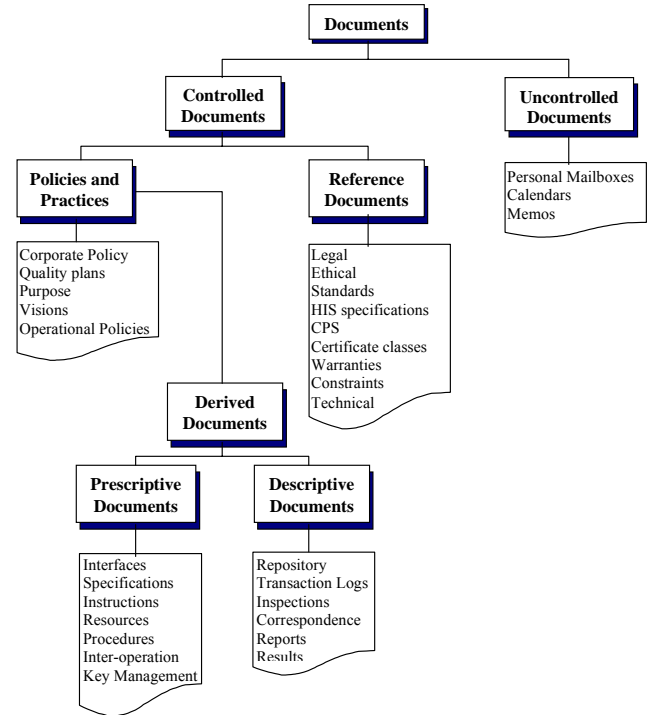
The design output must be verified against its input, namely the customer needs. This is achieved by exploiting the customer feedback within the quality loop. Especially for new services, a grace period for 'beta' testing should follow the service design. During this period every aspect of the service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

IX. 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 2], 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 which consist a reference in either of the above documents.

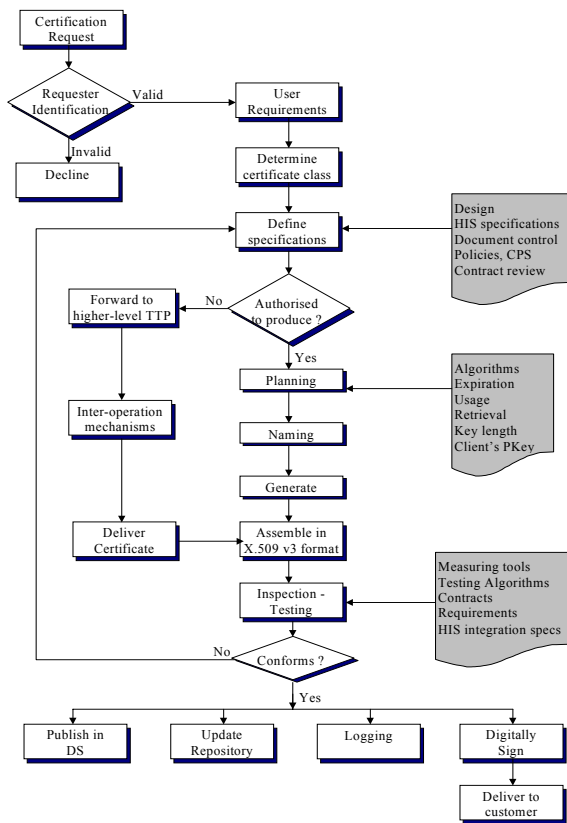


[Figure 2] : Classification and hierarchy of documents

X. 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 CSP, 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 3].



[Figure 3] : Simplified process flow example for Certificate issuance

XI. CONCLUSIONS

Enterprises and organisations invest in Information Technology and aim at improving the quality of commercial services they offer, while diminishing cost. The information systems they build are characterised as sensitive, high-risk systems since they are handling personal information and they are communication-based. 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 CSPs, that will enable the 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 CSP in Internet environment, according to ISO-9001 [1] and ISO-9004-2 [2]. The introduction of a quality system and the certification of a CSP 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 [18] and it will further promote the global trustworthiness of CSPs within the community. The CSPs/TTPs will further develop this framework in the future, towards the full compliance with the requirements of the standards.

XII. 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, "Certification Practice Statement", 1999, <http://www.entrust.net>
- [4] Viacode, "Certification Practice Statement", 1999, <http://www.viacode.com>
- [5] Castell, S. "Code of Practice and Management Guidelines for Trusted Third Party Services", European Commission, INFOSEC S-2101 project, report no. 2, 1993
- [6] Commission of the European Community, "Green Paper on the Security of Information Systems", ver.4.2.1, 1994
- [7] ISO 8402 "Quality management and quality assurance – Vocabulary" 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] Dimitrios Lekkas, Sokratis Katsikas, Diomidis Spinellis, Pavel Gladyshev and Ahmed Patel. "User requirements of Trusted Third Parties in Europe", UIPP'99 IFIP International joint Working Conference on User Identification and Privacy Protection, June 1999, Stockholm, Sweden, Kluwer Academic Publisher
- [13] Hoyle, D. ISO-9000 Quality Systems Handbook – Third edition, BH, 1998
- [14] MEDSEC, Spyros Kokolakis, Dimitris Gritzalis, Sokratis Katsikas "Health Care Security and Privacy in the Information Society", ISIS programme, EU, 1997
- [15] OPARATE, "Operational and Architectural Aspects of TTPs for Europe", CEC DGXIII ETS-II '98 project, EU, 1998
- [16] 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
- [17] "An Overview of the PKCS Standards", RSA Laboratories, 1993
- [18] RFC-2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", IETF, 1999