

Establishing and managing trust within the Public Key Infrastructure

Dimitrios Lekkas

*Department of Product and Systems Design Engineering
University of the Aegean, Syros Island 84100, Greece
tel: +30 10 6492042, fax: +30 10 6492399, e-mail: dlek@aegean.gr*

Abstract

The capabilities afforded by the Public Key Infrastructure certainly facilitate the growth of secure internet-based transactions. However, the provision of acceptable and effective certification services will only be achieved when an enhanced level of trust is established between the entities involved. Trust in the information society is built on various different grounds, based on calculus, on knowledge or on social reasons. The notion of trust against a Trusted Third Party expresses the customer's faith in specific operational, ethical and quality characteristics, while it also includes the acknowledgement of a minimum risk factor by the relying party. Trust has the properties of selectivity and transitivity and therefore it must be properly delimited and restricted. The trust relationships have to be effectively managed at the client side, where a trust database shall be maintained in three abstract levels, containing all the necessary information to enumerate, distinguish and evaluate the relationships with other entities. The major factors that affect trust are reflected in the requirements for quality of the services provided and in the terms and conditions of qualified policies.

Keywords

Trust, Security, Quality, Qualified policy, Trusted third party

1. Introduction

Public Key Infrastructure (PKI) and digital certificates are emerging as one of the foundation middleware technologies in the new economy and specifically in secure network-based 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 communication-based applications. A Trusted Third Party 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 an Information System is to provide end-to-end security services, which are scalable, based on standards and useful across different domains, geographical areas and specialisation sectors.

Hereinafter the TTP will be referred also as '**organisation**' and the users of the TTP services as '**customers**', which are distinguished in '**subscribers**' and '**relying parties**'. A subscriber is the party requesting secure services from the TTP and in the general case it is the identified party bind to a certificate and the holder of the private key that corresponds to this certificate. A relying party is the entity that needs to use and relies upon the accuracy of the information contained in a certificate or in other secure tokens provided by the TTP, such as notary and timestamps.

By studying the modern research projects and the commercial implementations on the field of PKI, we may identify two major problems. The first issue is that the designed TTP services

have minimal capabilities for interaction and interoperability, either on a functional level or on policy level. Consequently, serious limitations arise in the usability of such services by users who are moving between different geographical or business sectors, deploying different applications and interacting with users certified by different TTPs. The second issue is that the reasons why the society should trust the TTP are rarely mentioned. In most cases the notion of trust is not clearly identified and either the researchers do not address it or it is considered as de facto granted when using the commercial TTP services. The abovementioned problems, being the TTP services interoperability and the establishment of trust, are interconnected, since the interoperability between TTPs is partly relying on the existence of trust relationships, apart from the policy compatibility. On the other hand, the lack of a clear definition of trust and the lack of mechanisms for evaluating and managing the trust relationships, raise barriers not only against the TTP interoperability, but also against the usability of trusted services within the same TTP security domain.

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, as well as by establishing trust between the customers. The objective towards this achievement is to form a reference framework for the operation of a TTP, which conforms to functional, operational and quality requirements, as they are recorded in the respective policies. Failure to meet these requirements may have consequences in the trustworthiness that will adversely affect the customer, the organisation and the society.

The main objective of this paper is to analyse the concept of trust in connection with a PKI-enabled environment and to identify its meaning, its properties and the way it is established and managed. A trust relationship depends on many parameters and it is described by various categories of values. This information must be maintained by the trustor to be able to determine who, for what reasons, how much and for which actions one is trusted. The paper proposes a database schema that may be materialised on the client side and enable the relying party to fully manage its trust relationships. The factors that affect trust positively or adversely are then examined under two perspectives. The first perspective regards the characteristics of quality of the services offered and the second concerns the rules and procedures described in policies and the provision of evidence that the TTP conforms to them.

2. Trust

The concept of trust is fundamental for the very existence and operation of TTP as well as for all social activities of the community that bear any relevance with the services TTP provides. The fact that a third entity is trustworthy for the service it provides, strengthens the certainty that all parties involved in its activities are equally trustworthy. According to a Modern Greek dictionary, the definition of trust is the willingness to believe in the reliability, honesty, worthiness and capability of another entity. Respectively, the Oxford English dictionary defines trust as the reliance on a property or a virtue of a person, or the conviction that a given premise is true. Another, more detailed definition of the concept of trust, adjusted to the case of two parties involved in a transaction, can be found in [1] and it is the following.

“An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required”.

Thereinafter, an entity can be considered trustworthy, if the parties or people involved in transactions with that entity rely on its credibility. In general, the concept described above can be verbally represented by the term *reliability*, which refers to the quality of a person or entity that is worthy of trust. The term *reliability* also incorporates the concept of *discretion*, namely the ability to withhold personal and confidential information without disclosing it to a third party, the concept of *solvency*, which usually refers to secure financial or other kinds of transactions and finally the concept of *accrediting*, which refers to the official representation of the trustworthy entity by a person and to the social recognition of this entity by the community.

2.1 *The concept of trust and the information society*

In our modern age, most people spend the majority of their creative time interacting with other people whom they either don't know at all or have never met in person. And as it is stated in the [2] the meaning of the term 'stranger' has been transformed, as a result of modernism. In pre-modern civilizations, where local communities were the cornerstone of social structure, a 'stranger' was a person that came from the 'outside', the 'outlander' and who most frequently was suspected of possible unforeseen, unexpected activities. Earning the trust of such a community was not an easy task; it required time and effort. On the other hand, in post-modern society people started interacting in many different ways. Today, we constantly interact with nameless people and these interactions are brief and impersonal. This new phenomenon of ephemeral and impersonal interactions could be described with the term 'urban lack of attention', not in the sense of indifference but rather in the sense of a polite estrangement from one another.

The necessary trust for the successful execution of transactions and generally speaking, any kind of interaction in this post-modern urban environment of lack of attention, is acquired through two different ways: trust can develop firstly, between two parties that know each other well and it can be based on prior interactions or a long-term relationship. The second way refers to the general sense of trust that one has in the general social structures of their community, where sometimes the parties involved do not necessarily have to meet or make the acquaintance of one another. In this case, trust is ensured through the *access points* of the social system, which mainly represent the points of personal presence and commitment. This is where we can find the *representatives of the system*, who are the ones to interact with the community. The true trust relationship exists within the system and not at the access points, without however disregarding the importance of the human aspect of the actual representatives.

Furthermore, especially in the information society we locate four kinds of trust:

Calculus-based Trust: It is the most common kind of trust usually present at the commencement of a business relationship. The parties involved assess the degree of their dependency on the other entity, the expected profit and the possible risks in order to decide whether they will finally develop a trust relation with each other. This kind of trust is a result of careful calculations usually based on financial criteria [3].

Information-based Trust: As relations develop and interactions continue, the parties involved start collecting as much information as possible on the other parties, in order to enhance their ability to predict the behaviour of the other entities. The sense of uncertainty decreases, the possible risks are minimized and therefore, a trust relation can develop further.

Transitivity-based trust: In this category we classify the kinds of relations developed in the Public Key Infrastructure. The consolidation of a strong trust relation with a third entity indicates the transitivity property of that relation. Therefore, when one trusts a third entity, they are also inclined to trust the entities it points out or suggests, while providing them with useful, reliable information on them. [4].

Trust against the social system: Trust derives from the participation of a human being in a social system. In this case, the meeting, the familiarisation or the knowledge of details between the parties involved in a transaction, is not required. A typical example of this case is the monetary system and the bank transactions.

2.2 *Trust and PKI*

Since trust is an subjective notion, one of the most complex problems is the task of providing the concept of trust towards a TTP with a proper definition and framework. In many existing publications, the concept of trust has not been analysed sufficiently and its definition depends

entirely on the readers' reasoning. Since the aim of this paper is to define the concept of trust from the perspective of PKI, the following conclusions have to be underlined.

- Due to the distant and distributed nature of the TTP services, its activities and operations cannot always and at all times be visible or clear to its clients. It's also impossible for its clients to be fully aware of the technical details or the kind of technology it uses. Consequently, the interaction between TTP and customer is based to a certain extent on trust, since the parties cannot have complete knowledge of all this information.
- The trust one has in TTP is a two-dimensional concept: The first dimension refers to the faith in the moral integrity and the noble intentions that TTP and the people involved are supposed to bring in the interaction. The second dimension refers to the belief that the information system of the TTP is operationally and technologically sound. In this case the customer, who is incapable of knowing the structure or technical profile of TTP, trusts it on the grounds of her/his own perception of the soundness of its operation and the accuracy of the provided information. This is the reason why a quality system needs to be established, in order to strengthen this perception.
- On the other hand, one of the basic factors for the development of trust is the assessment of possible risks resulting from the very existence of a trust relation. Trust is strongly connected to the acceptance of a limited risk factor or to the certainty that risks have been reduced to an acceptable minimum, as the customer perceives it. It is also connected to the trust in the ability of the TTP to overcome an unforeseen, unfavourable result.
- Furthermore, customers trust the TTP for the security support it is supposed to offer in all transactions. The notion of *security* refers to a given situation where all possible risks are either eliminated or brought to an absolute minimum [2]. The customer's sense of security is determined practically by the extent of trust he has in the efficiency and reliability of the risk prevention and elimination mechanism TTP is supposed to possess.

Consequently, we can now reach an even more detailed definition of the concept of trust in the case of TTP.

'The notion of trust in a TTP could be defined as the customer's certainty that the TTP is capable of providing the required services accurately and infallibly, a certainty which also expresses the customer's faith in its moral integrity, in the soundness of its operation, in the effectiveness of its security mechanisms, in its expertise and in its abidance by all regulations and laws, while at the same time, it also contains the acknowledgement of a minimum risk factor, by the relying party.'

2.3 The properties of trust

The basic properties of trust in relation to TTP that should be discussed are two: the property of *transitivity* and the one of *selectivity*. A trust relation is transitive [5] when the fact that an entity A trusts an entity B and the entity B trusts an entity C, leads us to the conclusion that entity A is bound to trust entity C. Selectivity applies when trust in one entity is different and independent for every property that entity possesses and for every activity it executes.

In our modern society trust tends to be selective, but it lacks the property of transitivity. Besides, it would be rather surprising if the general concept of trust were indeed transitive, since that would probably lead to the paradox of one person resulting in trusting the entire world population. We also tend to trust certain people, based on various virtues they possess or certain choices they have made. For example, a person can trust a bank employee with his financial transactions, but have no confidence at all in the same person's driving skills. On the

opposite side, there are types of trust, which in many cases are closely connected to the global trust against an entity; that means that if one loses their trust in one entity for a specific function or task, it is very possible that this entity becomes totally unreliable and one is bound to distrust the entity in total.

In the case of TTP, the property of transitivity of trust is essential in order to ensure sound inter-operation, while there is a need of establishing specific restrictions and requirements. In particular, a general premise determining that ‘a user that trusts a TTP A can also trust a TTP B appointed by TTP A’ is applicable when:

- The TTP A provides the user with all necessary mechanisms and information to ensure a valid confirmation and documentation of the trust relation between TTP A and TTP B at all times.
- The transference property of trust is proposed but not imposed. The final decision on whether TTP B is to be trusted depends entirely on the user.
- The transference property cannot have infinite stages. The number of TTPs along which trust is to be transferred should be clearly stated and kept to a reasonable small figure.
- The policies by which both TTPs function are compatible or when there are adequate mechanisms to resolve possible conflicts.

Finally, it is generally desirable that trust also maintains its selectivity property. Trust towards a TTP should mainly refer to specific autonomous activities, such as certificate issuance, key management or time-stamping. The term ‘*authorised entity*’, which often replaces the term ‘*trusted entity*’, describes the very notion of trust in a specific set of activities. Respectively, if there is failure in trusting an entity for the processing of one activity, it should not cause a general trust failure. For this reason, the use of different certificates as well as cryptographic keys by every value-added service of the TTP, is recommended.

3. Trust Architectures

The establishment and the assurance of a trust relationship between two transacting parties shall be concluded as a result of specific acceptances, techniques and mechanisms. A TTP provides the necessary mechanisms for the establishment of trust relationships, by adding, in most cases, the property of transitivity in trust. The possible methods for establishing trust between different entities that participate in the PKI are the trust architectures or certification topologies and they must be distinguished as a concept from the communication architectures.

Three major categories of trust architectures may be identified. The simplest case is the establishment of explicit one-way trust relationships between individual end-users, forming a *web of trust*, without the involvement of other intermediate trusted parties. A typical example of this case is the PGP technology [6]. The second case is the establishment of a trust relationship between an entity and its *home TTP*, which consequently implies the transition of trust between all the entities of the TTP security domain. The last case is the architecture where multiple TTPs are involved. These TTPs are establishing trust relationships among each other and they are providing the necessary transitivity mechanisms to their users to build their relationships. These mechanisms eliminate any barriers in the users secure communication, even if they belong to different TTP domains. In any case the target is to find a minimal length *certification path* between the two transacting parties. This path is a directed chain of trust relationships, starting from the home TTP of the first party and ending at the second party. However, a trust architecture cannot be deployed as a stand-alone mechanism for enabling the interoperability between different TTPs, but it should be considered in conjunction with the issue of compatibility between individual policies.

Since the case of multiple TTPs involved in a trust architecture is expected to be the most common PKI architecture, it will be further analysed. Such an architecture may be

implemented simply by the establishment of a specific trust relationship between an end user and a TTP of another user, forming in this case a web of trust between end-users and TTPs. Another way is the initiation of trust relationships between TTPs by means of *cross-certification* [1] enabling trust transitivity between the end-users of each TTP. The third alternative is the establishment of *trust hierarchies*, where every end-user trusts the root TTP and consequently every other intermediate TTP and end-user. The cross-certification of root TTPs is also possible, creating a *forest* architecture. The disadvantage of this layout is that it usually results in long trust chains, thus weakening the final relationship. Two alterations of this model are proposed [7] addressing this problem: (1) the hierarchy based on *reverse certificates*, where the trust chain does not necessarily include the root TTP, but any common ancestor TTP and (2) the *directed graph model*, where any cross-certification between the TTPs of the hierarchy is possible, reducing consequently the length of the trust chain whenever it is necessary.

A modern and more interesting approach in trust architectures is the case of the involvement of a **trusted broker** or a **bridge certification authority** within the trust chain. A trusted broker is an entity, usually implemented on an organizational level, which nominates or recommends to the interested users the TTPs that may be considered as trusted. On the other hand a bridge certification authority [8] may be implemented even on a national level. It certifies different TTPs and provides a centralised mechanism to enhance interoperability standards among PKI service vendors. In both cases, different TTPs may operate within the PKI in a highly simplified architecture that minimise cross-certification management and enhances technical interoperability.

4. Limiting trust

As already described, trust may have the property of transitivity, through mechanisms like the cross-certification, trusted brokers, bridges and hierarchies or it may be delegated across different organisational levels. In any case it is possible that the resulting trust chain between two end-users becomes unexpectedly long. This long '*trust distance*' may introduce new risks and weaken the trust relationships, since the end-user has no control on this successive transitivity and in most cases cannot follow up the policies and practices of all the intermediate TTPs.

The restriction of trust distance is therefore a necessity in any trust architecture. The mechanism for the implementation of such restrictions is their embodiment in the certificates of the intermediate TTPs. The rules that limit the trust chain may be included in the certificate extension fields or the respective CPS and they are activated during the certification path validation procedure. These rules may have different targets, as for example:

- *Restriction of the length of trust chain*: Identifying a maximum number of transition steps may restrict the transitivity of trust to other TTPs. This number may be included for example within the cross-certificates.
- *Restriction of security domains*: A TTP may identify a set of other TTPs, which are considered as trusted and thus restricting the trust relationships of its users within this set of security domains. It requires that all the TTPs involved in a trust chain belong in this set, in order for the chain to be valid.
- *Restriction based on policy compatibility*: A certification is taking place according to a specific policy and TTP practices, which describe the rules and the conditions of this procedure. Typical examples of these conditions are the way of identity validation before the certificate issuance and the method applied to assure the uniqueness of the distinguished names. Stating these policy terms as critical, the trust chain will not extend to other TTPs that have policies with incompatible or conflicting procedures.

5. Functional management of trust

According to the general case of trust architectures, as already described, the identity certificate of an entity is acceptable and usable only in the case where one or more TTPs that exist in the certification path is trusted for the relying parties. Another case of a trusted certificate is the explicit declaration of trust against the entity by an individual. The consideration that arises out of these facts is how the declared or implied trust relationships are functionally managed on the application level at the client side.

A customer should have adequate information in order to be able to answer the following questions:

- Who is trusted and what is the need to trust her/him/it?
- What kind of entity is it?
- From which organisational level derives a trust relationship?
- Why a specific entity is trusted?
- For which functions or properties it is trusted, expressing the property of trust selectivity?
- How much it is trusted by means of absolute, comparable or objective values?

The widely used web browsers of Netscape and Microsoft have pre-selected some commercial Certification Authorities as being trusted by default for the certificates they issue. Although the user of the applications has the possibility to suppress these relationships, the fact of their pre-selection as trusted creates additional risks and raises suspicions of intended violation of the free competition rules. The reason of these possible negative side-effects is that the browsers and other related applications accept automatically and transparently the services provided by the pre-selected TTPs, misleading accordingly the ignorant user.

Aiming to an effective functional management of trust at the client side, we propose the creation and the administration of a trust database, named Trusted Entities List (TEL). This term denotes a superset of the already known term 'Certification Trust List' (CTL) and introduces a new concept in this context. Up to now the term CTL is used to denote a statically assigned list that contains only references to TTPs, including minimal information about the usage of their certificates. The term TEL designates a structured list that contains uniquely defined references to any trusted entity (not only TTPs, but to individual users, servers, services or sites) it is dynamically maintained in various levels and contains additional information that enables the end-user to enumerate, evaluate and distinguish her/his trust relationships with other entities.

In order to achieve the best possible efficiency in the management of trust, a TEL has to be maintained in three abstract levels, wherever this is applicable:

- *Enterprise level:* The TEL is maintained by the administration of the organization or the enterprise and contains entities that are qualified as trusted according to the general policy of the organisation. These trust relationships are proposed or imposed to the entities that participate in the organisation.
- *Information system level:* On this level the TEL includes the entities that are considered as trusted for the functions of the Information System of an organisation. The TEL is maintained by the system administrators according to specific security policies and the relationships it contains are reflected to the users of the particular IS.
- *Private personal level:* Every end-user maintains individually her/his personal trust relationships with other entities such as individuals, TTPs and sites. The user has the absolute authority to modify these relationships, which in any case remain private.

The entities that administer respectively the abovementioned levels of TELs are signing them in order to ensure their integrity and authenticity, before disseminating them to any relying party. The sets of trusted entities derived from each level may intersect. However the final decision to preserve or not the relationships of any level remains at the discretion of the end-user. As a result the entities that a user finally trusts are all the personal relationships plus a subset of the entities denoted by the enterprise level, plus a subset of the entities denoted by the IS level. This concept is depicted on [Figure 1].

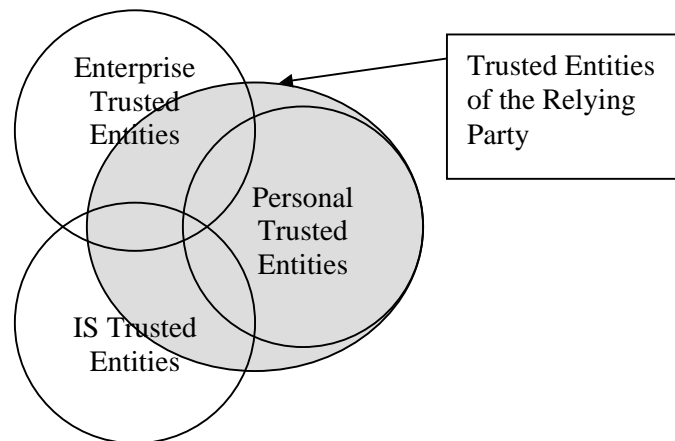


Figure 1. *Derived trusted entities of the Relying Party*

Another important functional requirement for the administration of the trust relationships is the possibility of performing automated procedures on the TELs at the application level. Therefore the TEL shall have specific structure, standard format and predefined classification of the trusted entities. We may distinguish the following classes:

- TTPs: root TTPs, hierarchically intermediate TTPs, cross-certified TTPs
- TTP services: Services that are operating autonomously using their own certificates, such as time-stamping, privilege management and non-repudiation.
- Sites and Servers: Named sites and servers that are explicitly declared as trusted, regardless of the TTP that certifies them.
- End-users: Physical entities that are explicitly declared as trusted, regardless of the TTP that certifies them.

For every entity listed in a TEL it is necessary to include its identity certificate and any additional details that describe for what reasons the subject entity needs to trust the target entity. For example, it may be an entity with whom the relying party has frequent secure transactions, it may be the home TTP or it may be a content provided that the trustor needs to use.

Since trust is selective, the declared trust against an entity is rarely global, whereas it is usually related to specific actions or properties. Consequently, for every entity contained in a TEL, the relying parties shall have the possibility to distinguish and declare the acceptance of the allowed usages or other properties contained in the entity's certificate.

The TEL must also contain a checklist, enabling the client to indicate and evaluate specific trust factors, which are introduced in paragraph [7.1]. These checklists may be predefined, however since the relying party may be not able to evaluate all trust factors, due to lack of knowledge or expertise, the required values should be either regarded as critical or ignored to

the discretion of the user. The values entered may be scalar, whenever the characteristics of a trust factor are measurable either subjectively or objectively. In any case the usage of binary values is not adequate and at least triple values must be used. A positive or negative value indicates a factor that increases or decreases trust respectively and the third value corresponds to a ‘do not know’ reply. Since lack of knowledge weights negatively in the establishment of trust, a ‘do not know’ reply shall be considered accordingly in the overall evaluation of trust for a specific entity.

An overall assessment of the trust against each entity shall be clearly noted in a TEL independently from the above checklists. Checklists may not indicate the reasons why an entity is generally trusted. For example an entity may be trusted for social reasons (e.g. being a governmental or banking institution) or it may be trusted due to the transitivity property. On the other hand the relying party may declare that she/he has adequate knowledge for the trusted entity and she/he can predict its actions or that trust is based on calculus, meaning that she/he evaluated several risk and profit factors and decided to trust it.

Incorporating all the above properties of trust and the requirements for its management, we propose the following database schema [Figure 2] for maintaining and managing all the necessary information. Summarising the previous analysis in accordance to the database schema, a trust relationship derives from a specific organizational level (e.g. enterprise, IS or personal) the entity is trusted for specific actions or properties, it is of specific type (e.g. TTP, server or individual user) it is trusted due to specific reasons (e.g. social, knowledge, calculus) the strength of the relationship depends on specific trust factors described in checklists and finally the administration of a relationship may be delegated to another party, which has specific privileges to perform specific actions.

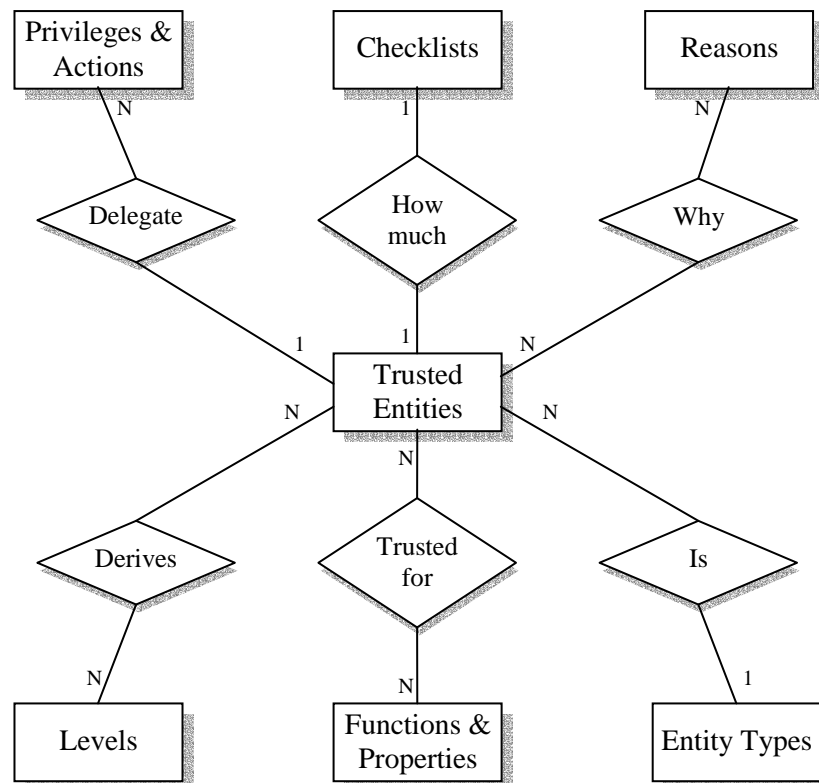


Figure 2. *Simplified Database entity-relationship diagram for Trust management*

Regarding the administrative functions of a TEL, we may identify manual operations by the TEL owner or any delegated entity, such as the manual insertion or deletion of entries

regarding trusted entities, the completion of checklists, the manual selection of accepted usages and the designation of security policies that apply. Accordingly, there are automated operations, such as the insertion of a home TTP, its subordinate or cross-certified TTPs, the automatic insertion of individual entities for which their reliability is accepted indirectly by other actions (e.g. the explicit acceptance of a server certificate during a secure http session or the acceptance of the certificate of the sender of a digitally signed message) and the automatic deletion of entries related to entities whose certificates are expired, suspended or revoked.

6. Trust Factors

The factors that determine whether an entity is trusted and furthermore how much trusted it is, are certainly objective. Trust is built from experience, personal knowledge and sometimes bias. It has also a contextual element to it, based on the action that the trustee is about to take. However there are several factors that may be measurable or comparable for a relying party in order to decide the amount of trust placed against a TTP. An attempt of evaluating trust is already recorded in [9] where an expert system is built that computes a trust quotient. Two major categories of trust factors are identified and analysed in the next paragraphs: (1) the quality of the services offered and the quality of the internal management, which indicate the intention of the TTP to satisfy the needs of the users; (2) the rules and procedures described in policies and especially in the CPS [10] and the provision of evidence that the TTP conforms to them.

6.1 Requirements for quality

In general terms a TTP is trusted by its customers 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.

According to [11] 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. By deploying quality assurance procedures a TTP strengthens its trustworthiness. 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].

A Trusted Third Party is an enterprise or organisation whose main activity is the provision of information security services. 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 used to evaluate the trust against a TTP and may be included in the recording of trust factors as described in paragraph [5]. They are identified and categorised as follows:

Quantitative requirements include 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, ease of use and comprehensiveness of the Certification Practice Statement. 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. An indicative subset of these requirements [13] is authentication, data integrity, confidentiality, non-repudiation, privacy, key management and time-stamping.

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.

6.2 *Quality of Service*

A service is defined as the result generated by activities at the interface between the supplier and the customer and by the internal activities of the TTP 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 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.

The Quality of Service (QoS) is described in terms of a set of features and characteristics that are observable and subject to customer evaluation [14]. They are expressed in common language that can be understood by the user and as a number of parameters. 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 [10] 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, while there are numerous measurable, comparable or subjective characteristics as described in paragraph [6.1].

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.

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 reduced human intervention. Therefore, the more definable and documented the processes, the easier to apply structured and disciplined quality system principles.

6.3 *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.

6.4 *Personnel responsibility and authority*

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

Within a TTP the personnel shall possess experience and qualifications necessary for the offered services and specifically in the public key cryptography and the electronic signature technology. The personnel shall be formally appointed to trusted roles, such as [15]:

- Managerial roles, defining the quality policy and objectives and allocating human and material resources.
- Security officers, having the overall responsibility the administration and the implementation of security practices.
- System administrators and operators authorised to install, configure and operate the trustworthy systems of the TTP. They may eventually have access to sensitive data.
- Auditors, responsible to maintain, view the audit logs of the trustworthy systems and to provide reliable information as needed.

7. Conformance to qualified policy

In general, the purpose of a certificate policy, referenced by a policy identifier in a certificate, states the requirements of the business, bounds the TTP security domain and determines the general rules of the operation. More specifically a certificate policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. A certification practice statement, on the other hand, consists of operational units, which define the practices and procedures of how these policies are to be carried out.

The term '*Qualified*' [16] is used to indicate that the policy incorporates specific standard requirements such as those described in the European Directive [17] on digital signatures as well as the requirements stated in [15]. Although the abovementioned documents are concerned only with certification services and not with other value-added functions such as time-stamping or notary, there are significant general terms for the operation of a qualified TTP that apply beyond certification services. In this context these requirements are considered as the basic trust factors where a relying party may be based, in order to decide how trusted a third party is. However, the sole embodiment of terms addressing these

requirements in the policy of the TTP does not imply trust enhancement. Additionally a TTP shall:

- Claim conformance to the identified qualified policy and make available to subscribers and relying parties on request the evidence to support the claim of conformance;
- Be possibly assessed to be conformant to the identified qualified certificate policy by an independent party and deploy audit trail procedures;
- Disseminate terms and conditions and ensure that they are clearly expressed and comprehended by the interested parties;
- Deploy procedures to maintain and administer the qualified policy and deploy review procedures to address new requirements.

Since PKI is still in its infancy and therefore consensus is not reached yet, nor it is a part of our social activities, the evaluation of trust factors is not a straightforward procedure. A TTP subscriber or relying party shall record the checklists of her/his trust database as described in paragraph [5], based on his knowledge or intuition about the capability of the TTP in satisfying several functional requirements, apart from the requirements for quality indicated in paragraph [6.1]. The specific policy terms and conditions that weigh significantly towards the establishment of trust against a TTP are quoted in the next section.

7.1 Important policy terms and conditions

The certainly most important procedures for the establishment of trust are those related to key management, regarding either the keys belonging to the TTP or to the subscribers. In case the TTP maintains subscribers' private keys for key escrow reasons, it shall protect them from usage by unauthorised entities wishing to decrypt confidential information. Furthermore, the TTP shall exhibit its commitment to follow strict procedures regarding the management of its own keys, such as:

- the private keys are generated and stored in physically secured environment by trusted personnel under at least dual control [15] and thereafter they remain confidential and maintain their integrity;
- the devices used shall meet the requirements set by various standards, such as the CEN workshop agreement [18];
- the integrity and authenticity of the public keys and any associated parameters are maintained during their distribution to relying parties.

Another important issue is the procedures to reliably verify the identity of a subscriber during her/his registration, as well as the identification of the subscriber's organisation and the usage of valid and unique distinguished names. The TTP shall disseminate the details of the registration procedure to the relying parties for each certificate issued. Since the usage of PKI services relies on the bind of the identity of the physical entity with its public keys, the registration procedure is a significant trust factor.

Among the other value-added services provided by a TTP we may identify numerous functional requirements that play a significant role in the establishment of trust. Such examples may be: the accuracy of the secure tokens provided by the notary or time-stamping services; the validity of the information provided to support non-repudiation and dispute resolution; the dependable certificate management, meaning that the TTP establishes accurate revocation procedures and ensures proper publishing of Certification Status Information.

Among the TTP obligations, the most important is its commitment to the satisfaction of all functional and quality requirements as applicable to the qualified policy and that the services provided are consistent with its CPS. Apart from TTP obligations, there are also subscriber

obligations, which are fundamental in establishing trust between PKI users, such as the obligations related to the creation, storage and usage of private keys. For the same reason, the obligations of the relying parties are also important, such as the reliable verification of the certification status information and the conformance to the limitations on the certificate usage.

Regarding the general operational and managerial requirements for the TTP as an organisation, there are several terms and conditions related to trust enhancement, apart from the quality requirements. Specifically, the TTP shall be concerned about physical security and ensure that physical access to critical devices is control and that physical risks to its assets is minimised. Furthermore, it shall deploy and maintain trustworthy systems, regarding both software and hardware and ensure that the systems are correctly operated with minimal risk of failure.

The existence of an effective disaster recovery plan is another important trust factor. A disaster includes the compromise of any of the TTP private keys, in which case the TTP shall ensure that the customers' damages are minimal and operations are restored as soon as possible. The continuity process in this case shall include the revocation of respective certificates or tokens and the dissemination of the incident to all subscribers and relying parties. Respectively, the TTP shall make provision of legal proceedings for the case of the cessation of the TTP services and ensure that potential disruptions to customers are minimised.

Finally, the TTP shall ensure the proper dissemination of all the above terms and conditions regarding the usage of certificates and services. Additionally, the TTP shall make available to subscribers and relying parties supplementary information regarding any limitations on service usage, limitations of liability, procedures for complaints and dispute settlement, the applicable legal system and information on how to validate the TTP certificates, procedures and services. Particularly, the statement of liability and possible indemnification of the relying parties contributes towards the establishment of *calculus-based trust* (see paragraph 2.1) since this statement gives the possibility to the users to evaluate eventual risks and benefits of financial nature.

8. Conclusions

The growth of PKI-enabled electronic market is still on its first steps. To fully reach the potential of the certification services provided by a Trusted Third Party, proper mechanisms should be set up to establish trust and encourage confidence in online transactions. The objective towards the establishment of trust is to form a reference framework for the operation of a TTP, which conforms to functional, operational and quality requirements, as they are recorded in the respective policies. Failure to meet these requirements may have consequences in the trustworthiness that will adversely affect the customer, the organisation and the society. The notion of trust against a Trusted Third Party expresses the customer's faith in specific subjective and objective characteristics, while it also includes the acknowledgement of a minimum risk factor by the relying party.

On the other hand, a trust relationship for a subscriber or a relying party depends on many parameters and it may be based on calculus, on knowledge, on transitiveness or on social reasons. The information that fully describes a trust relationship must be maintained by the trustor in order to be able to determine who, for what reasons, how much and for which actions one is trusted. The paper proposes a database schema that may be materialised on the client side and enable the relying party to fully manage its trust relationships. The factors that affect trust positively or adversely are then examined under two perspectives. The first perspective regards the characteristics of quality of the services offered and the second concerns the rules and procedures described in policies and the provision of evidence that the TTP conforms to them.

The requirements for quality may be quantitative, qualitative, social or related to security properties, while the quality of service is described in terms of features and characteristics that are observable and subject to customer evaluation. A TTP must provide evidence that it conforms to a qualified policy, where the most important terms and conditions relate to the key management, the accuracy of identity verification, the conformance to the CPS, the physical security, the continuity plan and the limitations on liability.

It is certain that future work will focus on the standardisation of a framework for establishing, managing and evaluating trust, since this is an essential requirement for the evolution of PKI.

References

- [1] 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
- [2] Giddens Anthony, “The Consequences of Modernity”, pp.29-36 & 83-111, Polity Press, UK, 1991
- [3] Ba Sulin, “Establishing online trust through a community responsibility system”, Decision Support Systems Vol.31, pp.323-336, Elsevier Science, 2001
- [4] Fernandes Andrew, “Risking Trust in a public key infrastructure: old techniques of managing risk applied to new technology”, Decision Support Systems Vol.31, pp.303-322, Elsevier Science, 2001
- [5] Vincent Buskens, “The social structure of trust”, Social Networks, Volume 20, Issue 3, pp.265-289, July 1998
- [6] Zimmermann, Ph., “Pretty Good Privacy - Public Key Encryption for the Masses. PGP User's Guide”, Vol 1&2. PGP Version 2.6.1, Cambridge, MA, MIT Press, 1995
- [7] Menezes A., Oorschot P., Vanstone S., “Handbook of Applied Cryptography”, Series on discrete mathematics and its applications, CRC Press, 1997
- [8] Alterman P., “The US Federal PKI and the Federal Bridge Certification Authority”, Computer Networks, No.37, pp.685-690, Elsevier Science, 2001
- [9] Chadwick D.W., Basden A., “Evaluating trust in a public key certification authority”, Computer & Security, Vol.20, No.7, pp.592-611, Elsevier Science, 2001
- [10] Chokhani S., Ford W., “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, Request for Comments 2527, IETF, March 1999
- [11] ISO 8402 “Quality management and quality assurance – Vocabulary” 1994
- [12] Besterfield D. H., Besterfield-Michna C., Besterfield G., Besterfield-Sacre M., “Total Quality Management”, Prentice Hall, 1995
- [13] Gritzalis S., Katsikas S., Lekkas D., Moulinos K. and Polydorou E., “Securing The Electronic Market: The KEYSTONE Public Key Infrastructure Architecture”, Computers & Security Journal, Elsevier Science, Vol.19, No.8, pp.731-746, December 2000
- [14] D. Hoyle, “ISO-9000 Quality Systems Handbook”, Third edition, Butterworth - Heinemann, Oxford, UK, 1998
- [15] ETSI, “Policy requirements for certification authorities issuing qualified certificates” Draft TS 101 456, European Telecommunications Standards Institute, 2001

- [16] Santesson S., Polk W., Barzin P., Nystrom M., “Internet X.509 Public Key Infrastructure, Qualified Certificates Profile” Request for Comments 3039, IETF, January 2001
- [17] Directive 1999/93/EC of the European Parliament and of the Council, “Community Framework for Electronic Signatures”, December 1999
- [18] Farrukh Ahmad, “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures”, CEN/ISSS Workshop on Electronic Signatures, Draft CWA 14167-1, July 2001

Dimitrios Lekkas holds a Ph.D. in the area of Information Systems Security and an M.Sc in Information Technology. He is currently teaching at the department of Systems and Product Design Engineering, university of the Aegean, Greece. He has participated to many research projects funded nationally and by the European union and published several papers in international journals and conferences. He is a member of of Greek National Educational Network (EDUnet) technical committee and coordinator of the Greek academic network Computer Emergency Response Team (GRnet-CERT). His current research interests include computer security, incident response, public key cryptography, database management systems, dynamic web design and distributed systems.