Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

8th International Conference
on Electrical Engineering
ICEENG 2012

A Performance Analysis Methodology of a Public Key Infrastructure

By

Dr.Tarek Abdel Mageed * **Asem A El- Ashqar** ** **Prof. Ali Ali Fahmy** ***

Abstract:

Recent years have seen rapid growth in the number and scope of standards dealing with aspects of Public Key Infrastructures (PKIs). This has primarily been fuelled by the much increased interest in implementing PKIs, which is itself largely a result of the development of commercial and wider public use of the Internet, not least for e-commerce activities. With the growth in awareness of, and requirements for, PKIs, there has been a parallel increase in development effort devoted to standardizing all aspects of PKIs and PKI assessment measures helping the performance analysis of these PKIs. The potential benefits are clear, including the possibility of large scale interworking between PKIs, and lower costs through economies of scale and increased competition.
This paper is devoted as a guide to present the assessment criteria of a PKI system providing the reader with different views of these assessment measures. The assessment measures applied to a PKI during this process have different perspectives. One of them is derived from The Information Security Committee (ISC) that published, in 2001, a draft of their PKI Assessment Guidelines (PAG) v0.30 for public comment which assumes that the set of policies, standards and procedures, as well as other PKI related documents, must be established before going onto the assessment procedures. The other perspective, relies on the ISO standard model published and have been used in the PKI assessment measures in many organization. The last perspective concentrates on the core of any PKI system, which is the security strength of this system and how to execute a security diagnosis to a PKI. In other words, can the organization trust it, through its continuous assessment procedures, as a secure system for its daily network communication transactions?. This paper organized so that it starts with a basic introductory part for the

* E-Gov Security Consultant
** IT Consultant Engineer
*** Cairo University, Faculty of Computer and Information

PKI system from different views, and continuing with explaining the components of a PKI system. Then exploring the different assessment visions to measure the performance analysis a PKI system such as PAG assessment guidelines, and the ISO 27001 standards, ending with an opinion to add some suggested security strength measures to the well known and published assessment measures for the performance analysis.

Keywords:

Performance analysis, public key infrastructure, and PKI.

1. Introduction:

Public Key Infrastructure (PKI) is one of the current widely used words, and there are a lot of issues surrounding the implementation of a PKI. The term PKI is derived from public key cryptography, the technology on which PKI is based. PKI constitutes the core of an Internet security infrastructure and is the key to ensuring authentic and private communications. Many definitions are introduced for this term, PKI:

- PKI is a comprehensive set of functions supports security mechanisms such as confidentiality, integrity, authentication, and non-repudiation (Jianying & Moti, 2010).
- PKI has been widely recognized as a fundamental technology process for supporting digital communication (Liu et al, 2001).
- An enterprise PKI can be seen as a collection of policies, procedures, roles, responsibilities, decisions, services and controls for using public-key cryptography within an organization, across applications (Murray, 1999).

From different definitions and different viewpoints of individuals to PKI, we can re-formalize this view and to look to PKI as a set of hardware equipments, software programs, encryption technologies, people utilizing, policies, standards, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on public-key cryptography.

With PKI being implemented in global organizations at an increasing rate, assessing the security of these PKIs is increasingly important as well (ISM, 2000). In general, PKI assessment is the process of determining whether a PKI satisfies a set of defined criteria. Assessment can take various forms, including self-assessment, formal audits, and rigorous technical evaluations. Therefore, the term “assessors,” includes inspectors, auditors, accountants, and information security professionals and the entities they represent.

The problem that will be addressed in this paper is to explore some different views to

assess the security strength of a PKI. The basic theme of most articles reviewed saying that PKI assessment is a very important and valuable process. However, most also contain one or more of the following themes:

- PKI is not what people think it is Ellison, & Schneier, 2000).
- PKI cannot work the way that people think it will work (Bhimani, 2000).
- PKI is extremely challenging to implement (Bhimani, 2000).
- There are counter-points to the risks identified in other articles (Brands, 2000).

Regardless of the varied opinions and statements, the common theme of all of these articles is that PKI is NOT an application, **but a process**. In fact, many of the articles reviewed indicate that it is "easy" to implement the software to support a PKI, but the "I" – the Infrastructure is the most difficult to achieve. The single biggest problem with PKI is that organizations forget that the "I" stands for "infrastructure." PKI is 10 percent technology and 90 percent policies and procedures, which is not easy to deploy and maintain (Rothke, 2001).

This brings us to the problem that will be addressed in this paper, which is that it is challenging to conduct a security assessment on a PKI. It has been shown that a PKI is a process and not an application, and since all processes have rules that need to be followed, the owners of the information being secured by a PKI need to have assurance that the rules are being followed.

2. PKI Basic components:

PKI components are the elements that comprise a public key infrastructure, including entities (such as CAs) and individuals (such as subscribers) participating within the system, technologies (such as algorithms and key generation software), processes (such as key management procedures), records (such as digital certificates), and policy instruments (such as CPs and CPSs). These components can be organized in a simple way as follows, explaining every component role in the PKI system:

- Certification authority which generates, revokes, archives and publishes public key certificates.
- Subscribers to the PKI system who are individuals and/or organizations operating the private key corresponding to the public key within the certificate.
- Relying parties such as individuals and/or organizations relying upon the certificate to use the public key within that certificate.
- Registration authority which assists CA to oversee key generation and authenticate the identity and/or other attributes of a certificate applicant, initiating the revocation of certificates upon a subscriber's request or otherwise, and approving or rejecting requests to renew or rekey a certificate).
- Repositories (Certification Archives) which are entities and/or organizations contain

an archive of all certificates and Certificate Revocation Lists (CRLs) and providing publication, storage, and access to certificates and other PKI-related information.

The process of how these entities work together needs to be documented in CP and the CPS. These documents will drive the creation of, or become part of the existing policies, standards and procedures that every organization should have (Austin, 2001). It should be noted that realistically, some level of policies, etc., exists at an organization that has the need for a PKI. The participants within a PKI use the PKI technologies to establish a secure infrastructure to issue certificates, collect certificate applications, validate those certificate applications, issue certificates, publish or distribute certificates, revoke certificates, renew or rekey certificates, and ultimately decommission the infrastructure. The participants use these processes consistent with security policies and practices

*3. **PAG PKI Assessment Guidelines:***

Much work has already been done in the area of PKI assessment measures and performance analysis of the PKIs. The Information Security Committee (ISC) has already published a draft of their PKI Assessment Guidelines (PAG) v0.30 for public comment. Comments were to be received, so it is assumed that a period of time will elapse before those changes are incorporated as necessary, and that the final document will be published. The information on the website notes that this document is planned to be a living document. This means the document will be updated frequently as the technology changes, and more is learned about PKI assurance best practices and other methodology enhancements (Information Security Committee, 2001). It is certainly a step in the right direction with regard to assessing a PKI.

Assumptions

For purposes of setting a model of assessment, it is assumed, at first, that a risk assessment has been completed, and a PKI has been implemented within the organization being discussed. The results of the risk assessment would have shown that it was appropriate to implement a PKI. So, the organization did just that. The question is, does it work as expected or not?

Security policies, standards, and procedures

Before any evaluation is done, a set of policies, standards and procedures, as well as other PKI related documents, must be established. The policy is a high level document that is generic in the respect that specific technology is not called out specifically (Briney, 1999). The standards support the policy, and spell out more specific instructions on how to carry out the policy (Peltier, 1999). The procedures should be thought of as the “where,” “when” and the “how” to implement a standard (Tudor, 2001). The policies, standards and procedures, are in general, a set of rules and requirements that must be followed in order to have a successful and secure computer

system. In order to validate that the system is indeed secure, the established criteria must be reviewed alongside what is actually being done within the organization, and see if they match. Simply put, if the organization is not following established rules, the validation fails. Sometimes "failure" is due to multiple interpretations of the same rule, therefore the policies, etc. must be clear.

PAG Assessment Inputs

If an organization were implementing a PKI system, and wanted to use the PAG as their assessment guide, they would have to start from the assessment criteria and work backwards. This would mean ensuring that what will be assessed becomes part of the policies, standards, and procedures. The PAG lists primary inputs to the assessment process as (Information Security Committee, 2001):

- Any set of requirements that assesses the Certificate Policy (CP). The CP is not diagrammed or discussed in great detail within the PAG, but it is mentioned as a checkpoint to be reviewed at some level, whether the CP is within the PKI, or outside of it.
- Any documented assessment criteria required to be followed, based on the type of business being reviewed. This can include government standards such as the Health Insurance Portability and Accountability Act (HIPPA), among many others.
- PKI Standards need to be followed. Various standards for PKI implementations are expected to be applied in the implementation of the PKI being evaluated.

High-Level Security Requirements

There are many security requirements that need to be part of the policies and procedures that an organization uses when they are implementing a PKI. At a high level, these requirements need be addressed when assessing a PKI (Austin, 2001).

- Private keys must be kept confidential
- Private keys must only be used by the owners of the keys
- Public keys' integrity must be assured
- Initial authentication of the subscriber (private key holder and the subject of the public key certificate) must be strong so that identity theft does not occur at the point of certificate application.

These should be in the format of a Certificate Policy (CP) and a Certification Practices Statement (CPS). The role of these documents is significant. They must cover actions by the Certification Authority (CA), the Certification Archive, the Organization Registration Authority, the Directory Server and The Trusted Time Stamp Server.

Certification Policy and Certification Practices Statement

Mentioned in the section above are these industry standard documents that cover the key topics for establishing a secure PKI. These documents are created for many reasons, too many to list here, but it is important that all interested parties are aware of the contents of these documents. The CP and CPS are critical, and if they are not

written correctly, it is unlikely that other organizations with PKIs will be willing to cross-certify with them. It is a standard that the PKI industry is holding to, in order to keep cross-certified PKIs secure (Austin, 2001).

The PKI Disclosure Document (PDS)

Although the CP and CPS are important documents to ensure the infrastructure is appropriately implemented, what about the users? Do they care what cryptographic method is being used? Most likely they do not care. Enter the PKI Disclosure Statement into the picture. This document is generally no longer than two pages, while still covering critical items such as warranties, limitations and obligations, it reads more like an End User License Agreement (ELUA) than a manual for a technical engineer. This document is a simple checklist that ensures that two organizations have generally the same security practices so that a trust relationship can be established, among other benefits. One approach is to create a PDS, then a CPS, and finish with technical procedures based on the CPS. This is simply one approach among many to ensure the proper documentation is created for a PKI.

Provisions of the PAG

The PAG provisions should be reviewed in order to best implement the PKI so that it follows some established standards. The PAG provides suggested guidelines on areas that need to be assessed. In each area of provisions of the PAG, there are three main sections. The first is the **Issue Summary**, which is a sentence or two that notes the issue that is being discussed, and is meant to state an issue without making specific recommendations. The next section is **Relevant Considerations**. This section includes background information about a particular issue or topic, and may also present the possible options that a PKI may choose to adopt in response to an issue. Finally, **Relevant Considerations** may also inform assessors what information they may wish to seek and what analyses may be appropriate concerning an issue as part of their assessments. **Appropriate Requirements and Practices** is the final section in each of the provisions. PAG actually makes recommendations in this section. These recommendations may be based on what are considered “best practices” within the industry or provide typical responses to the issue. The recommendation is highly dependent on the type of PKI is in place, and will be based on various factors. Where appropriate, these factors are listed as part of the recommendation (Information Security Committee, 2001).

PKI Implementation and Policy Creation Issues

A literature search yielded several high- level issues that need to be dealt with in both implementing and creating the policies for a PKI. These issues, and many others need to be reviewed and decided upon before any policy can be called complete. The High-Level Issues are:

- Some high- level examples of what should be in a policy are (Henrey, 1999):

- What is the process to handle lost keys?
- How long should a key/certificate be valid?
- What is the policy surrounding Certificate Revocation lists?
- What keys are kept in the repository? All of them? Just signature keys?
- What are the liabilities?

There are varying approaches to implementing PKI. One is to store the key on a person's computer. While this works, and it is cheaper in most cases, smart cards are revered in the industry as a more viable option. Many say that using tamper-resistant smart cards are a beneficial way to technically implement PKI. It is easy to protect them from viruses, since smart cards have a password or a personal identification number (PIN) associated with them, even if they are stolen, the thieves cannot use the certificates, and the tamper-resistance of smart cards prevent copies being made. Another issue for PKI is to decide on what CRL delivery model to use. There are basically two different CRL delivery models. One approach is called polling, and the other is called pushing. For polling, this requires the certificate user to request a current copy of the CRL, which may take a few hours. This time delay is crucial, as a revoked certificate may be able to be used during that delay. The push approach has the CA push a new copy of the CRL at once, right after a certificate is revoked. The issue with this is that the user is constantly getting new versions of the CRL, and may not need them. Also, the new version of the CRL may be intercepted by an attacker, which would compromise the process (Mel & Baker, 2001). Costs are an additional issue regarding the CRL (Briney, 1999). Each approach has advantages and disadvantages. Regardless of the decision made, the risks listed must be mitigated by creating the proper policies, standards and procedures which will minimize these risks.

Policy, Standards, and Procedures

At this point, it has been shown that for a PKI deployment, in order to assure that it has been deployed successfully, the criteria under which it must be reviewed must be part of the polices, standards and procedures that are shared with the organization personnel. This way, users can use the PKI the way it is supposed to be used, and technical people can implement the technical aspects appropriately in order to support the established requirements.

Selecting the Criteria

It is known in the industry that creating complete and appropriate criteria is challenging, due to the complexity and intricacies of PKI technology (Austin, 2001). That being stated, based on the standards and other factors listed above as inputs, an appropriate selection of the above information, based on various factors such as results of risk analysis, legal responsibilities, user policies, etc., as well as PKI specific factors, such as the PKI model itself, the PKI security service, the level of assurance required, the policies, standards and procedures, as well as other factors, the criteria can be

established. In the end, the criteria ultimately used must be able to answer the question, "Does the PKI faithfully implement the Certificate Policy that it is asserting?" Government Criteria, such as the Common Criteria, may also be leveraged in order to create proper criterion to assess the PKI (Information Security Committee, 2001).

PKI Security Diagnosis

At this time, the criteria are available for a diagnosis. The question is, what kind of diagnosis should be implemented? There are many issues regarding the validation of a PKI for security. The reason that the term "security diagnosis" is used here, instead of the term "security assessment" is that based on a literature survey, there is a finer level of granularity that can be discussed regarding security diagnosis, in general. Basically, a diagnosis can be divided up into three different approaches. The first, being a **penetration test**, the second, an **audit**, and the third being an **assessment** (Winkler, 2000a). The latter two are sometimes combined, but based on the definitions that will be presented next; the differences will be made clear.

Penetration Test

A penetration test is a test that determines whether or not a motivated person can get into the system under consideration. This is a covert test where person acts like a "hostile attacker" who tries to compromise the security a computer system or process. The test is done without any warning to the security department, can be done physically or electronically, and done with secrecy. Most likely, high- level requests this type of test (Winkler, 2000b). It has been stated in the literature that if a PKI is implemented using smart cards, for example, an attacker can both simply break into a computer lab, or more likely, "social engineer" their way into an office, and sign documents with an unattended computer with the smart card still active (Ellison & Schneier, 2000c). While this is a risk for PKI, it is a risk for all computer use in general. However, to specifically penetration test PKI security, it would be interesting to see if this was possible. It should be noted that penetration tests are not indicative of overall PKI security, whether it passes or fails, it simply shows that there is or is not, as physical security hole at that point and time. If it fails, it is simply and indicator that the policies are not being followed (Kurtz & Prosise, 2000; Winkler, 2000a).

Audit

An audit is to determine whether or not the organization measures up to certain standards, either self-imposed or government set. This test reveals how well a organization sticks to set standards, and the results of the test will drive ways that the organization can improve their security through following the standards more thoroughly. In general, an audit is the practice measuring current security practices against the established set of security rules and policies (Winkler, 2000b). Although an audit is an evaluation that is mostly applicable to accounting principles, it is applicable in the circumstance due to the detailed nature of a PKI. This is where well- written policies, standards and procedures, as well as the CP and CPS are absolutely critical

(Austin, 2001). There is no way that a PKI will pass an audit if these documents are not in order, and the PKI is not implemented according to their rules. The results of an audit should be a checklist of what items that were supposed to be implemented, either were not, or were implemented in an incorrect manner.

Assessment

A security assessment is an open study of the current computer network system of the organization under study, in an effort to study the current security and identify possible improvements to that security implementation. In order to do this, the assessment team must have full access to the whole system, hence, an "open study." The assessment potentially finds holes in the existing security policy. Only when given this access can the team gain a full picture of the network and what needs to be done (Winkler, 2000b). An assessment within a PKI would be, in the author's view, an opportunity to have outside experts review the established policies, etc., as well as the diagnosis criteria, and assess the situation as a whole, reviewing where areas can be implemented in a better way, or a sub-process can be followed in a more efficient way, based on a new industry best practice. This type of review is no t necessarily a "checklist," like the audit, but more of a level set of the current documents versus the current industry standards.

4- ISO standards for PKI

The International Organization for Standardization (ISO) defines a standard referred to as IS0 27001, announced in 2005, to help achieving goals of the standard includes providing the Information Security Management System (ISMS) a model or framework in relation to Establish, Implement, Operate, Monitor, Review, Maintain, and Improve the PKI system. So, it is a framework of procedures that incorporates several, all physical and technical controls that are involved in an organization's management processes. The standard is primarily used for certification purposes. Once you have met ISO 27001 requirements, you can have a registrar audit your entire system. The requirements for the standard really vary up on the size of the organization's management systems requirements. As for the requirements, it varies on size and structure as well as the needs and objectives of your organization. Other than that, business processes and security requirements must be also taken into consideration. For example, every organization has its own industry standards where specific guidelines are followed. In short, not every requirement is the same for all organizations. What may be applicable to one may not necessarily be required from another organization.

Upon its creation, it is said that the ISO27001 was developed to provide a model for establishing as well as implementing and improving an information security management system. The standard uses a risk-based approach and is quite neutral in terms of technology. The specification for the ISO 27001 has six parts:

- Defining the security policy on information security, the policy would define and set the organization's rules and regulations on information security.
- Defining the nature, scope, and purpose of the organization's ISMS
- Conducting a security risk assessment procedure, after the security policy and scope has been in place.
- Managing identified risks, once the risks are identified, there should be a corresponding solution and the organization should determine the methods of managing said risks which brings risk reduction.
- Selecting the control objectives and the controls that need to be implemented and applied, once assessing risks, deciding controls and mitigations that are more appropriate for implementation and application.
- Preparing a statement of applicability or SOA which will signal that the organization is ready for running the ISO 27001

In the present status of industry exchanges and businesses, not every organization has proven to be at par with the rest. By complying with ISO 2700, an organization is believed to be of the finest standards and is certainly a cut above the rest. ISO 27001 must not be confused with ISO 27002, which has different types including one another. One of the best benefits that are received from implementing the ISO 27001 is avoiding specific security objectives such as threats vulnerabilities such as theft, terrorism, misuse of information and a viral attack. This is extremely important to any organization where any of the said factors can be applicable. For example, if a business has a computer network that is hacked or has had a virus uploaded to it, it could lose all the information in the network which is very detrimental to the operations of the business. Now why would an organization need to be certified with the standard? Is it really that important to be certified with ISO 27001?

There are many benefits when it comes to being certified with this industry standard. For one, business continuity or the continued operations of business is insured through legal compliance and avoiding future security failure issues as well as concerns. Besides that, you are assured that the customer will be extremely satisfied by being confident that their information will never be compromised by means of hackers or vagrants. When you are certified, this will give your business or organization increased credibility by showing that you are indeed within the industries' related standards. Finally, it is quite tough to acquire more clients in today's economy. A lot of potential clients now require that an organization they are looking into has an ISO certification as well. By being certified, you are assuring your clients that you are compliant with the standards and you intend to do business for the long haul. To be certified with ISO 27001, your organization must go through the process of registration first. Though it may seem daunting to proceed with the registration process, there really is not much to it if you have all the requirements and the things that are needed from you.

There are three stages when one wants to seek independent certification information and audit for the ISO 27001. The first stage entails a visit from the auditor to confirm that the organization is ready for full assessment. This includes checking for compliance, as well as the production of report that identifies any noncompliance or any potential for noncompliance. The second stage involves a visit to confirm that the management system standards covers types is fully compliant the requirements of ISO 27001. With that, the assessor in charge will document how the entire system is complying with the standard. The assessor will thoroughly checked everything, and may report on any of the noncompliance issues as well as any potential for non-compliance. Finally, the third stage involves periodic visits from the assessor to make sure that the corporation continues to operate within the industry's standards and there is no inkling or hints of noncompliance. A lot of large corporations all over the world are now looking to have themselves ISO certified. If one has foreign clients, by showing that you have ISO certification, the other party is better assured of your corporation's credibility. Finally, completing all the requirements for certification is a must and applies to all types of organizations. If by chance an organization has shown a sign of noncompliance regardless of how small it is, certification will not be granted. This is of course, until correct actions have been taken and all requirements are followed down to the dot.

The PKI Performance Monitoring and Optimization feature provides a way to identify and characterize the performance within the Public Key Infrastructure (PKI) subsystem and debug and analyze PKI performance related issues. When PKI applications are deployed in a environment that scales, they can sometimes create challenging problems that are difficult to debug and identify. Traditional use of debug commands may be less effective in this operating environment. However, the PKI Performance Monitoring and Optimization feature provides an efficient way to gather data and report PKI operations to identify performance related issues and enables you to collect the following types of PKI performance data:

- Time to validate entire certificate chain.
- Time to verify each certificate.
- Time to check revocation status for each certificate.301
- Time to fetch certificate revocation list (CRL) database for each fetch location.
- Time to fetch Simple Certificate Enrollment Protocol (SCEP) method capabilities to retrieve the CRL.
- Time to process each CRL.
- Time to process the Online Certificate Status Protocol (OCSP - a certificate revocation mechanism) response.
- Time to fetch Authentication, Authorization, and Accounting (AAA).
- CRL size.

- Validation result.
- Validation Bypass (pubkey cached).
- Method used to fetch a CRL.
- PKI session identifier.
- Crypto engine used (hardware, software, e-token)

5- Suggested assessment features of PKI

Regarding what is introduced before in discussing the different assessment measures provided through the PAG (Public key infrastructure Assessment Guide), published 2005 or its updates published 2011 by the Federal Public Key Infrastructure (FPKI), Security Controls Profile of Special Publication 800-53A Assessment Guidance for Security Controls in PKI Systems (FPKI, 2011), or the ISO standards for PKI assessment procedures used for the evaluation of the organization's security systems compliance with these standards, this paper suggests additional assessment measures welling to be taken into consideration while performing the assessment procedures focusing on the engineering (technical) aspect of this process. These assessment measures are:

- The security strength of the encryption algorithms (symmetric or asymmetric) used in the implementation of the components of the PKI system.
- How is the implemented PKI system is cryptanalysis resistant, and to what extent?
- The encryption key length, and who the hardware and software limitations (constrains) affecting the ceiling of the extension of this key length.
- The network risk management systems that constrain (detect, defend, and destroy) the hackers (or crypt analyzers) trials to attack there security systems.

6. Conclusions:

It has been shown in this paper that there are more than one assessment technique used for the process of the performance analysis of the implemented PKI systems. It is certainly challenging to execute a security diagnosis on a PKI. This difficulty has been made clear by a review of the current literature. There is some work being done in this area, namely the PAG is in draft mode, and ready to be established as a de facto assessment standard. Even though there are standards, such as ISO 27001 presented by the International Organization for Standardization, they must be integrated into organization' established security policies, standards and procedures. A well formed CP and CPS must also be established in order to lend credibility to the security of the PKI from an outside point of view. Once these criterions are established, various types of diagnosis can be executed, such as: a penetration test, an audit, or an assessment. If

these steps are basically followed, an organization in a better position to have a secure PKI. Taking into consideration the last technical assessment measures presented in section five of this document, the next challenge is to assure that their infrastructure is indeed secure by performing a security diagnosis, proving that their implementation was truly a success. Any PKI implementation is complex – and this means that assessing the PKI is just as complex. It is important for every organizations to remember that PKI is a process, not just a technology. It also must be internalized by organizations that when PKI is adopted, they are also adopting a new way to assess their security systems, including their PKI. Organizations should beware not to treat the assessment as a second thought, but an integral part of the initial implementation of a PKI. Organizations that implement PKI, with the eventual assessment in mind, will, in the author's opinion, will ultimately have a more successful Public Key Infrastructure.

References:

[1] Austin, T. (2001). *PKI*. New York City, NY: John Wiley & Sons.

[2] Bhimani, A. (2000). PKI: Be Careful What You Wish For. *Information Security*(December 5, 2001), 39-50

[3] Brands, S. (2000). *Rethinking Public Key Infrastructures and Digital Certificates*. Cambridge, Massachusetts: MIT Press.

[4] Briney, A. (1999). Pioneers...or Guinea Pigs? *Information Security*, 34-40.

[5] Canavan, J. (2001). *Fundamentals of Network Security*. Norwood, MA: Artech House, Inc.

[6] Ellison, C., & Schneier, B. (2000). Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. *Computer Security Journal*, *16*(1), 1-7.

[7] Henrey, D. (1999). Who's got the key? *Proceedings of the 27th annual ACM SI/GUCCS conference on Mile high expectations*, pp. 106-110.

[8] ISM. (2000). *Infosecond*. Retrieved 2001, from the World Wide Web: http://www.infosecuritymag.com/articles/march00/departments_news_info_second.shtml .

[9] Jianying Z. & Moti Y., 2010. "Applied Cryptography and Network Security", 8th International Conference on Applied Cryptography and Network Security, ACNS 2010.

[10] Liu, C., Ozols, M., & Cant, T. (2001). An Axiomatic Basis for Reasoning about Trust in PKIs. *6th Australasian Conference, ACISP*, Sydney, Australia, pp. 275-291.

[11] Mel, H. X., & Baker, D. (2001). *Cryptography Decrypted*. Boston: Addison-Wesley.

[12] Murray, W. (1999). You Can't Buy PKI. *Information Security*, 28-29.

[13] Peltier, T. (1999). *Information Security: Policies and Procedures*. Boca Raton, FL: CRC Press LLC.

[14] Rothke, B. (2001). *The Problem with PKI: An Insider's View*. Retrieved 2001, from the World Wide Web: http://www.infosecuritymag.com/digest/2001/09-06-01.shtml.

[15] Tudor, J. (2001). *Information Security Architecture*. Boca Raton, FL: CRC Press LLC.

[16] Winkler, I. (2000a). *Audits, Assessments & Tests (Oh, My)*. Retrieved October 20, 2001, from the World Wide Web: http://www.infosecuritymag.com/articles/july00/features4.shtml.

[17] Winkler, I. (2000b). Audits, Assessments & Tests (Oh, My). *Information Security Magazine*. Retrieved October 20, 2001, from the World Wide Web: http://www.infosecuritymag.com/articles/july00/features4.shtml.

[18] Federal Public Key Infrastructure (FPKI), 2011. Security Controls Profile of Special Publication 800-53A Assessment Guidance for Security Controls in PKI Systems