Design and Implementation of PKI (For Multi Domain Environment)

Imran Ijaz

Abstract—**Different organizations make use of internet for intercommunication. To ensure confidentiality, integrity, authentication and non-repudiation, there is a requirement to have a secure communication system like PKI. Since the requirement of each organization for security is different therefore they adopt different PKI policies for the purpose. The problem arises due to inoperability between the organizations due to different PKI policies. Different solutions have been suggested so far but these have made the system more complex. There is a requirement to have a comparatively simple system but providing all security services i.e. confidentiality, integrity, authentication and non-repudiation. This article not only presents an architecture but also the implementation of PKI model in multi domain environment (Between different Universities of Pakistan) to facilitate data and resource sharing in a secure way. The model uses the existing network infrastructure of Gigabit bandwidth links between different Universities. In the model, a National Level CA was defined and all others Universities forming different domains intercommunicated under the National CA.**

Index Terms—**Public key infrastructure (PKI), certification authority (CA), national CA, multi domain PKI, X.509, VPN certificate services.**

I. Introduction

The Internet has become an energetic communication infrastructure but the carrier for network attacks. There exist a number of network threats like wiretapping and alteration of data etc. To prevent these threats, confidentiality, integrity, authentication, and non-repudiation are security requirements. These requirements are supported by a number of security solutions. One of them is a Public Key Infrastructure (PKI). Most of the protocols for secure communications like email, web service, virtual private networks, and authentication systems use PKI.

In PKI, a trusted third party called Certification Authority (CA) issues a certificate digitally signed by using its private key. A certificate is used to bind an entity's identity information with the corresponding public key.

Over insecure networks, responsibility of PKI is to issue, maintain, and revoke public key certificates. A PKI permits users of such networks to exchange data through the use of a public and private key pair that is obtained and shared through a trusted authority. Digital certificates identify individuals or organizations. Basically the design of PKI is based upon the concept of trust. A trust domain is a set of PKI systems linked by a uniform management or subjected to a common set of security policies. A certification authority, CA, is a trusted third party that issues digital certificates.

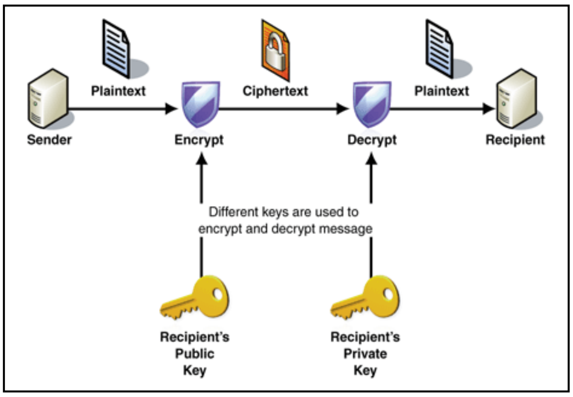

Fig. 1. PKI example.

The first task is to design PKI architecture to allocate the trust domains and define their borders. PKI implementations vary from country to country and from region to region. The resulting different huge number of implementations raises serious questions. How to create trust domains for different regions and countries and how to inter-connect the different PKI Certificate Authorities so that they intercommunicate as a single, coherent system?

II. Literature Review

In PKI architecture the performance and efficiency of a system are very important when multi domain environments are connected as a single PKI.

Long paths can be difficult when bidirectional trust relationships are established, especially when storage and processing capacities of the verifier are limited. The efficiency of certification path validation will becomes greater. So choosing the shortest path between root and the hierarchies that has only one root CA is a major issue [1].In PKI Mesh network, length of certificate path is minimized but no guarantee that selected path between two entities will be the shortest one [2]. As for as Trust Domain Modeling is concerned, it is useful in building and managing large scale PKIs throughout the entire nation and even the world but relationship between PKI and PMI cannot be established [3].Merging of CAs without Using Cross Certification is possible but with the expansion of network, management becomes painful [4]. The PKI model must be simple to avoid any confusion in further enhancement and expansion and all nodes, their function and policy must be finalized [5]. In P2PPKI Model cheating can be avoided by maintaining a database for good and bad clients but additional feature will be an overhead for maintaining this database [6].

Manuscript received May 25, 2012; revised June 25, 2012.

Imran Ijaz is with the working as System/Network Administrator in Fatima Jinnah Women University, Rawalpindi, Pakistan.

To manage the trustworthiness of security infrastructures private keys which are often stored on and utilized by the end users computers that causes the exposure of the private keys the duration of keys can be short [7].In group based trust model (F-PKI) it enhance the platform security, but also make it possible to establish trust relationship between peers who never know each other before [8]. When configuring Peer-to-Peer Network efficiency increases in checking authenticity of a node. So message publication and retrieval tasks are forwarded via less than log2 (N) to other nodes [9].Two layered PKI model can also be used for device authentication in multi domain networks. It will minimize the end-device's operations, user interventions, and communication time delay by using the local and global PKI layers in overall device registration and authentication process [10].For large networks bridge certificates are required. CA (BCA) is complex than traditional but more efficient. An independent mechanism can be used to automatically discovery and verifies these certificate paths among domains [11].

So it is clear that for managing a large multi domain network, the model must be simple but efficient to provide a better response to issue and manage certificates.

III. Public Key Infrastructure Service and Components

Public key infrastructures have become the starting point for modern security mechanisms on the Internet. PKI is closely linked to the asymmetric key encryption, digital signatures and encryption services, but to enable these services, digital certificates are used.

A. PKI Service

PKI facilitates storage and exchange of electronic data in a secure way, safety is ensured by using public key cryptography. Security services offered by PKI are:

1) *Confidentiality* - Keeping the private nature of the message is achieved by using the encryption. Only the owner of private key will be capable to decrypt the encrypted message.
2) *Integrity* – It is evidence that the message has not been altered. It is obtained with the help of a digital signature. By verifying the signature successfully it is ensured that message has not been changed after signing.
3) *Authenticity* - Confirming the identity of an individual or an application which transmits the message is done using a digital signature.
4) *Non-Repudiation* - Property providing security as the certainty that the message cannot deny it later passed.

B. PKI Components

Components of a PKI include system components such as one or more Certification Authorities and a certificate repository; documentation including a Certificate Policy document and one or more Certification Practice Statements and trained personnel performing trusted roles to operate and maintain the system.

The main components of infrastructure are:

1) *Certifying Authorities* – Basic components of a PKI to issue and revoke digital certificates.
2) *Registration Authorities* – Validates requests for issuing certificates and identity of end users.
3) *Repository* – Store and distribute certificates and certificate revocation lists (CRL), they are issued periodically by the CA and are lists of certificates that are no longer valid.
4) *Archives* – An archive is responsible for long-term storage of information in the name of the certifying authority, certifying that the information archived it was good when that was received and was not changed while it was archived.
5) *End Entity* – They are end users for which digital certificates are issued.

IV. PKI Architecture

Architecture of a PKI is composed of operations and security policies, security services and protocols that support interoperability using public key encryption and key management certificates. In PKI a digital certificate issued by CA and applications are usually processed by the Registration Authorities (RA). The responsibility of an RA is to analyze individual user who examines each application and notifies the CA, which is closer to the level of confidence of the applicant by checking the level of confidence, CA issue the certificate.

A. Stand Alone Root CA

Standalone Root CA is implemented where we require an offline Root CA. Stand Alone is not integrated with active Directory. However information from the CA, such as CDP and AIA, could still be published to Active Directory. Typically the Stand Alone CA is a member of its own workgroup as opposed to being a member of a domain. It is disconnected from the network only accessible to the operators of the CA server.

B. Enterprise Root CA

Enterprise Root CA is comparatively easy to implement as there is only one server required to establish PKI and there is no subordinate CA servers and certificate chaining. Enterprise CA server is integrated with Active Directory. An Enterprise CA can be used to auto enroll certificates in an Active Directory environment.

C. Stand Alone Issuing CA

A Stand Alone Issuing CA means that the CA server is a subordinate CA server and it has gotten its CA certificate signed by another CA server. Typically this type is used when the CA server won't be issuing certificates to objects in an Active Directory domain, or using an offline policy CA server in three-tier PKI hierarchy.

D. Enterprise Issuing CA

An Enterprise Issuing CA is a member of an Active Directory domain and is integrated to Active Directory. User and computer accounts can enroll or auto enrolls for certificates from this CA. The CA server provides the same functionality as an Enterprise Root CA server, but the Enterprise Issuing CA is a subordinate CA server.

V. How Many Tiers?

Most PKI setups will have one, two or three tiers. With one tier there is only Root CA which is responsible for issuing and revoking all the certificates. In a two tier environment there are offline Root CA and one or more subordinate CA servers. In a three tier environment there are an offline Root CA, one or more subordinate policy CAs which can also be offline. These policies CAs will govern the policy of the subordinate CAs below them, the issuing CA servers.

VI. Problem Statement

Different organizations adopt different PKI trust model for their applications. On a large scale, all certification authorities and end entities construct a huge network. As a result, serious PKI issue arises due to implementation of different security policies and implementations from organization to organization. This raises the question of interoperability between these various implementations, especially in such a way as to create a global trust domain.

Any PKI model cannot facilitate all security related issues. Requirement of PKI vary from organization to organization. Another organization may need certificates for their VPN users only, some need to users only etc. The result will be the mixture of different CAs and policy conflicts between these CAs. At the end, the inter domain communication will not be possible even the organizations may be located within a same city or country.

VII. Proposed Architecture for Multi Domain Enviroment

To avoid the inter communication problem, it is strongly recommended that National Certificate Authority must be defined at the central level that will be responsible to issue the certificates. This authority can be for one particular service like Education, Business and Law Enforcing Agencies etc. A ROOT CA must be declared for each service. These National CAs will be configured under "New Forest in a New Domain" policy. Any new organization or educational institute interested to implement PKI for their organization will be configured under the national forest but with a new domain.

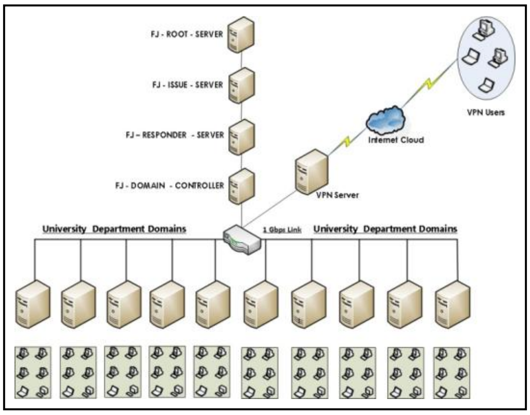

Fig. 2. Implemented CA architecture of PKI model.

By adopting this technique, inter domain policy conflicts can be avoided. So any organization of a specific sector will be able to communicate to any other organization of the same sector without policy conflicts between them, which was the major reason of failure for PKI inter-domain communication.

In our model, we have not only suggested the architecture but implement this model at a national level and measure its performance. In the model, we used existing network between the Universities i.e. PERN. PERN is providing communication infrastructure to the universities, institutions of higher learning and research organizations to meet their networking and internet requirements. It is providing valuable services, like high-speed internet, audio/video conferencing, and access to digital library resources. Currently more than 50 public and private sector universities/institutes are interconnected on local network with a core capacity of 10Gbps.

The objective of our PKI model was to facilitate exchange of information securely between different domains at the National level. Different architectures were designed and considered and one of the best that full fills the requirements in a pretty good way, was adopted.

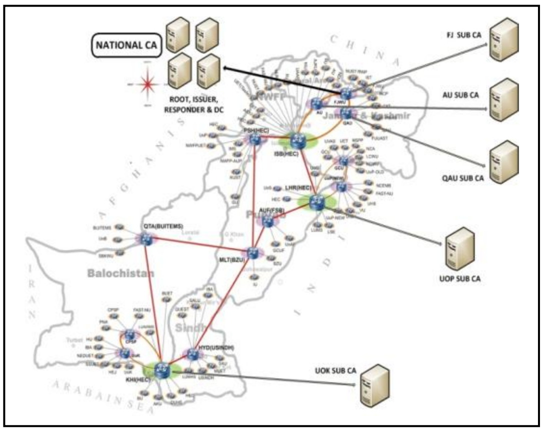

Fig. 3. Placement of servers in PKI model.

In finalized model, we selected the FJ University as a National CA. Domain Controller was configured as "New Forest in a New Domain". Root Server was configured that will act as an offline root server. Subordinate certificate authority (SUB-CA) server named as ISSUE CA was configured to issue the certificates to Local Domain and other Sub Domains. Responder Server was configured that will respond against the received request from user or computer. Twelve sub domains were configured under the primary domain of FJ in the University. In addition, VPN Server was created under L2TP policy. The function of VPN Server was to provide access of remote users to local network resources. So authorized remote users (having VPN Server Certificate) were able to access the University resources over the internet by using their certificate.

At the second stage, five different universities were selected from three different regions of the country. In each university, Domain Controller Server was configured. Each Domain Controller of each University was configured as "New Domain Controller in Existing Forest". Of course the forest was FJ. These Domain Controllers were then configured as subordinate issuing servers. Now these servers were actually Subordinate Issue Servers but had become the issuing authority of their respective domains. Responding and Revocation service was configured on the same servers. At the final stage, these servers were Domain Controller, Issuer, Responder and Certificate Revocation List publisher.(single tier). Active Directory service was used to publish the certificates. Each server got cross certificate from other four servers. Three to five users were authenticated in each university to communicate over this PKI model at the initial stage. The placement of servers in our proposed architecture has been shown in Fig. 3.

Different group policies were defined for each domain to issue the certificates like only to user, only to computers and to both user and computer etc. Each policy executed successfully and certificates were issued as per defined in group policies. All users and computers of every domain got their certificate from their respective Issue Server. Moreover inter domain logon facility was configured to access the resources of other domains. Users were able to log-on to other domains and got the certificate of the second domain successfully. Thus resources had been shared and inter domain logon had been implemented without policy conflicts that was the major aim to implement this model.

VIII. Certificate Flow Process

Initially all computers that join their respective domain will get the computer certificate. For better security, policy was configured to issue the certificate to domain user also. The flow of certificate is shown in Fig. 4:

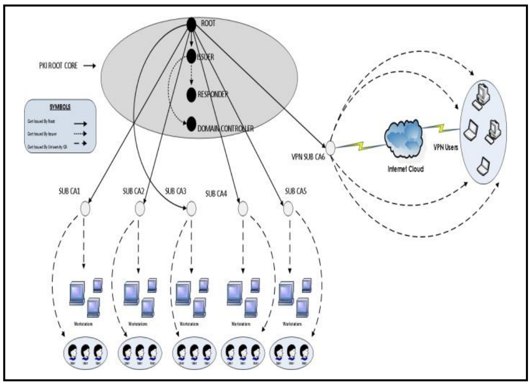

Fig. 4. Certificate flow in PKI model.

A. *Certificates Issued to:*

Domain Computers, Domain Users, VPN Users

B. *Flow of Certificate Paths:*

a) ROOT→ISSUER→RESPONDER→DC SUB CA→ Computers

b) ROOT→ISSUER→RESPONDER→DC SUB CA→ Users

c) ROOT→ISSUER→RESPONDER→VPN Server→ VPN Users

IX. Performance Analysis

After installation, configuration and implementation of complete model, the performance of each server was analyzed. All processes were running smoothly without over burdening the servers and major increase in network traffic. (Fig. 5 and Fig. 6).

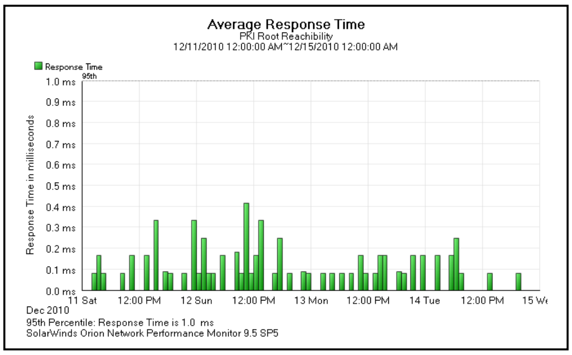

Fig. 5. Average response time (0.19ms).

The performance of implemented model was analyzed on the bases of delay, response time, reachability and path validation.

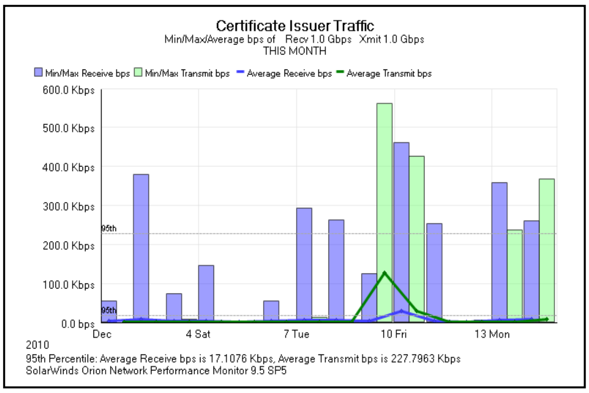

Fig. 6. Traffic on certificate issuer server interface.

Availability of CA Server and certificate traffic were analyzed to monitor the load and its performance. The results show good performance against each evaluation.

X. Conclusion

Public key infrastructure has become an essential point in the development of a country because it offers three services, namely: authentication, digital signature and encryption. In our work, we not only design, but implement this model at the National level. By using the PKI model, secure inter domain communication was performed between different Universities under different domains. The certificates were distributed from different certificate issue servers to users and computers successfully. Results were successful in a way that different users from different domain were authenticated. . This implementation makes it possible to achieve secure electronic data transfer between the different Universities in the country. Same model can be adopted by any government or private sector for the implementation of PKI model at National level

This model is a prototype model that can be implemented at the national level by the government agencies. Inter domain communication was successfully achieved in a secure way.

References

[1] C. Satiz ábal and R. P áez, “JordiForné “PKI Trust Relationships: From Hybrid Architecture to a Hierarchical Model,” *International Conference on Availability Reliability and Security IEEE*, 2006

[2] C. Liu, Y. Feng, M. Fan, and G. Wang "PKI Mesh Trust Model Based on Trusted Computing," *International Conference for Young Computer Scientists IEEE*, 2008

[3] H. Yu, C. Jin, and H. Che "A Description Logic for PKI Trust Domain Modeling," *International Conference on Information Technology and Applications IEEE*, 2005

[4] S. K. K. Sakurai "A Merging Method of Certification Authorities without Using Cross Certifications," *Presented at International Conference on Advanced Information Networking and Application IEEE*, 2004

[5] J. Lopez, R. Oppliger, and G. Pernul "Why have public key infrastructures failed so far?" *Emerald Internet Research*, 2005

[6] H. Jiang and Y. Tan, "Research In P2P-PKI Trust Model," *International Conference on Computer Science and Information Technology IEEE*, 2010

[7] S. Xu, "Can We Manage the Trustworthiness of Security Infrastructures and Services?" *Trusted Infrastructure Technologies Conference IEEE*, 2008

[8] N. Liu, J. Li, L. Hao, Y. Wu, and P. Yi "Group-based Trust Model in P2P System Based on Trusted Computing," *International Conference on Computer Science and Software Engineering IEEE*, 2008

[9] T. Wölfl, "Public-Key-Infrastructure Based on a Peer-to-Peer Network," *International Conference on System Sciences IEEE*, 2005

[10] J. H. Wang, D.-W. Kim, Y.-K. Lee, and J.-W. Han "Two Layered PKI Model for Device Authentication in Multi-Domain Home Networks," *International Conference on Availability, Reliability and Security IEEE*, 2006

[11] M. Li, Y. Ren, Z. Wang, J. Xie, and H. Yao "A New Modified Bridge Certification Authority PKI Trust Model," *International Symposium on Pervasive Computing and Applications* 2006.

Imran Ijaz is working as System/Network Administrator in Fatima Jinnah Women University, Rawalpindi, Pakistan. Mr. Imran Ijaz born in 1976 has completed his MS/M.Phil program in 2011. Currently he is doing his Ph.D. in Network Security. He served in different private/government organizations and completed a number of Network Projects at National Level. Currently he is supervising research in field of Network Security and PKI.