Solution to PKI Inter- Domain Interoperability Issue

Sarvesh Tanwar, Dr. Prema K.V

Abstract - PKI is a framework for the management of public keys and certificates that is responsible for issuing, maintaining and revoking of the public key certificates over the internet. A number of serious security issues have already occurred with the rapid deployment of electronic transaction. One approach to guaranteeing security is the public key infrastructure (PKI). PKI provides a structure of trust among its users or principals. However there are serious PKI implementation issues as different countries and different organizations may adopt different security policies and implementations. This raises the question of interoperation between these various implementations. In the paper, we propose a new solution using same algorithm to achieve the digital certificate validation and resolve the general PKI interoperation problem.

Keywords: PKI, interoperability, security issues, digital certificate.

1. INTRODUCTION

IN contrast with secret-key cryptography, public-key cryptography is very new. It was first conceived in 1976 by Diffie and Hellman ([DH76]), and in 1977 Rivest, Shamir and Adleman invented the RSA Cryptosystem ([RSA78]), the first realization of a public-key system. There have since been several proposals for public key schemes, including the ElGamal Cryptosystem ([El85]) and elliptic curve cryptosystems ([Sa96]).

PKI is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over an increasingly insecure Internet [3]. The first stage in designing PKI architecture is to allocate the trust domains and define their borders. PKI implementations vary from country to country and from region to region. The resulting different implementations raise a number of serious questions, such as how to create trust domains for different regions and countries and how to interconnect the different PKI CA's so that they interoperate as if they were a single, coherent system. We can use trust models and validation authority to achieve the digital certificate validation and resolve the general PKI interoperation problem.

1.1 Public Key Infrastructure

By allowing digital signatures to be as valid as handwritten signatures, public key infrastructure (PKI) provides businesses with a quick alternative to the sometimes lengthy process of documentation.

- *Sarvesh Tanwar: currently pursuing Ph.D in computer science & engineering in Mody University, Laxmangar, E-mail: sy_kanu@rediffmail.com*
- *Dr. Prema K.V : Professor in CSE Department , Mody University,Laxmangarh, E-mail: drprema.mits@gmail.com*

Public Key Infrastructure shows programmers and engineers how to build appropriate layers of security throughout the network, letting businesses put to rest concerns of how to protect assets and freeing them to concentrate on adding value for employees, customers, and business partners. "A PKI is a set of agreed-upon standards, Certification Authorities (CA), structure between multiple CAs, methods to discover and validate Certification Paths, Operational Protocols, Management Protocols, Interoperable Tools and supporting Legislation".

Public Key Infrastructure (PKI) is a framework that enables integration of various services that are related to cryptography. The aim of PKI is to provide confidentiality, integrity, access control, authentication, and most importantly, non-repudiation.

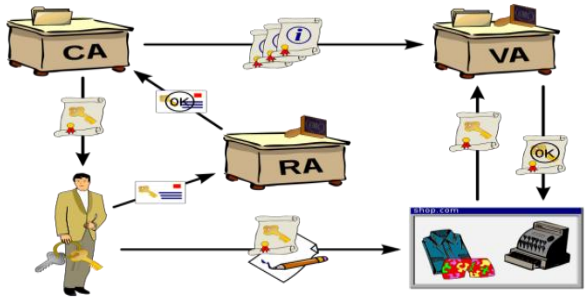

Figure 1.1: Public key Infrastructure

Non-repudiation is a concept, or a way, to ensure that the sender or receiver of a message cannot deny either sending or receiving such a message in future. One of the important audit checks for non-repudiation is a time stamp. The time stamp is an audit trail that provides information of the time the message is sent by the sender and the time the message is received by the receiver.

1.2 PKI Technologies Architecture

The architecture of a PKI involves implementing various interdependent technologies and processes to make it possible to issue, validate, renew, and revoke certificates. These include:-

- One or more servers running Certificate Services and that provide certificate enrolment, revocation and other certificate management services.
- Active Directory service that provides account management, policy distribution, and certificate publication services.
- Domain controllers that can authenticate end users and computers when they request certificates.
- Domain client computers and users, who request, receive, and use certificates for specific purposes. Although certificates can also be used by services and by non-domain clients, in most Windows PKI environments, domain users and computers are the primary recipients and users of certificates. In some cases, the domain client can be a subordinate CA that requests and receives a certificate authorizing it to issue certificates of its own.

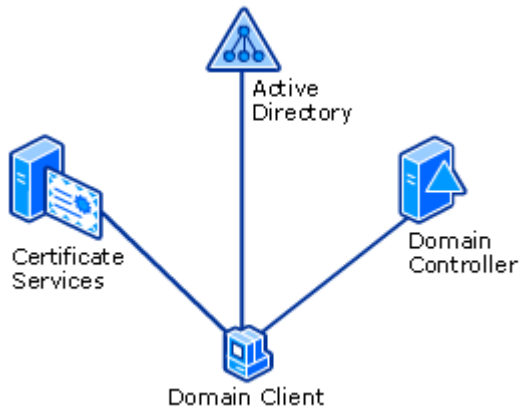

Figure 1.2: PKI Technologies Architecture

1.3 PKI Technologies Components

The key technology components of a PKI and their relation to the PKI architecture diagram are described in the following table.

Components of a PKI

Components	Description
Certificates	Provide the foundation of a PKI. Digital certificates are electronic credentials that are associated with a public key and a private key that an organization uses to authenticate users. Certificates are created on servers running Certificate Services and stored on clients and in a directory such as Active Directory.
Certificate templates	Can be used to define the content and purpose of a digital certificate, including issuance requirements; implemented extensions, such as application policy or extended key usage; and enrolment permissions for certificates that a CA issues. Certificate templates are stored in

Certificate templates	issues. Certificate templates are stored in the Active Directory and used by enterprise CAs to provide the default attributes for a certificate.
Certificate Services	The part of the core operating system that allows a business to act as its own CA, and issue and manage digital certificates. Certificate Services includes tools to manage issued certificates, publish CA certificates and CRLs, configure CAs, import and export certificates and keys, and recover archived private keys.
CAs	Servers on which Certificate Services has been configured to issue, validate, and manage certificates. Windows Server 2003 supports multiple levels of a CA hierarchy and a cross-certified trust network. This includes offline and online CAs.
Certificate Revocation Lists	List of certificates that a CA considers no longer usable. Certificates have a specified lifetime, but CAs can reduce this lifetime by a process known as certificate revocation. Publishers can use any kind of directory service, including X.500, Lightweight Directory Access Protocol (LDAP), or directories in a specific operating system, including Active Directory, to store CRLs. Publishers can also publish CRLs on Web servers.
Certificate policy and practice statements	The two documents that outline how a CA and its certificates are to be used, the degree of trust that can be placed in these certificates, legal liabilities if the trust is broken, and so on. These documents can also define or impact PKI designs, operations, and usage, including how a CA is configured, how client requests are processed, and guidelines and procedures for revoking certificates.
Certificate policies	Configurable limitations on the scope of a certificate. Certificate policies can be implemented as required and allowed certification path length, the range of namespaces that are permitted or excluded by a qualified subordinate CA, the extent to which an organization trusts the identity presented in a certificate, and the applications that can be used in conjunction with certain certificates.
Certificate and CRL repositories	A directory service or other location where certificates are stored and published. In a Windows Server 2003 domain environment, the Active Directory is the most likely publication point for certificates issued by Windows Server 2003–based CAs.
PKI-enabled applications	Examples of PKI-enabled applications include: Encrypting File System (EFS), Microsoft Internet Explorer, Microsoft Money, Internet Information Services (IIS), Routing and Remote Access, Microsoft Outlook, and Microsoft Outlook Express. Also included are a variety of third-party applications that work with Windows 2000 and Windows Server 2003 Certificate Services.

2. The components of PKI

- Encryption using Public Key & secret key -Hybrid Approach
- Digital Signature Process
- Transporting Encryption Keys
- Digital Certificates
- Message Decryption and Verification

The main service provided by PKI is to issue digital certificates and to make them widely available and accessible. Just as a telephone book contains a list of names and numbers, a PKI directory lists the public key with an individual or organization. PKIs solve the key management problems: creation, distribution, authentication, and storage of keys.
Encryption and decryption, digital signature, and key exchange are the three primary functions of a PKI. RSS and elliptic curve algorithms provide all of the three primary functions: encryption and decryption, digital signatures, and key exchanges. Diffie-Hellmen algorithm supports key exchanges, while Digital Signature Standard (DSS) is used in digital signatures.

(a) Public Key Encryption:

It is the encryption methodology used in PKI and was initially proposed by Diffie and Hellman in 1976. The algorithm is based on mathematical functions and uses asymmetric cryptography, that is, uses a pair of keys.

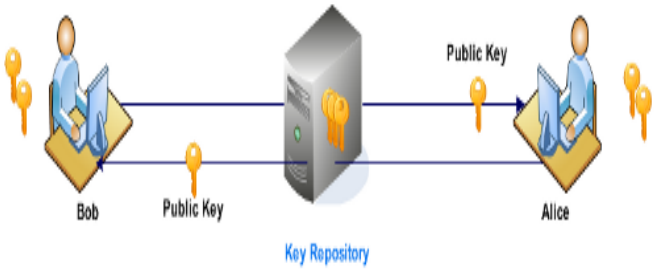

Figure 2.1: Public key encryption

PKI supports all the above four requirements with methods such as secure messaging, Message digests, Digital Signatures, and Non-Repudiation services.

(b) Secure messaging

To ensure that the document is protected from eavesdropping and not altered during the transmission, Bob will first encrypt the document using Alice's public key. This ensures two things: one, that the document is encrypted, and two, only Alice can open it as the document requires the private key of Alice to open it. To summarize, encryption is accomplished using the public key of the receiver and the receiver decrypts with his or her private key. In this method, Bob could ensure that the document is encrypted and only the intended receiver (Alice) can open it. However, Bob cannot ensure whether the contents are altered (Integrity) during transmission by document encryption alone.

(c) Message digest

In order to ensure that the document is not altered during transmission, Bob performs a hash function on the document. The hash value is a computational value based on the contents of the document. This hash value is known as the message digest. By performing the same hash function on the decrypted document the message, the digest can be obtained by Alice and she can compare it with the one sent by Bob to ensure that the contents are not altered. This process will ensure the integrity requirement.

(d) Message authentication

Message authentication is an authenticity verification procedure that facilitates the verification of the integrity of the message as well as the authenticity of the source from which the message is received.

(e) Digital signature

In order to prove that the document is sent by Bob to Alice, Bob needs to use a digital signature. Using a digital signature means applying the sender's private key to the message, or document, or to the message digest. This process is known as signing. Only by using the sender's public key can the message be decrypted.

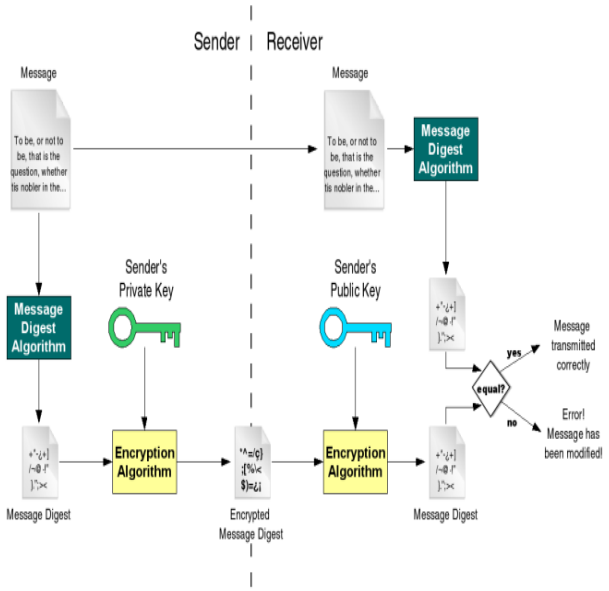

Figure 2.2: Digital Signature

Bob will encrypt the message digest with his private key to create a digital signature. In the scenario illustrated in the image above, Bob will encrypt the document using Alice's public key and sign it using his digital signature. This ensures that Alice can verify that the document is sent by Bob, by verifying the digital signature (Bob's private key) using Bob's public key. Remember a private key and the corresponding public key are linked, albeit mathematically. Alice can also verify that the document is not altered by validating the message digest, and also can open the encrypted document using her private key.

3. Interoperability Issues in PKI

Interoperability is a critical issue. But what does interoperability really mean? In most cases, organizations need seamless application-to-application interoperability. One could argue that this is all an organization needs to worry about. However, other aspects of interoperability, including the ability to mix and match various components from one vendor with another are also important. Many corporations are processing transactions between their enterprise domain and other enterprise domains - in order to conduct B2B transactions. This is of particular concern when the technology deployed in one domain is supplied by a different vendor than the technology deployed in another. Organizations are also concerned with risk mitigation. They want assurance that they can have graceful transition to another vendor's products without having to start their deployment over from scratch. The PKI interoperability framework adopted by the PKI Forum is based on a presentation offered by Tim Polk of NIST at the first PKI Forum Members Meeting in Foster City, CA, USA on 6-8 March 2000, in which he identified three major interoperability areas as follows:

1. Component-Level Interoperability;

2. Application-Level Interoperability; and
3. Inter-Domain Interoperability.

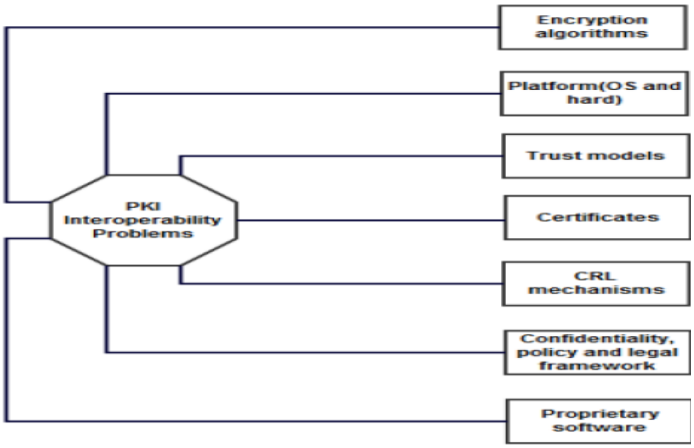

Figure 3.1: PKI interoperability problems [2]

(A) Application-Level Interoperability

Application-level interoperability is concerned with compatibility between two peers, regardless of the supplier of the application or any ancillary infrastructure components used to support the application. For example, two S/MIME-based e-mail clients must be capable of interoperating with one another, even when the application software is supplied by two different vendors, the applications run on two different platforms, an d each S/MIME client uses PKI technology supplied by different vendors. Note that the term "application" is not meant to limit this category of interoperability to the Application Layer.

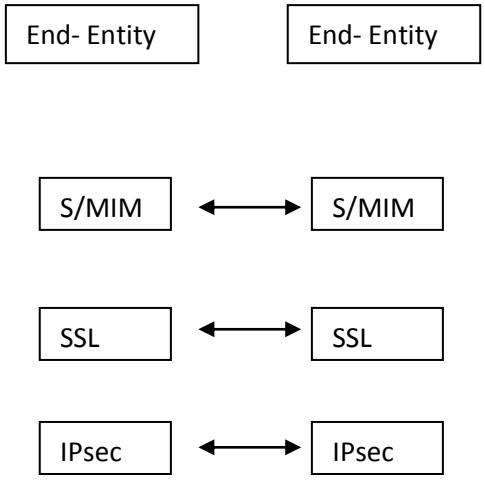

Figure 3.2: Application Level Interoperability

For example, IPSec is considered to be an application in this context.

1. Certificate and certificate status information must be compatible (at least to the extent that any incompatibilities will not affect interoperability);
2. Business controls must be implemented to ensure that certificates that are being used are consistent with intended key usage and any associated constraints;
3. Algorithms (including cryptographic algorithms and key sizes) must be compatible;
4. Data encapsulation and encoding formats (e.g., file format, message formats, etc.) must be compatible;
5. Underlying communications protocols used to exchange information between peers must be compatible; and
6. Any in-band methods for sharing public-key related information (e.g., end-entity and CA certificates, certificate status, etc.) must be compatible. Single-key, dual-key and N-key hybrids must be supported; and
7. Private credentials must be accessible regardless of storage method (e.g., software, smart card, h/w token).

(B) Component-Level Interoperability

Component-level interoperability deals with interaction between devices directly supporting and/or consuming PKI-related services. For the sake of simplicity, we are only considering intra-domain interoperability here. The typically more complex issues associated with inter-domain interoperability. Figure 1 allows for the possibility of additional CAs that, in this context, would represent intra-domain cross-certification (i.e., peer-to-peer relationships in the case of a meshed trust model or superior/subordinate relationships in the case of a hierarchy) [6].

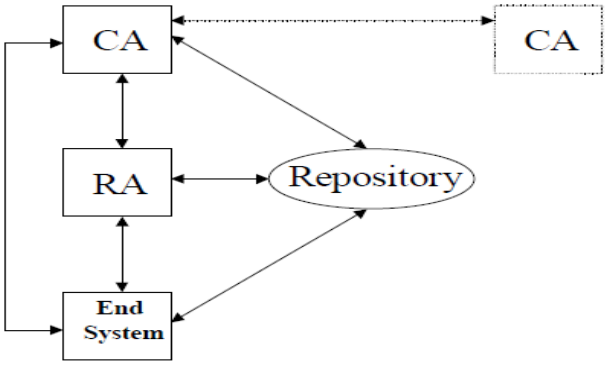

Figure 3.3: Component level interoperability

Source: PKI Forum

Component-level interoperability includes the following considerations:

1. Common protocols and message formats (e.g., PKIX-CMP and PKIX-CRMF) must be implemented between applicable PKI components – this applies to CA-CA, CA-RA, client-CA, and client-RA interaction;
2. Common algorithms for entity authentication and the protection of the exchanged data between PKI components must be implemented (e.g., cryptographic algorithms to support secure CMP exchanges);
3. Common protocols and underlying authentication scheme must be supported to facilitate the storage and retrieval of certificates and certificate revocation information between the repository and the PKI components;
4. Common certificate revocation mechanisms must be supported (e.g., CRLDPs, OCSP);
5. A standard cryptographic interface in support of a hardware security module at the CA must be supported; and
6. Support for flexible certificate types and profiles should be provided.

(C) Inter-Domain Interoperability

Inter-domain interoperability deals with the issues and options associated with achieving interoperability between two otherwise isolated PKI domains5. Inter-domain interoperability is perhaps the most complex of the three interoperability areas, since it involves, among other things, the cooperation of multiple administrative domains. It represents the requirement to exchange PKI-related information between the two PKI domains (which can be accomplished in a variety of ways). The bi-directional arrow between the two domain boundaries can be facilitated in a number of ways, as discussed in the PKI Forum's CA-CA Interoperability White Paper, March 2001 [6].

Inter-domain interoperability involves a number of challenges, both technology and policy-related. The following issues must also be addressed:

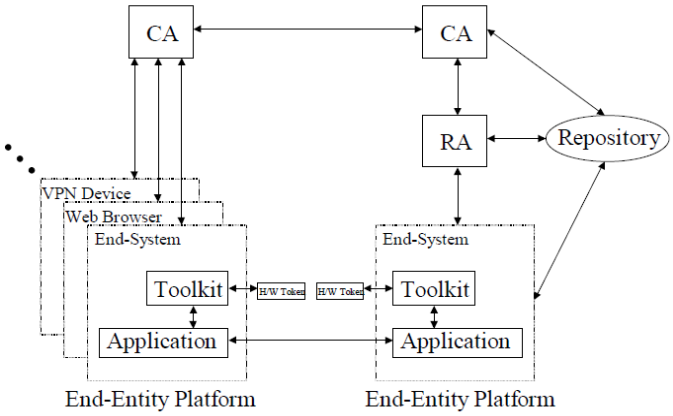

Figure 3.4: Interoperability Boundaries

1. A method for establishing trust relationships between the PKI domains is required (see the PKI Forum's CA-CA Interoperability White Paper, March 2001 for a discussion of options);
2. Appropriate PKI-related information in one domain must be made available to the other, and vice versa (as applicable based on the associated trust relationship); and
3. Each PKI domain must agree to adhere to certain policies (e.g., what a given certificate is to be used for), and each PKI domain needs to have mechanisms in place to enforce adherence to the agreed-upon policies.

4. Approaches to PKI Inter-Domain Interoperability

A. Trust Models and Certificate Paths

A method for establishing trust relationships between the PKI domains is required. Algorithms (including cryptographic algorithms and key sizes) must be compatible. Data encapsulation and encoding formats (e.g., file format, message formats, etc.) must be compatible.

B. Cross Certification

Simply put, cross-certification is the act of one CA issuing a certificate to another CA. This definition is entirely consistent with the X.509 [X509] where it is stated:
"A certification authority may be the subject of a certificate issued by another certification authority. In this case, the certificate is called a cross-certificate…"
And "Cross certificate – This is a certificate where the issuer and the subject are different CAs. CAs issue certificates to other CAs either as a mechanism to authorize the subject CA's existence (e.g. in a strict hierarchy) or to recognize the existence of the subject CA

(e.g. in a distributed trust model). The cross-certificate structure is used for both of these."

The fundamental purpose of cross-certification is to establish a trust relationship between two CAs. This is typically done to establish an interoperability path for one or more applications between two distinct PKI domains or between two CAs within the same PKI domain. The former is referred to as inter-domain cross-certification and the latter is referred to as intra-domain cross-certification [4].

C. Same algorithm policy

As PKI is designed by different vendors for different purposes. They must use the same algorithm so that they are compatible for the changes. While designing the PKI must be tried to use the same algorithm for the encryption and decryption.

Conclusion

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 are mainly used to identify individuals or organizations. A PKI built on the concept of the trust i.e. how much confidence users may gibe to the digital certificates provided by the PKI. In PKI Certification Authority is a trusted third party who is responsible for issuing the certificates. By using the given solution we can implement the PKI in more effective way and remove the problem of inter-domain interoperability issue and it can also remove the replay attack if the same algorithm policy is used in both sides. Certificates must be cross certified by the trusted third party.

References

[1.] "PKI Interoperability Framework", PKI Forum white paper, March 2001, see http://www.pkiforum.org/resources/pki_framework.pdf

[2.] "Interoperability of Digital Signatures in Public Administration ", World of Computer Science and Information Technology Journal(WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 264-268, 2011

[3.] "Public Key Infrastructure: Deployment Benefits and Features", products_white_paper09186a0080179739.shtml#wp42285

[4.] Understanding Public Key Infrastructure: Concepts, Standards and Deployment Considerations, C. Adams and S. Lloyd, 1999, ISBN 1-57870-166-X.

[5.] "PKI Interoperability Framework", white paper, March-2001

[6.] "Entrusts Open PKI Solution: Interoperability and Standards Support", Entrust securing digital identities & information, August 2000