CMSGu2013-01

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Public Key Infrastructure (PKI)

CERT-MU

National Computer Board
Mauritius

Version 1.0

February 2013

Issue No. 1

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to provide the starting point for the implementation and operation of a PKI in organizations. It elaborates on the strategic planning of a feasible trust model that provides confidence to users making use of that facility.

1.2 Audience

The target audience includes all senior management and lower level information security staff involved in or responsible for the implementation or management of a PKI.

1.3 Document Structure

This document is organized into the following sections:

Section 1 outlines the document's content, the targeted audience and the document's structure.

Section 2 presents a background on PKI.

Section 3 describes the Public Key Cryptography process.

Section 4 discusses Digital Certificates.

Section 5 elaborates on the components of a PKI.

Section 6 depicts the challenges of PKI.

Section 7 exemplifies the planning of a PKI.

Section 8 concludes the document.

Section 9 comprises a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

Public Key Infrastructure (PKI) is a security architecture that is based on Public Key Cryptography. Public Key Cryptography supports security mechanisms such as confidentiality, integrity, authentication, and non-repudiation. It is a mathematical technique that uses a pair of related cryptographic keys to verify the identity of the sender (signing) and/or to ensure privacy (encryption).

However, to successfully implement these security mechanisms, an infrastructure must be carefully planned to manage them. Hence, the PKI has been introduced to provide an increased level of security and confidence for exchanging information over an ever more insecure Internet.

The term PKI can be confusing at times because it is used to refer to various different things. On the one hand PKI may mean the methods, technologies and techniques that together provide a secure infrastructure. On the other hand, it may mean the use of a public and private key pair for authentication and proof of content.

A PKI infrastructure normally offers its users the following benefits:

- certainty of the quality of information sent and received electronically
- certainty of the source and destination of that information
- assurance of the time and timing of that information (providing the source of time is known)
- certainty of the privacy of that information
- assurance that the information may be introduced as evidence in a court of law

PKI facilities have been developed principally to support secure information exchange over insecure networks, such as the Internet, where such features cannot otherwise be readily provided. PKI facilities can, however, be used just as easily for information exchanged over private networks, including corporate internal networks. PKI can also be used to securely deliver cryptographic keys between users, including devices such as servers, and to facilitate other cryptographically delivered security services.

3.0 How does Public Key Cryptography work?

Public Key Cryptography uses a pair of mathematically related cryptographic keys. If one key is used to encrypt information, then only the related key can be used to decrypt that information. If you know one of the keys, you cannot easily calculate what the other one is.

Consequently, in a 'public key system' you have the following:

i) **A public key**

This is something that you make public - it is freely distributed and can be seen by all users.

ii) **A corresponding (and unique) private key**

This is something that you keep secret – it is not shared amongst users. Your private key enables you to indisputably prove that you are who you claim to be.

3.1 The Public Key used for Encryption

Normally, a sender will use your public encryption key when they want to send you confidential information. The information to be sent is encrypted using your public key. You can provide your public key to the sender, or it can be retrieved from the directory or website where it is published.

Note: In normal practice, the actual information being sent is encrypted using a secret key algorithm (symmetric cryptography). Symmetric algorithms are much faster than public/private key algorithms (asymmetric cryptography). A random key (the session key) is generated, and it is used with the symmetric algorithm to encrypt the information. The public key is then used to encrypt that key and both are sent to the recipient.

3.2 The Private Key used for Decryption

A private key is used to decrypt information that has been encrypted using its corresponding public key. The person using the private key can be certain that the information it is able to decrypt must have been intended for them, but they cannot be certain from who the information is.

Note: In normal practice the private key is used to decrypt the session key, and that key is used to decrypt the actual information rather than the private key decrypting all the information.

3.3 The Private Key used for Signature

If the sender wishes to prove to a recipient that they are the source of the information, they use a private key to digitally sign a message (known as a digital signature). Unlike the handwritten signature, this digital signature is different every time it is made. A unique mathematical value, determined by the content of the message, is calculated using a 'hashing' or 'message authentication' algorithm, and then this value is encrypted with the private key, creating the digital signature for this specific message. The encrypted value is either attached to the end of the message or is sent as a separate file together with the message. The public key corresponding to this private key may also be sent with the message, either on its own or as part of a certificate.

Note: Anyone receiving information protected simply by a digital signature can check the signature and can read and process the information. Adding a digital signature to information does not provide confidentiality.

3.4 The Public Key used for Signature

The receiver of a digitally signed message uses the correct public key to verify the signature by performing the following steps.

1. The correct public key is used to decrypt the hash value that the sender calculated for the information
2. Using the hashing algorithm (where certificates are in use it will be stated in the public key certificate sent with the message), the hash of the information received is calculated
3. The newly calculated hash value is compared to the hash value that the sender originally calculated. This was found in step 1 above. If the values match, the receiver knows that the person controlling the private key corresponding to the public key sent the information. They also know that the information has not been altered since it was signed
4. If a public key certificate was sent with the information it is then validated with the Certification Authority (CA) that issued the certificate to ensure that the certificate has not been falsified and therefore the identity of the controller of the private key is genuine

5. Finally, if one is available, the revocation list for the CA is checked to ensure that the certificate has not been revoked, or if it has been revoked, what the date and time of revocation were.

Example: Suppose you are sent a Word document by e-mail. The sender has signed it by calculating a hash value for that Word document, and then encrypted that value with their private key. You receive the Word document, and calculate the hash value for it. You decrypt the hash vale that the sender encrypted and compare the two. If they are equal, the document hasn't changed and you are certain who sent the document. (If they don't match you know that the document has changed or the sender is not who they claimed.) In this way, you can be certain of the authenticity and accuracy of the information that has been received.

The table below shows who uses public and private keys and when:

Key Function	Key Type	Whose Key Used
Encrypt data for a recipient	Public key	Receiver
Sign data	Private key	Sender
Decrypt data received	Private key	Receiver
Verify a signature	Public key	Sender

Table 1 Public and Private Key Usage

To encrypt information that will be stored for your own use (that is, you will be the only person able to read it), you must use your own public key in order to be able to decrypt and read the information later. If you use someone else's public key, then only they will be able to decrypt and read the information.

To avoid the difficulty associated with not being able to read encrypted messages if you are not one of the recipients, that is, you do not have the private key, some systems do not delete the original message after encryption whilst others store a copy of the key used for encryption either under the sender's Public Key or under a System Recovery Key. These methods are also referred to as key escrow or key recovery.

4.0 Digital Certificates

A digital certificate, also referred to as a certificate, is information referring to a public key that has been digitally signed by a CA. The information normally found in a certificate conforms to the ITU (IETF) standard X.509 v3. Certificates conforming to that standard include information about the published identity of the owner of the corresponding private key, the key length, the algorithm used, and associated hashing algorithm, dates of validity of the certificate and the actions the key can be used for.

A certificate is not essential to the operation of a PKI, however, some scheme is necessary to locate information about the controller of a private key, and the X.509 certificate is the most commonly implemented scheme.

4.1 Controlling Key Usage

One of the fields in a public key certificate (certificate) is the key usage field. It is used by the CA to state the uses the CA has approved. It does not mean that the corresponding private key cannot be used in any other ways. There is no certificate with a private key. People receiving information protected using a public key system should check, where a certificate is provided, that the key usage stated in the certificate corresponds to the actual use.

4.2 Storing methods for Public and Private Keys Certificates

Public keys are stored within digital certificates along with other relevant information (user information, expiration date, usage, who issued the certificate etc.). The CA enters the information contained within the certificate when it is issued and this information cannot be changed. Since the certificate is digitally signed and all the information in it is intended to be publicly available there is no need to prevent access to reading it, although you should prevent other users from corrupting, deleting or replacing it.

4.3 Protection

If someone gains access to your computer they could easily gain access to your private key(s). For this reason, access to a private key is generally protected with a password of your choice. Private key passwords should never be given to anyone else and should be long enough so that they are not easily guessed. This is the same as looking after your ATM card and PIN. If someone manages to get hold of your card then the only thing that prevents him or her using it is the PIN protecting it.

Different vendors often use different and sometimes proprietary storage formats for storing keys. For example, Entrust uses the proprietary **.epf** format, while Verisign, GlobalSign, and Baltimore, to name a few, use the standard **.p12** format.

5.0 The components of a PKI

A public key infrastructure is created by combining a number of services and technologies:

5.1 Certification Authority (CA)

A CA issues and verifies certificates. The CA takes responsibility for identifying the correctness of the identity of the person asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

- **Generating key pairs**

The CA may generate a public and private key pair or the person applying for a certificate may have to generate their own key pair and send a signed request containing their public key to the CA for validation. The person applying for a certificate may prefer to generate their own key pair so as to ensure that the private key never leaves their control and as a result is less likely to be available to anyone else.

- **Issuing Certificates**

Unless you generate your own certificate, you will generally have to purchase one from a CA. Before a CA issues you with a certificate they will make various checks to prove that you are who you claim to be.

The CA could be thought of as the PKI equivalent of a passport agency. The CA issues you a certificate after you provide the credentials they require in order to confirm your identity, and then the CA signs the certificate to prevent modification of the details contained in the certificate.

A CA may also state the quality of the checks that were carried out before the certificate was issued. Different classes of certificate can be purchased that correspond to the level of checks made. There are three or four general classes of certificate:

- Class 1 certificates can be easily acquired by supplying an email address
- Class 2 certificates require additional personal information to be supplied
- Class 3 certificates can only be purchased after checks have been made as to the requestors identity

- Class 4 certificates may be used by governments and organizations needing very high levels of checking

- **Using certificates**

An individual may have any number of certificates issued by any number of CAs. Different web applications may insist that you use certificates issued only by certain CAs. For example, a bank may insist that you use a certificate issued by them in order to use their services, whereas a public website may accept any certificate you offer.

The CA can be a unit within your organization, a company (i.e. a bank or a post office), or an independent entity (VeriSign).

- **Verifying Certificates**

The public key certificate is signed by the CA to prevent its modification or falsification. This signature is also used when checking that the public key is still valid. The signature is validated against a list of 'Root CAs' contained within various 'PKI aware' applications (e.g. your browser).

Some CA certificates are called 'Root Certificates' as they form the root of all certificate validation. Certificate validation occurs automatically using the appropriate public certificate contained within the root CA list.

Note: PGP (Pretty Good Privacy) users normally act as their own issuing authority, so you accept their certificate on the basis that they are who they say they are without further verification. This method is called the 'Web of trust' because it is based upon people you trust rather than liability by contract.

5.2 Revocation

Certificates are revoked when they are no longer valid. This can be done in one of two ways. Certificates can be deleted from the directory or database in which they should be found. As a result, any attempt to find them to check that they still exist will fail and anyone looking for them would know that they have been revoked.

There are two problems with this approach:

i) A denial of service attack on the directory or database might create the appearance of a failed certificate

ii) The directory was designed to optimize the time to read information, so deleting information is normally avoided, as is updating

Also, deleting the record does not tell the person asking for the information why it is not there, and they may need to know why and when it was removed.

As a result, a system of revocation lists has been developed that exists outside the directory or database. This is a list of certificates that are no longer valid, equivalent to a lost or stolen ATM card list. Revocation lists may be publicly available even when the matching directory or database is not. This is because certificates may have been distributed for use beyond the private network of the organization involved.

5.3 Registration Authority (RA)

A CA may use a third-party, a Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to ensure that they are who they claim to be. That RA may appear to the certificate requestor as a CA, but they do not actually sign the certificate that is issued.

5.4 Certificate Publishing Methods

One of the fundamentals of PKI systems is the need to publish certificates so that users can find them. There are two ways of achieving this:

i) Publish certificates in the equivalent of an electronic telephone directory

ii) Send your certificate out to those people you think might require it

The most common certificate publishing approaches are listed below.

- **Directories**

  Directories are databases that are X.500/LDAP-compliant. This means that they contain certificates in the X.509 format, and that they provide specific search facilities as specified in the LDAP standards published by the IETF. Directories may be made publicly available or they may be private to a specific organization. A directory is kept private when it contains information that the owner does not wish to be publicly

available. Public directories on the other hand can be read by anyone with access to them.

- **Databases**

  A database can be configured to accept X.509 format certificates. This may be done for private systems where the search methods for locating certificates do not follow the LDAP structure. Because it is essentially proprietary, this method is not used for public systems.

- **Email, CDs etc.**

  Certificates may be sent within an e-mail so that the recipient can add them to their own collection on their server or desktop, depending upon the way their security systems have been configured. They may also be put onto CDs, or any other medium.

5.5 Certificate Management System

This term refers to the management system through which certificates are published, temporarily or permanently suspended, renewed or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA and perhaps an RA will run certificate management systems to be able to keep track of their responsibilities and liabilities.

5.6 'PKI aware' Applications

This term usually refers to applications that have had a particular CA software supplier's toolkit added to them so that they are able to use the supplier's CA and certificates to implement PKI functions. The term does not mean that the applications have any 'knowledge' built into them about what the security requirements really are, or which PKI services are relevant to delivering them. These issues are quite separate from having PKI services available.

6.0 Challenges of PKI

6.1 Issues and Risks in a CA system operation

To issue digital certificates, a CA must verify subscribers' identities; determine the appropriate content of digital certificates; create, distribute, and ensure acceptance of digital certificates; and ensure internal security. Each of these actions introduces some risk to the parties involved. This section discusses some of these risks and tradeoffs that can be made to reduce or spread the risk.

CA systems may be characterized as primarily open or closed. A fully closed system has contracts defining the rights and obligations of all participants for authenticating messages or transactions. This type of system offers the CA operators less risk exposure because there is little uncertainty regarding obligations. Conversely, a fully open system would not have formal contracts defining the rights and obligations of relying parties in the system. In such a system, the firms that perform the CA activities could be exposed to an uncertain level of risk for each authenticated message or transaction. It is likely during early stages of development that most CA systems will be neither fully open nor fully closed, with contracts defining the rights and responsibilities of at least some, but not all, of the system participants.

6.1.1 Verifying Identity

To confirm the identity of a subscriber, the CA either reviews the subscriber's credentials internally or contracts with a registration authority (RA). The decision to outsource and the choice of RA expose the CA to risk. If the CA or RA confirms an identity that is false, or somehow inaccurate, the CA may suffer loss of business or even expose itself to legal actions. Moreover, the CA's outstanding certificates may become suspect if there is a pattern of insufficient due diligence in verifying identities for issuing certificates. The risk exposure from falsely identifying a subscriber may be reduced when a CA issues digital certificates for use within a closed system, because there are contracts in place between some or all of the participants in the system.

6.1.2 Certificate Content

Certificates' content varies by CA system. Content and a certificate's limitations are a source of strategic risk to the issuing CA. Standard certificates identify the subscriber and the issuing CA. Another important element of a standard certificate is the expiration date. The X.509 standards for certificate content require that digital certificates contain the distinguished (i.e.,

unique) name of the certificate issuer (the signer), an issuer-specific serial number, the issuer's signature algorithm identifier, and a validity period. The more limited the life of a certificate, the lower the risk exposure for the issuing CA. A certificate's security has both physical and logical vulnerabilities that are outgrowths of the software used to generate a digital signature. The longer such software is in use, the greater the likelihood that it will be corrupted or that someone will gain unauthorized access.

Certificate extensions provide information in addition to the identity of the subscriber and the issuing CA. Additional information may include suggested limitations on uses of the certificate, such as the number of and type of transactions or messages that subscribers are authorized to sign. Any such limitation reduces the transaction and reputation risk of the issuing CA. The CA also may use extensions to establish classes of digital certificates for use with financial transactions or for transmitting highly sensitive information. Such certificates may be for a single message or transaction, used only with a specific relying party, or limited to a maximum financial amount.

6.1.3 Certificate Creation, Distribution, and Acceptance

The process of creating, distributing and documenting acceptance of a subscriber's certificate exposes a CA to transaction, strategic, and reputation risk. In certificate creation, the transaction and reputation risk exposures arise from possible errors occurring in the systems that match appropriate certificate limitations to each subscriber's unique signing capabilities. Risk exposures are associated with the policies and procedures that control the process.

Certificate distribution and acceptance often are not solely the responsibility of the CA. The subscriber likely will obtain the technology to create digital signatures from a software provider or other technology firm. However, the certificate is not complete until the CA acknowledges the subscriber's signing capability with its own digital signature to create the certificate of record. In a closed CA system, the CA risk exposure may be modified by the contract establishing the exact roles and responsibilities of the parties. Some of the transaction risk may be allocated to a lead organization, individual subscribers and relying parties, or another entity maintaining the database of certificates. However, the CA still may have a reputation risk exposure if problems with the technology are attributed to the CA.

Generally, a digital certificate will not be operational until the subscriber accepts the signed certificate. Certificate acceptance implies that the subscriber agrees to the terms and conditions established by the CA for the overall system as well as any specific conditions that apply to the subscriber. Errors in the communication process with subscribers regarding acceptance, from either inadequate policies and procedures or technical difficulties, expose the CA to both transaction and reputation risk.

6.1.4 Managing Digital Certificates

When a CA issues certificates to support subscribers' digital signatures, the CA usually is interacting only with subscribers or a representative or agent acting on behalf of the subscribers. However, if the CA also chooses to manage outstanding certificates, i.e., act as a repository, the CA will transact with relying parties that receive messages. The following discussion outlines the risk exposures that arise with respect to repository services for both subscribers and relying parties. It is organized to address four aspects of managing digital certificates:

- **Customer Disclosures**

  Although there is no legal disclosure requirement at present, a CA will need to provide some information concerning the basic services provided and the rights and responsibilities of subscribers and relying parties. The nature of the disclosures will have an impact both on the transaction and reputation risk exposure of a CA. For example, if disclosures clearly describe the CA error resolution procedures and privacy policy, there may be less confusion on the part of subscribers. Further, if the CA provides technical documentation on the use of the software associated with certificates, subscribers will be better able to distinguish between problems resulting from the software rather than the CA, shifting some of the reputation risk exposure away from the CA.

- **Subscriber Service and Support**

  Like many new information technology products and services, a CA requires customer support, which is a source of reputation risk. A CA may consider establishing a help desk or some other form of direct interaction with subscribers and relying parties. The policies, procedures and operation of the help desk are a potential source of transaction and strategic risk. Resolving problems or errors that subscribers

and relying parties encounter from lack of familiarity with the use of the underlying technology will require substantial resources from the CA or a customer service contractor. Although the CA typically will not supply software for creating a digital signature, there may be some circumstances in which subscribers attribute all difficulties in using the technology to the CA.

Subscribers may have technical problems because of software configurations on their personal computer systems that may not become apparent until they attempt to sign a message or transaction. Because an organization providing CA services ultimately may wish to maintain the customer relationship, the practical decision may be to provide customer service either internally or to contract with a firm with appropriate expertise. Some technology firms now provide smart cards to hold subscriber certificates. Instead of downloading the software to the PC hard drive, the subscriber would have a smart card reader attached to his PC. The smart card and reader would be pre-programmed to load the certificate information appropriately for the subscriber. Some of the transaction and reputation risk of subscriber service and support may be reduced by the simplicity of the use of hardware rather than requiring PC users to load the software from another source.

- **Suspending and Revoking Certificates**

  Because the subscriber is responsible for maintaining the security of the signature capability, the potential exists that the system may be compromised and made available for unauthorized use. Thus, the CA may be required to suspend or revoke a certificate. If the CA (or another responsible party within the system) does not monitor and take such action in a timely manner, the CA may authenticate messages or transactions carrying expired digital signatures. Thus, CA systems that render a subscriber's digital certificate invalid are potentially exposed to substantial transaction, strategic, and reputation risks. Poorly designed policies and procedures are a source of strategic risk, and improperly implemented ones expose the CA to transaction and reputation risk. The timing of necessary repository updates may differ with the type of certificates involved; a delay in the suspension of a certificate used for sensitive messages or transactions carries relatively high risk.

  A digital certificate may be rendered invalid in one of two ways. The CA may revoke a certificate if it is certain that a subscriber has compromised his signing capability.

The most likely compromise would be if the subscriber did not keep his private key secure. If a subscriber's private key became known, unauthorized individuals could sign messages and transactions. If there is some question as to the status of the certificate, the CA instead may suspend the certificate until its status is determined. Transaction and reputation risk may result from errors in processing both requests for revocation and suspension of certificates. For example, a subscriber whose certificate is erroneously invalidated and hence is unable to sign messages could potentially experience losses and may pursue legal action, damaging the CA's reputation in the process. Conversely, the CA may suffer exposure if a relying party accepts a message or transaction that is signed by a subscriber whose certificate should have been revoked or suspended.

- **Processing Relying Party Requests**

  Substantial transaction, strategic, and reputation risk exposure is associated with processing requests by relying parties regarding the status of individual certificates. Although the CA-subscriber contractual relationship may define obligations to subscribers and others, such contracted protection may not exist for transactions with relying parties, particularly in open systems. For example, if the CA represents a revoked certificate as operational to a relying party, the CA may be exposed to reputation damage or a lawsuit. There is an additional risk in an open system that the circumstances of an individual subscriber or class of subscribers have changed during the valid period of a circulating certificate. Any delays in processing certificate revocation requests as a result of inadequate policies and procedures or technical processing may result in such errors. If the repository processes requests in batch mode as opposed to real time, the risk exposure is greater. As the volume of transactions processed by the repository increases and as more certificates are placed in circulation with varying limitations and expiration dates, risk exposures also may increase.

- **Certificate Revocation**

  There are two recognized methods for responding to a request about the validity of an individual certificate. The most well known method requires the repository to retrieve a lengthy list of invalid certificates, the Certificate Revocation List (CRL), to check the validity of a single certificate. Inaccuracies in the CRL are a source of transaction risk for the CA system. In addition, the scheduled frequency for generating the CRL

will affect the risk exposure of the repository. More frequent generation of CRLs will reduce a CA's transaction and reputation risk exposure. There is also an issue as to whether certificate status is "pushed" out by the CA repository to interested relying parties, or "pulled" from the repository by the relying parties in question.

There are different transaction and reputation risk exposures associated with each method. The "pull" method allows the CA repository to transfer any reputation risk exposure successfully to the relying party with respect to accepting an invalid certificate. On the other hand, the "push" method places the responsibility clearly on the CA if the CRL is not accurate or is not distributed on a timely basis. Because of the risks and cost inefficiencies of the CRL approach, the industry is developing a second method. Several technology firms have developed software that allows a repository to search its records for the validity of a single certificate in real time. Another source of repository transaction risk relates to the ability of a relying party to understand certificate extensions.

7.0 Planning a PKI Infrastructure

This section briefly discusses how different business opportunities have different needs, and how these differences should be considered when planning a PKI.

7.1 Defining Business Requirements

A short example will illustrate how different business opportunities have different needs. If a business is a news magazine that freely distributes data over the Internet, the primary concern is maintaining the integrity of the data so it cannot be modified without authorization. Implementing a PKI to simply enable data integrity may not be a cost effective expenditure of resources. On the other hand, if a business is selling products or services over the Internet, implementing a PKI may be in order. For an e-commerce business, the following must be accounted for when planning a PKI:

- Integrity for the posted prices
- Identification and authentication for a potentially large population of customers
- Confidentiality of customer and transaction information
- Non-repudiation for supporting dispute resolution

Implementing a PKI to enable these various security mechanisms can provide an online merchant with a cost effective approach to risk management. Other considerations for defining business requirements of a PKI include:

- **Careful planning**

  Internet-based e-commerce business solutions are often complex, as are the PKI solutions necessary to support them. Take the time to perform a detailed evaluation of your business and technical environments before taking steps to implement a PKI.

- **Interoperability**

  Does your current business model require interoperability? With whom? For what purpose? If your PKI requires interoperability, you should determine which of the different standards and protocols you must adhere.

Tangentially, most PKI related standards are in the early stages of development and acceptance. ISO, ANSI, IETF, IEEE, and PKCS are a few examples of standards under development for PKI. Because of the competing standards and protocols and the various interpretations that different vendors have of these, it is critical that organizations determine their interoperability needs.

- **Performance and capacity**

In situations where large amounts of data must be enciphered for confidentiality, public key cryptography may not be suitable because the cryptographic algorithms perform at relatively slow speeds.

Symmetric or secret key cryptography is typically used for these applications. Key management is where public key cryptography plays a role in supporting the encryption of large amounts of data for confidentiality. A PKI can be established for the distribution of the symmetric or secret keys that are subsequently used for the encipherment of data. Public keys and public key certificates can also be significantly larger than symmetric keys and this can affect how they are stored. For example, in the limited memory constraints of a chip card, size can matter.

7.2 Determining a PKI system/Architecture and Vendor

There are different PKI and cryptographic systems from competing vendors. Several different protocols, certificate formats, and platforms exist. Some investigation is needed to decide which PKI and vendor is the best for your particular business enterprise. Often a standards compliant solution from one vendor will not integrate with that of another vendor. This may cause problems if you consider a multi-vendor PKI solution.

Also, the implementation of a PKI requires an analysis of the trust relationships that exists in their environment. The awareness of these trust relationships leads to the establishment of an overall trust model that the PKI enforces. The following are three common examples of trust models presented for comparison purposes:

- **Hierarchical**

A hierarchical trust model represents that most typical implementation of a PKI. In its most simple instantiation, this trust model allows end entity's certificates to be signed

by a single CA. In this trust model, the hierarchy consists of a series of CAs that are arranged based on a predetermined set of rules and conventions.

For example, in the financial services industry, rather than having a single authority to sign all end entities' certificates, there may be one CA at a national level that signs the certificates of particular financial institutions. Then each institution would itself be a CA that signs the certificates of their individual account holders. Within a hierarchical trust model there is a trust point for each certificate issued. In this case the trust point for the financial institution's certificate is the national or root CA. The trust point for an individual account holder is their institution's CA. This approach allows for an extensible, efficient and scalable PKI.

There are trade-offs to be considered when determining the placement of trust points for end entities in a KI. In a tiered hierarchy with multiple CAs, categorization of risk can be established, but each CA multiplies the administrative effort necessary to maintain the entire hierarchy. Conversely, a flat hierarchy with a single CA is much easier to administer. However, a failure of that single CA will corrupt the entire trust model and potentially all certificates signed by it.

- **Distributed (Web of Trust)**

A distributed Web of trust is one that does not incorporate a CA. No trusted third party actually vouches for the identity or integrity of any end entity. PGP uses this type of trust model in email environments. This trust model does not scale well into the Internet-based e-commerce worlds because each end entity is left to its own devices to determine the level of trust that it will accept from other entities.

- **Direct (Peer-to-Peer)**

Direct peer-to-peer trust models are used with secret or symmetric key-based systems. A trusted third party does not exist in a direct trust model. Thus, each end entity in a peer-to-peer relationship established trust with every other entity on an individual basis. This indeed, is rather manual and similar to the Web of trust model. This trust model does not scale well into the Internet-based e-commerce world.

8.0 Conclusion

There are few security solutions as comprehensive in what they offer as a well deployed and well managed Public Key Infrastructure. In real world, the trust inbuilt in a normal signature and in the established relationships of personal contact is essential to the business process. Duplicating that in an electronic environment requires a mechanism for establishing the non-repudiation of commitments. PKIs provide trust and bring the confidence of facilitating the electronic duplication of well-established business practices.

9.0 References

- Articsoft, Introduction to Public Key Infrastructure, **http://www.articsoft.com**
- NIST, Introduction to Public Key Technology and the Federal PKI Infrastructure, csrc.nist.gov
- Sun Microsystems, Public Key Infrastructure Overview, **http://www.sun.com/blueprints**
- Real User, The Synergy of Passfaces and PKI, www. realuser.com