Global Information Assurance Certification Paper

Aligning PKI Technology and Business Goals

> The Gartner Group indicates that 80 percent of Public Key Infrastructure (PKI) deployments are pilots and of the 20 percent of production deployments, a full 40 percent will fail within two years of implementation because PKI fails to provide measurable value.[1]

To ensure that an organization does not become one of the failures a full understanding of the total costs involved in a PKI deployment venture as well as the return on this investment, both tangible and intangible must be explored. This paper is not intended to address all the relevant costs or returns associated with a PKI implementation but to give a perspective into some areas that are often overlooked.

Fast and efficient exchange of information is a requirement in today's global economy. For end-users, making the elements of PKI simple and transparent will ultimately be the key for success. Upper management believes that PKI is the means to solve many of the problems that are encountered today. Security professionals are told PKI will be required for e- commerce, B to B, B to C and everything else under the sun. PKI is an enabling technology, an infrastructure that will authorize people and protect data. Many security professionals are examining the infrastructure of PKI to get the jump on businesses by understanding how the technology of PKI works. However, are the costs involved with PKI deployment versus the returns being examined?

> The lesson to be learned from PKI pioneers, say experts: Don't get so carried away by PKI's promise that you let the technology drive the business model rather than the other way around.[2]

The driving force behind any business improvement is to generate revenue. To run the business more efficiently than before by adding software, hardware that will improve, enable, and specifically change their current business processes to increase the bottom line. For example, a business would not purchase a fax machine or implement an email system unless it can be shown that it will improve the bottom line. Keep in mind that in all organizations money is the ultimate driver of change.

Prior to deploying PKI every organization should first define:

1. What application(s) PKI will be used for?
2. What is the financial investment (total costs) required to develop the infrastructure of PKI?
3. How will PKI improve the bottom line and increase revenue (return on investment & return on opportunity)?
4. What are the parameters of PKI use for each application? The rules and guidelines that govern PKI must be in place prior to implementation. Define the policies (Certificate Policy-CP) and management practices (Certification Practice Statement-CPS) involved before, during, and after certificates are issued.

Throughout the world organizations are implementing a new generation of distributed, business-critical applications, enabling delivery of new products and services on an unprecedented scale, over intranets (employees), extranets (trading partners), and the Internet (worldwide customers and prospects). The bottom line of these organizations can be affected significantly by selecting the right approach to PKI.

The market value of a commercial enterprise springs not only form its physical and financial assets, but from the intangible assets it creates. At a minimum the approach to deployment of these PKI applications must ensure that customers have a high confidence level, will be able to operate in a secure environment and have high availability. This will enable organizations to exploit the advantages of the electronic marketplace as seen with faster time-to-market, lower distribution costs, and greater access to global customers. The goal organizations should strive for is running a trusted online service for end users. Success will be determined by the ease of obtaining trusted certificates that will enable internal clients, business partners, and customers secure messaging, access control and security for business applications. Security

professionals will be staking their organization's reputation as well as their positions on the success of the PKI solution.

To explore the costs associated and the economic returns of PKI, businesses need to examine the following questions:

- What are the drivers of this project?
- What do customers want?
- PKI will require change, what level of change is required?
- How will it save the organization money?
- How will PKI improve the bottom line, make more money?
- How will PKI enhance competitive advantage, customer satisfaction?
- How will PKI support existing applications and new applications?
- What will be the economic returns if this technology is applied to specific targeted applications?
- What are the liabilities?
- How will security professionals define the parameters of PKI use for each application?
- What will it cost to build an infrastructure to support PKI?

PKI will establish a framework of trusted relationships among employees, suppliers, customers and a common, comprehensive infrastructure for existing applications and environments as well as, enabling new applications and e-commerce opportunities. Additionally, PKI may have to support different user communities, both inside and beyond the enterprise. How will an organization architect PKI to operate and scale successfully across such communities—intranets, extranets, industry trading groups, and large-scale Internet commerce? What could derail these efforts?

Consider the financial impact to the business by applying the goal of PKI, which is to protect information assets through:

Authentication – to ensure the parties involved are who they say they are by validating the identity of these parties in communications and transactions.
Availability – to ensure that transactions or communications can be executed reliably upon demand.
Authorization – to control parties' access to information.
Confidentiality – protects sensitive information by ensuring that information is not intercepted during transmission.
Integrity – guarantee the transaction is not altered.
Non-repudiation – provide evidence the transaction occurred by ensuring that transactions, once committed, are legally valid and irrevocable.

How can deployment of this tool protect information and meet the business goals of the organization?

To be effective, PKI applications should be tied to measurable business goals and linked to overall business strategy. During the 1980's there was an emphasis in businesses on Quality Improvement and by doing so the organization gets the benefits, to improve business. What has to be asked is what is the value to shareholders if the investment in PKI is made? If an investment in quality is made then there is an expectation of increase in returns. What will be the returns and how will it be shown to shareholders if the decision is made to invest in PKI? To determine this look at what the financial impact to the business, the value and expense associated with PKI and what is the return if the decision is made to invest. Organizations will differ in how they approach PKI business relationships and customer service. There needs to be criteria for selecting PKI that has measurable parameters that will quantify the existing resources and future needs. Many organizations neglect to define an appropriate process of how and what PKI will be used for, in other words what are the businesses specific needs and the corresponding business case that addresses these specific needs.

Many organizations will look at cost as the most important element in their choice of PKI instead of total cost versus the important issues of perceived benefits, flexibility and risks. Organizations should move away from a cost centered focus to one that helps evaluate a project in terms of goals and return on investment. A

return on investment can be calculated by weighing the cost of deployment against the current cost of doing business and how effective an organization could be in serving customers. Additionally, businesses should consider procedures that promote an integrated approach to identifying, capturing, evaluating, retrieving and sharing the organizations information assets.

What are the costs?
When determining the total cost of implementing PKI organizations should look at several important concepts: when possible, leverage existing investments and keep the purchase of PKI in perspective. Examine the impact of costs for products, technologies, processes, people, plant (facilities) over a multiyear period. In addition businesses should scrutinize cost and investment in:

- The requirements to update and include in the overall cost the physical plant for secure computing facilities, physical security, and redundancy.
- PKI products and technologies with the inclusive maintenance and support for client software, client hardware, server software (certificate server, security server, directory services, and PKI server certificates).
- Maintenance and support for the hardware required for the PKI Server.
- The cost for implementation of key recovery for PKI and disaster planning.
- The number of people who will need to get involved in the process, and what costs are associated with those involved. Which applications will PKI be used for and who are the application owners. Full time equivalents (FTE's) required for team members. Subject matter experts will be required, project manager, security manager, PKI architect, and legal advisor. Expertise in networking, servers, help desk development and application integration will also be required.

What are the PKI drivers – why should the business spend the money?
Economic Drivers: reduced cost, new revenue opportunities, shrink cycle time, business partner requirement, reduced risk/fraud, and competitive requirement. Balance of costs and business returns, what can be enhanced? Look at how the organization does business today, how will it be improved? What is the financial impact if this is done differently?

To determine how PKI can support e-business applications look at specifics:
Select a specific business process/application then determine appropriate metrics. Examine the current utilization of this process/application, document current costs and revenues for business as usual. Determine a specific business objective to utilize this application, determine new costs, and revenues. Compare business today to business as a result of integration within a PKI infrastructure.

Three different views (ways to look at PKI returns)
I.) Business to Customers, Business to Business and Internal Advantages
II.) Application
III.) Cost reduction

I.) Business to Customers, business to business and internal advantages

1. Business to Customers, expanding accessibility:
Increase revenues generated online by increasing the number of existing customers doing business online, the amount a customer spends online, and the online customer return rate. Develop a higher level of service and increase overall revenues by authorizing one part of the business to access another part of the business thereby selling other products to the customer.
If PKI is used by the business can it increase revenues by:
   - Increasing an application process completion rate by using digital signatures to complete the transaction online as well as eliminate the cost of printing, paper, and postage.
   - Expand current online accounts to additional product lines.
   - enabling authorized customers to resolve help desk calls directly, online, to maximize customer satisfaction as well as reduce help desk support costs.

2. Business to Business:
   Increase revenues and make it easier to do business with partners. Determine the right metrics for business-to-business interactions and examine enabling benefits of authorizing partners via a secure connection and strong authentication access to sensitive information. Reduction of delivery times and inventories, through the use of web page authorization so the customer could have access to inventory and supplies.

3. Internal Advantages:
   Increase the speed to which a business can adapt to changing market conditions, and reduce costs, through reductions in; cycle time, physical signatures and password resets. What processes today require a physical signature, how could the process be enhanced through the use of digital signatures? Additionally, a business could improve productivity through the use of secure remote access.

II.) Applications of tangible and intangible enhancements: Look for the right strategic fit and systems integration in business applications and processes. If PKI is used by the business can it increase revenues by:

- improving collaboration with others, protect intellectual property, without compromise? In the arena of supply chain design and development PKI will enable strong authentication of users, private communications via encryption, and access to information at the source as well as the destination.
- addressing customers concerns about privacy? Many corporations are looking at secure privacy for applications as a method to enhance customer base. What elements of privacy when added to legacy and new applications will address customer concerns thereby, making the customer more comfortable. Customers and suppliers demand that their information be secure, an Organization's on-line reputation is at stake over intranets and the Internet. PKI can meet the requirements of authenticity and integrity of online information.

> I can assure you that a company's greatest asset is their credibility. This is known as brand equity, the measure of a customer's faith in a company. It is one of the most valuable assets a company has, and it can be damaged severely by incidents that shake customer faith.[3]

- expanding access to specific processes? Greater value could be realized if both customers and suppliers are allowed to submit orders, open accounts, process invoices and obtain the status of orders online. PKI will address the requirements needed by authentication of both parties in a transaction, ensuring privacy and the integrity of transmitted data.
- allowing customers and suppliers to transfer funds and make payments online? PKI will enable, privacy, integrity of information, and non-repudiations.
- increasing the ability for employees, customers, partners and suppliers to access controlled/proprietary, copyrighted information? Distribution of copyrighted material to specific individuals can be ensured and the organizations can control the privacy of information, and protect intellectual property.
- reducing the time it takes without reduction in integrity to process an application?
- using strong authentication to eliminate help desk calls caused by password resets?

III.) Cost reductions

What costs can be avoided through the use of PKI? How do organizations spend fewer dollars than before by the inclusion of PKI in existing and new processes? PKI can benefit savings and reduce cost by authentication of users, insuring the integrity and accessibility of information.

- Examine what applications a physical signature is required for and a business can realize the direct cost saving advantages of PKI both internally and externally.
- Reductions in personnel can be realized if these benefits are applied to self-service organizations. For example, enablement of 24x7 access.

- Keep selected customers instantaneously informed about an ever-changing set of products and services specific to them and their contractual needs.
- A big return on a PKI investment can be gained through changes to help desk service. Examine the type of online customer service verses cost per transaction and ensure that the new application is as good and responsive as the legacy agent involved.
- Remote communications can realize benefits of site-to-site through secure VPN connections.
- Additionally, stronger authentication than with a userid/password alone, easier management and administration of devices.
- Savings can be seen with a reduction in administrative staff, training costs, and improved customer service.
- Prevention of opportunity losses. Failure to implement a PKI infrastructure could result in loss of business relationships or the ability to participate with a key partner as seen today in the auto supplier network with ANX and Covisint. There are regulatory compliances as seen with HIPAA that if not met can reduce profitability significantly.

Additionally, PKI infrastructure enables a secure environment for business, suppliers and customers to keep informed about an ever-changing set of products, services and real time inventories. As businesses outsource more and more activities to supply chain partners, competitive advantage is dictated less by physical assets and more by intangibles such as brand equity, rate of innovation, compressed product development cycles and sophisticated logistics. For example: just in time inventories, and the ability to access a global supply base instantaneously enables manufacturers to construct, deconstruct and reconstruct a unique supply chain to satisfy each instance of demand.

Policies and Practices

Another area that businesses neglect to have in place prior to going down the PKI road are the rules. A business must first determine the parameters for use.

The rules and guidelines that govern PKI for each application must be in place prior to implementation. Surrounding the implementation of a CA are the policies and management practices involved before, during and after a certificate is issued. There are two documents that will need to be addressed prior to PKI implementation. A Certificate Policy (CP) and Certification Practice Statement (CPS). A determination must be made if the business will be the Certificate Authority or outsource the function.

Certificate Policy is a named set of rules that define the applicability of a certificate to a particular community and/or class of application with common security requirements. While all Certificate Authorities (CA's) need strong security, the cost of building and operating a secure facility and the up-front financial commitment are daunting to many organizations. Outsourcing the CA function is not necessarily the answer either. Enterprises frequently want full policy control over PKI, in terms of deciding who receives a certificate, what the certificate contents are, how and when certificates are revoked, and day-to-day operation of the CA.. The full complement of strong security controls must also be employed, including physical security of the facility (room, building, and equipment) housing the CA, personnel security measures (including screening and specialized training of all staff with access to the CA), and procedural controls to enforce such policies as dual control over all sensitive functions. The secure facility typically needs to be operational on a 24x7 basis, and needs full disaster recovery backup.

A Certificate Policy should address and define the following:

- General provisions addressed by the policy, what is covered and what is not covered.
- Registration Authority
- The community involved and the applicability of the PKI (whether this will be an open or close system)
- Technical security controls
- Procedural security controls
- Operational requirements
- Key management

- Certificate and Certificate Revocation List (CRL) profiles
- Policy administration

Certification Practice Statement
While the CP states what policies are to be adhered to the CPS defines how those policies are implemented. Generally the CPS defines the roles and practices for the operation, maintenance and administration of a CA. It will also take into account liabilities and legal responsibilities. The published statements of the CPS will address start up procedures, audits, disaster recovery, financial and legal responsibilities. The operations context of the CPS will address enrollment, validation of applications, issuance, acceptance, publication, certificate usage, suspension, revocation and expiration. Additionally, warranties and limitations of liability, conflict resolution procedures, and change procedures are addressed.

Components of a certification practice statement:

- Operational policy will address backup procedures, certification revocation list (CRL) issuance frequency, lifetime of keys and certificates, disaster recovery, investigation of system and user key compromises, key generation and protection.
- Management policy should address validation of applicant identity for specific utilization and type of CA to be issued (registration authority). Staffing requirements, certificate issuance, distribution, and retrieval. Recording keeping and audits.
- Security policy will outline network and host security, physical security for the CA, directory and user workstations, certification revocation list checking and ensuring that all applications and devices check the CRL before granting access to a resource. Confidentiality of user information and protection of enrollment information.
- Legal policy will summarize the warranty, what applications and devices is the certificate good for? The liability, what risk does the organization incur if the certificate is used for a fraudulent transaction? What precautions should the organization take to prevent fraud, and how should a certificate be insured. Define the responsibilities of users, partners, agencies etc.
- Classes of Certificates. Depending on the type of credentials presented by the requestor and the validation methods and tools used by the registration authority, different levels of assurance may be associated with a certificate.

Summary

A PKI investment for enterprise wide utilization would not be prudent without a complete understanding of all the costs involved. The decision to purchase PKI should be based on the ability of PKI to provide operational efficiency's and cost savings. Total cost of this purchase and it's returns need to be understood before the investment is made. Additionally, the guidelines for PKI; defined infrastructure, how it will be used, deployed, limitations, liabilities need to be defined and communicated to the organization in their entirety prior to deployment of this infrastructure. The nature of information security from the business point of view is that an organization has a dual responsibility of making money with this technology (i.e.: creating ROI), while protecting it's own and its customers information by mitigation of security risks.

Take it one project at a time and remember to keep it simple for the end user. Many PKI implementations fail because companies succumb to the temptation to integrate too many applications with PKI at once.

References:

[1] Armstrong, Illena. "PKI: Has it Truly Arrived Yet?" SCMagazine, August 2000
URL: http://www.scmagazine.com/index2.html

[2] Chen, Anne. "PKI starts to deliver", Eweek, April 1, 2001
URL: http://www.zdnet.com/eweek

[3] Proctor, Paul. Practical Intrusion Detection Handbook, page 102, Copyright 2001 Prentice Hall

Armstrong, Illena. "Budgeting for Infosecurity" SCMagazine, March 2001
URL: http://www.scmagazine.com/artframe_thismonth.html

Boeyen, Sharon. "Certificate Policies and Certification Practice Statements", Entrust, February 1997
URL: http://www.entrust.com/resourcecenter/pdf/cps.pdf

Marinier, Francios. "25 Steps to the Successful Implementation of a Corporate Public Key Infrastructure"
URL: http://www.pkilaw.com/25step.htm

PKI Law
URL: www.pkilaw.com

Public-Key Infrastructure (PKI) The VeriSign Difference
URL: www.verisign.com/whitepaper/enterprise/difference/introduction.html

RSA Security "Unlocking PKI's Return on Investment" presentation, February 2001

Understanding Public Key Infrastructure (PKI) – Technology White Paper
http://www.rsasecurity.com/products/keon/whitepapers/pki/PKIwp.pdf

VeriSign's Certification Practice Statement
URL: http://www.verisign.com/repository/summary.html

Zimits and Montano. "Public Key Infrastructure: Unlocking the Internet's Economic Potential" IStory Volume 3 , Issue 2 (April 1998)
URL: www.iword.com/iword32/istory32.html

Aligning PKI Technology and Business Goals
Practical Questions

1. Why do many implementations of PKI fail within two years?
   a.) PKI will support new applications but not legacy applications.
   b.) Outsourcing the Certificate Authority is too costly.
   c.) PKI fails to provide measurable value.
   d.) Security professionals do not understand the technology.

Answer: C According to the Gartner Group 40% of PKI implementations will fail within two years because PKI fails to provide measurable value.

2. The non-repudiation aspect of PKI protects information by
   a.) Protecting sensitive information
   b.) Providing evidence the transaction occurred and is legally valid
   c.) Controlling parties access to information
   d.) Ensuring transactions can be executed upon demand

Answer: b. Non-repudiation is a fundamental goal of PKI as seen with a digital signature.

3. PKI can increase trust in a transaction by guaranteeing the transaction is not altered. The goal of PKI that is responsible is:
   a.) Authentication
   b.) Confidentiality
   c.) Integrity
   d.) Availability

Answer: c Trust is an intangible asset that can increase an organizations revenue.

4.) Brand equity is:
   a.) The measure of a customer's faith in a company.
   b.) The ability to authenticate both parties of a transaction.
   c.) The measure of how well a company can adapt to changing market conditions.
   d.) The measure of a businesses ability to expand current online accounts to additional product lines.

Answer: a A businesses greatest asset is their credibility, which can be severely reduced by the perception of lack of privacy or unsecured transactions.

5.) The goal of PKI that will ensure the parties involved are who they say they are is referred to as:
   a.) Integrity
   b.) Authentication
   c.) Authorization
   d.) Confidentially

Answer: b. Authentication by based upon a private key, which gives the receiving party knowledge of identification.

6.) A Certificate Policy states what policies are to be adhered to and the Certificate Practice Statement defines how those policies are implemented.

Answer: True

7.) An organization should look at infrastructure cost as the most important element to determine if PKI should be implemented.

Answer: False Infrastructure cost is one of many elements that should be scrutinized when making the determination if PKI should be implemented. The most important element is how PKI will add value to the business.

8.) PKI is an enabling technology, an infrastructure that will authorize people and protect data.

Answer: True

9.) Operational policy, and Classes of Certificates should be included in a Certification Practice Statement.

Answer: True

10.) A secure facility that houses a Certificate Authority typically needs to be operational on a 24X7 basis and needs full disaster recovery backup.

Answer: True