Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

No Single Killer App for PKI

Talk about Public Key Infrastructure (PKI), the technology behind digital certificates, and opinions start flying. While there have been a number of successful implementations over the past five years, many evaluators still see PKI as a technology poised at the starting gate. As with most research papers on the subject, this one covers the well-known security functions enabled by PKI. More attention, however, is focused on business and technology issues associated with PKI implementations. Reflecting on five years of P...

Copyright SANS Institute
Author Retains Full Rights

AD

No Single Killer App for PKI
So, where is the value?

Cliff Schiller

GSEC Practical Assignment, version 1.4

October 1, 2002

© SANS Institute 2003, Author retains full rights

Abstract:

Talk about Public Key Infrastructure (PKI), the technology behind digital certificates, and opinions start flying. While there have been a number of successful implementations over the past five years, many evaluators still see PKI as a technology poised at the starting gate. As with most research papers on the subject, this one covers the well-known security functions enabled by PKI. More attention, however, is focused on business and technology issues associated with PKI implementations. Reflecting on five years of PKI project experience, the author will identify technology trends and valuable lessons learned that might help the success of any PKI project. Finally, after evaluating truths about the title statement "No single killer application for PKI" this paper presents the author's perspective on the real benefits of PKI as a technology.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents:

1. Table of Contents 2
2. Introduction 3
2.1. Observations, perspectives, convictions 3
2.2. Discussion topics 5
3. Background 5
3.1. PKI – vision 5
3.2. PKI market overview 6
4. Functions / uses of PKI 8
4.1. Authentication 9
4.2. Signing 10
4.3. Encryption 12
4.4. Non-repudiation
5. Issues to address 15
5.1. Technology 15
5.2. Certificate Architecture and Policy 19
5.3. Legal 20
5.4. People 21
6. Conclusions 22
6.1. The real value of PKI? 22
6.1.1. PKI as an enabling technology 22
6.1.2. The scalability of PKI 23
6.2. Closing observations 23
References 25

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction:

(Observations, perspectives, convictions)

As with most technologies, the true value of PKI lies somewhere between vendor hype and the apprehensions of their targeted audience. For years, vendors have pushed PKI, as the "Holy Grail" of secure E-commerce. Many IT professionals shun the embrace of PKI for various reasons:

- The technology is not proven
- It's too costly
- It's too complex
- The learning curve is too high
- They are still waiting for someone to create the first killer application for PKI before their organization will consider its use

Honest assessments of these statements will reveal varying degrees of fact combined with some degree of fiction. These statements should, however, be discussed fully when addressing legitimate issues but not in the context of why to avoid the technology. Consider the above statements another way.

Is PKI unproven?

Many who feel this is true are not aware that an SSL-enabled web server uses a machine-based PKI certificate to achieve that protection. Other proven PKI technologies will be discussed later in this paper.

Is PKI too costly?

The upper end of the technology can be somewhat costly, but not all PKI solutions require high-end solutions. Also, the first implementation of digital certificates is typically not the last. With a sensible strategic architecture vision, an organization can mitigate the cost of the technology by targeting the same digital certificates in a second, third or fourth security implementation. Scaling the use of a technology across multiple applications, uses, functions and environments is much more attainable with PKI than with most other security technology.

Is the technology complex and is the learning curve high?

There is a degree of complexity to the initial installation of some of the PKI components. Over the past couple of years, vendors have begun ironing out many of the issues impacting the digital certificate installation. They have also improved the customer support models allowing implementation of personal digital certificates to be come easier for the end user. In addition, once past the implementation stage, the actual use of the technology is in many cases a no-brainer.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Are there any killer applications for PKI?

If one is convinced that there are none, this paper will not change his or her mind. I actually believe this myself. The true value of PKI, however, does not lie within the limits of any single application or function. Consideration should be given to PKI's capacity for multiple use and flexibility. Many technologies will match (maybe even exceed) the performance capabilities of PKI on single situation evaluation. For example, when comparing the merits of two-factor authentication between a high assurance digital certificate and technology similar to RSA's secureID®, the debate can be long, heated and may not produce a clear winner. Unlike secureID® technology, however, PKI-based digital certificates are rapidly being embraced as an authentication mechanism by a growing number of vendors plus they can be used for other security functions such as signing, encrypting, etc. I believe the trend will continue, as more and more vendors embrace the standards around X.509 certificates for diverse business functions.

For the past five years, I have been involved in several projects that incorporated the use of many security technologies. I have experienced PKI used as the enabling technology for:

- Signing and validating electronic forms in an Internet-based process
- Verifying posted credentials of web-based components
- Enforcing nonrepudiation of electronically submitted files
- Encrypting documents and data files containing sensitive and confidential information
- Securely transmitting E-mail and other electronic messages
- Authenticating users through a single sign on portal to a protected environment
- Validating server and user authentication credentials prior to the creation of a VPN connection
- Validating server credentials for creating SSL connections to a protected web site

There is wide variety and a number of uses for this technology. A more notable concept, however, is that PKI is not the primary solution, but the enabling technology for all of these (and several other) security-related functions. When looking to compare PKI with competing technologies (e.g. biometrics, smart cards, authentication tokens, other encryption algorithms, etc.) experts will line up on both sides of the debate. Some technologies for specific reasons and in specific implementations provide comparable protection. Where PKI outshines each of these technologies is its scalability. It can enable a broader range of security and authentication solutions than any other security technology. Because a growing number of vendors are embracing X.509 PKI standards, digital certificates will soon be useable across more hardware, software and operating system environments than competing technologies.

Any thorough study of PKI technology should acknowledge there are significant issues that cloud the way to the ubiquitous use of PKI technologies. I will touch on some of the more visible and painful. Although I will cover some technology details in discussions of what makes PKI work, this paper will assess the mix of implementation issues (business,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

technical and policy) that organizations will have to address within any successful project that uses PKI as a security technology enabler. Much of the foundation work for this paper was gathered during the PKI related projects I mentioned above and from "lessons learned" reviews of each of these projects.

(Discussion topics)

If an organization is planning an IT project involving a PKI or digital certificate component, sorting through all the issues can be quite challenging. During the first PKI project in which I was involved some years ago, fewer resource materials were available. Other organizations that were involved in or had completed similar projects were extremely hard to find. The discussion topics in this practical will cover areas where our projects faced many of these issues and learned significant lessons. In addition to recent research some resources were collected over the past five years. The following topics are included in this research paper:

- Background
- Functions and uses of PKI
- PKI - issues and trends
- PKI technology trends
- Conclusion – So, where is the value of PKI?

Background:

(PKI – Vision)

The origins of PKI have been around since shortly after 1976 when Whitfield Diffie and Martin Hellman published their foundational paper on public key infrastructure entitled "New Directions in Cryptology". The RSA public key infrastructure cryptosystem was the earliest implementation. Earliest uses of PKI and digital certificates were found in financial institutions, telecommunications companies and (federal) government institutions. As a security technology, PKI has both enthusiastic proponents and opponents. From the very early days, vendors looking to market their product have extolled the virtues of PKI as the great E-commerce enabler. Many vendors had what I call a precious metal perspective. They saw PKI as a combination of their silver bullet and personal gold mine. At last, they thought, we have a technology that the world can use to:

- Resolve the identity of the intangible person on the other side of the Internet
- Encrypt sensitive data for transmission over the wire
- Ensure transaction integrity with a personal signature mechanism

One seriously underestimated projection was user endorsement. One perspective of endorsement is evident in the following quote from a SANS Alert in the fall of 2001.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

> "PKI will continue to steadily but not explosively evolve and improve. It will not (must not) die. Throughout 2001, the world will still rely primarily on passwords/PINs for online authentication."[1]

Although the number of successful implementations continues to slowly grow, one still finds mixed endorsement from the user community. It can be accurately stated that scores of users did not quickly jump on the PKI bandwagon. Right or wrong, many of the arguments cited in the introduction of this paper were at play as drivers to hold back the floodgate of user endorsement.

Any objective writing on PKI is not complete without an acknowledgment of views from those who hold the technology in a negative light. Many IT experts believe the technology is full of flaws for one reason or another. One opposing view belongs to Carl Ellison and Bruce Schneier. According to Carl and Bruce, issues with the technology include weaknesses with the Certificate Authorities (CA) model and processes, lack of controls over managing private keys, security issues on the computer or hardware devices that store the private keys, and the inability to absolutely know who the person is that is using the digital certificate on the other side of the connection. The coauthors also make several points about old theory of the security chain being only as strong as its weakest link[2]. There are some truths to Mr. Ellison's and Mr. Schneier's analysis. Although somewhat valid, the issues cited should not result in the total dismissal of the technology. In particular organizations should not rely only on technology to address all of its security issues. Technology and business policy should be driven by the same requirements. Also, looking for a single technology or single solution to cover all the bases of security requirements is a pipe dream. There are many issues that can be addressed with PKI. No security technology, however, will ever negate the need for policies, trading partner contracts, legal agreements, etc., enforcing the organization's rules from a business perspective. There are steps on the technology and business side that organizations can take to intelligently address the areas of concern identified about PKI, without throwing the baby out with the bath water.

In reality, the acceptance and use of PKI falls somewhere in the middle between the vendors' utopian dreams and the vision of those who feel the technology is unproven. There are unilateral successes with the use of PKI for enabling SSL. The technology is also finding growing uses as an enabler for other security technologies such as VPN, S/MIME and authentication portals including Single Sign-On (SSO) solutions. PKI may not be the tool for solving every security problem. It does, however, have significant value and I believe its use will continue to grow. For the PKI vendors who survive the death of their early gold mine vision, there will be a market niche for their product.

(PKI market overview)

---

[1] Moulton, Bruce. Vice President - Infrastructure Risk Management. Fidelity Investments. "Expert Predictions for Security Trends In". SANS SECURITY ALERT. December 2000

[2] Ellison, Carl and Schneier, Bruce. "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure". Computer Security Journal. Volume XVI, Number 1, 2000

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A look at the early market reveals that the vendor's hype was met with low endorsement by the general IT and user communities. Besides apprehension, some of the tangible roadblocks of PKI acceptance included a lack of developer tools, RSA's encryption algorithm patent, high priced and immature marketing practices, interoperability between vendors, implementation complexities, certificate management and revocation, scalability, and in some cases response time impacts due to encryption.

In spite of some of the early challenges, some important endorsements of PKI have come in the last several years from a couple of areas including health organizations, the finance industries and government. The endorsements appear to embrace PKI's strengths in the areas of authentication, nonrepudiation and encryption. One long-term bright spot seems to be server-side PKI implementations. Few people actively campaign against the merits of SSL. Server certificates for enabling SSL have received positive endorsement since around 1995. SSL is a PKI enabled process between a web server with a PKI certificate and any web-browser client that has the root certificate for that server in its root certificate store. Because of scalability issues related to symmetric cryptography and authentication using pre-shared keys, there is also a growing market for the use of PKI enabled IP Sec certificates for the handshake processes enabling VPN. VPNs are used to provide an encryption tunnel between two servers and between a server and a client workstation.

Early PKI companies to become CAs included Baltimore Technologies, VeriSign and Entrust. These companies marketed their certificate engines and their own Certificate Authority services for generating and managing certificates. At some point in time, another CA model appeared. New CA companies contracted with one of the major PKI vendors for their certificate generation engines. The new companies found their niche by selling other CA services including policies, practices and protections around certificate distribution and management, Certificate Revocation List services (CRL), Certificate Policies, (CP) and Certificate Practice Statement (CPS). Early CA services were immature. As vendors' visions of the silver bullet began to fade, the combination of too many vendors, not enough market, and immaturity of product/services caused some CAs to sell, buy or go out of business. Recently, I opened up my weekly electronic subscription to CIO's *Security & Privacy Update* to find the first article entitled "Why PKI is only mostly dead". The article quoted a manager of one of the major PKI vendors as saying, in so many words, that the days of hype were over. That company was removing the term from its vocabulary because, "marketing PKI as a concept doesn't work[3]". This relates closely to the key hypothesis of this paper. With PKI, there is no single killer application, selling PKI as a solution in and of itself is a hard sell. Just because a vendor has a PKI solution to provide, does not mean it has the keys to the gold mine. Vendors who were not able to put this into perspective have, and will continue to have, trouble surviving. Of the CA companies that did survive, many have finally

[3] Berinato, Scott. "Only Mostly Dead - RIP PKI. Why a security platform never took off". CSO online, Alarmed column. May 23, 2002

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

matured in the delivery of products and services. It did take years, but CA products and services are beginning to reach a usable level of maturity. Issues mostly resolved include those relating to certificate issuance, key escrow and recovery, interoperability, certificate management and revocation, scalability, and encryption speed. Almost from the beginning, the right standards were in place, although not all vendor implementations embrace those standards the same way. This has mostly been worked out.

In addition to using a vendor-managed CA, some organizations have chosen to provide their own CA services. Options include homegrown packages that offer total CA services and several versions of vendor/organization hybrids. In these hybrids, sometimes the vendor is the actual CA and the organization provides varying degrees of Registration Authority (RA) services. Organization-based RA services range from managing the identity proofing responsibilities to managing the generation of public/private keys using the CA's key generation engine. Other functions, such as on-sight mirroring of certificate revocation lists (CRL) are sometimes provided within the business organization.

On the lower end of the personal digital certificate scale, some low-cost and free PKI certificate services have made an appearance. These certificates tend to be browser-based, that is, the private key lives in an internal browser storage location. The free certificate services also tend to have little or no process for identity proofing. Most of these services are Internet-based. Typically, the requestor visits the vendor's web site and supplies some basic user information. Upon completion of the on-line request process, the user is issued a certificate. In most cases there is little or no identity proofing involved in the process. Also, formal structure tends to be very light, if present at all, for most CA practices relating CP, CPS and CRL. These are the processes, policies and standards involved in protecting the issuance, maintenance and revocation of PKI-based digital certificates. One market trend that has emerged in the last two years is the universal acceptance of standards supporting X.509-based PKI. Version X.509 appeared in 1988, while the current version 3 for PKI certificates and version 2 for CRL was adopted by the Internet Engineering Task Force (IETF) in 1996. Acceptance of this standard by most vendors has provided the groundwork for interoperability of the technology. More work is needed, however, in the area of CPs and CPSs. Much of this work is being addressed in the Federal Bridge Certificate Authority (FBCA) policy. The concept of this draft certificate policy is to supply standards for mapping CPs from independent CAs against five certificate assurance levels. The FBCA standard certificate levels are entitled test, rudimentary, basic, medium, and high. Theoretically, the issue of interoperability between CAs for different PKI domains can begin to make strides towards resolution as government agencies and independent CAs sign up for the Federal Bridge CA services.

Functions / uses of PKI

Before presenting any of the issues related to PKI, a discussion of the functions this technology provides is in order. Even though researchers do not agree on the extent to which PKI is able to perform, the data is fairly clear on the functional categories of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

service this technology provides. Most references tend to cite a similar set of PKI functions. However, they differ slightly on how they categorize these functions. For the purposes of this paper, I have grouped the functions that PKI provides into the following four categories:

1. Authentication
2. Signing
3. Encryption
4. Nonrepudiation

I will define and describe each category then break them down into the individual functions PKI provides in delivering this service.

(Authentication)

Authentication is the act of establishing the identity of an individual combined with the verification of authority granted to that individual. PKI provides authentication services by validating the presence of an individual's digital certificate and the knowledge of the certificate's password, combined with the validation and communication of preestablished information about the identity of the key holder by a trusted third party. It is commonly understood the use PKI for this service falls into the category of two factor authentication. Something one has (a digital certificate) with something one knows (a password or passphrase). This is especially understandable with hardware-based implementations where the user's private key is housed in a token, smart card or hardware device. During the authentication process the user is challenged for his or her digital certificate credentials which are validated against a certificate revocation list (CRL), managed either at the CA or produced by the CA, and mirrored in an environment accessible to the application or authentication service.

Functionality provided by PKI within the category of authentication includes establishment of identity as listed above. Unlike other methods of authentication, PKI also has the ability to provide a linkage to valuable user attributes. Let's look a little deeper into both of these functions.

The diagram (figure 1) below depicts a PKI-based authentication process used for sensitive applications. It is used to protect access to applications within a secured web environment. It assumes the trading partner is already a registered user of the application and that their PKI credentials are known to the application's internal user profile.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

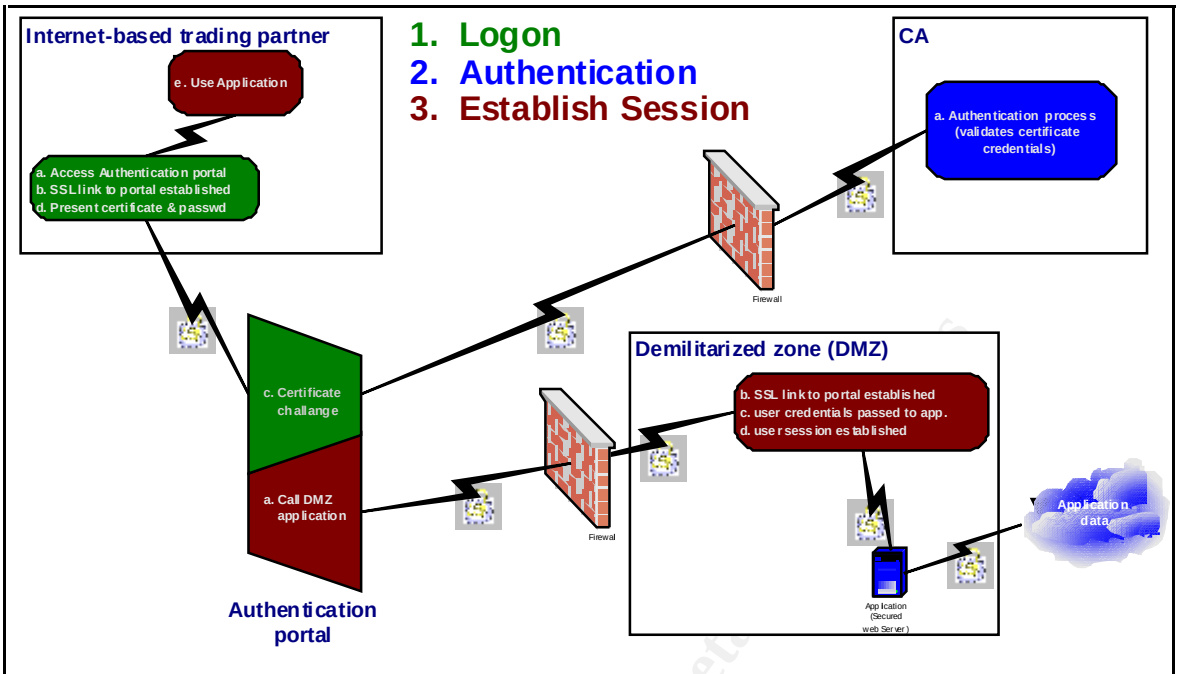

figure 1 – PKI authentication to secured web environment

In this example, the credential challenge happens at the authentication portal outside the application. The identity of the potential user is verified before any connections to the application are created. Only after the Certificate Authority authenticates the trading partner's certificate, is the secured link from the portal to the application established.

As stated above, PKI-based certificates can enable processes for associating relevant user attributes. Sometimes it is just as important to know a trading partner's associations and credentials, as it is to identify the individual. Information such as a person's employer, professional licenses, certifications, organizational affiliations, etc. is sometimes used to determine eligibility and user privileges within an environment or application. PKI-based authentication mechanisms have several methods available that can provide or link to this type of data. User attributes are sometimes carried within the digital certificate data, but more often are housed in external data structures. Directory Access Protocol (DAP) that support the full X.500 protocol or Lightweight Directory Access Protocol (LDAP) that support subsets of the X.500 protocol allow X.509 certificates to link to a person's attribute data. LDAP has gained in popularity because it is smaller, faster, and easier to implement. Examples of this kind of directory services include Microsoft's Active Directory, and Novell's eDirectory.

(Signing)

Signing with a PKI-enabled digital certificate is the act of using an encryption hashing algorithm to bind a person's certificate credentials with the object being signed. PKI signing functions include the ability to sign such objects as documents, electronic forms, files and fields. Although a few implementations of PKI client side software

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

independently enable the ability to sign files and documents out of the box, most do not. Enabling this functionality requires the use of third party software. More details on this are provided in the issues section below.

Another signing function that can be achieved with PKI is workflow enablement or verification. This functionality is actually an extension of the ability to sign fields on an electronic form or within a PKI-enabled application. The workflow example (figure 2) shows a simplified scenario of how workflow enablement might work within an automated travel reimbursement request application, which has four required fields, two signatures and designated business processing rules.

Requestor	• Fills out an electronic "travel reimbursement request" form entering four required fields and applies his/her signing private key to sign the designated signature field ➢ The application locks the four required fields and uses an encryption algorithm to create an electronic hash combining those fields with requestor's signature ➢ Form is submitted for approval to the approving manager
Approving Manager	• Uses the requestor's signing public key to verify both the signatures and the values in the four required fields • Assuming the values in the required fields meet business requirements, grants permission by applying his/her signing private key to the designated signature field for approval ➢ The application locks requestor's signature field and uses the same encryption algorithm to create an electronic hash combining the two signature fields ➢ Form is submitted for payment to the fiscal officer
Fiscal Officer	• Uses the approving manager's signing public key to verify the approving manager's signature and the value of the signature field of the requestor • Assuming the values in the two signature fields meet business requirements, cuts a check for reimbursing the requestor

figure 2 – Workflow example

Because of the ability to specify which fields are bound up in the encryption algorithm applied by each signature, a sequential, auditable process can be configured and automated using PKI's signing functionality. It is this auditable sequence that allows PKI to enable workflow functionality.

It is important to note that in the signing process an encryption algorithm is used, but the process only produces a hash or abstract of the values and does not encrypt the signed data. In most digital certificates, the signing keys are a different key pair from that of the encryption keys. A person who has the need to both sign and encrypt is usually required

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

to possess both types of key pairs. The diagram in figure 3 depicts a document signed with the signing private key of a digital certificate holder.

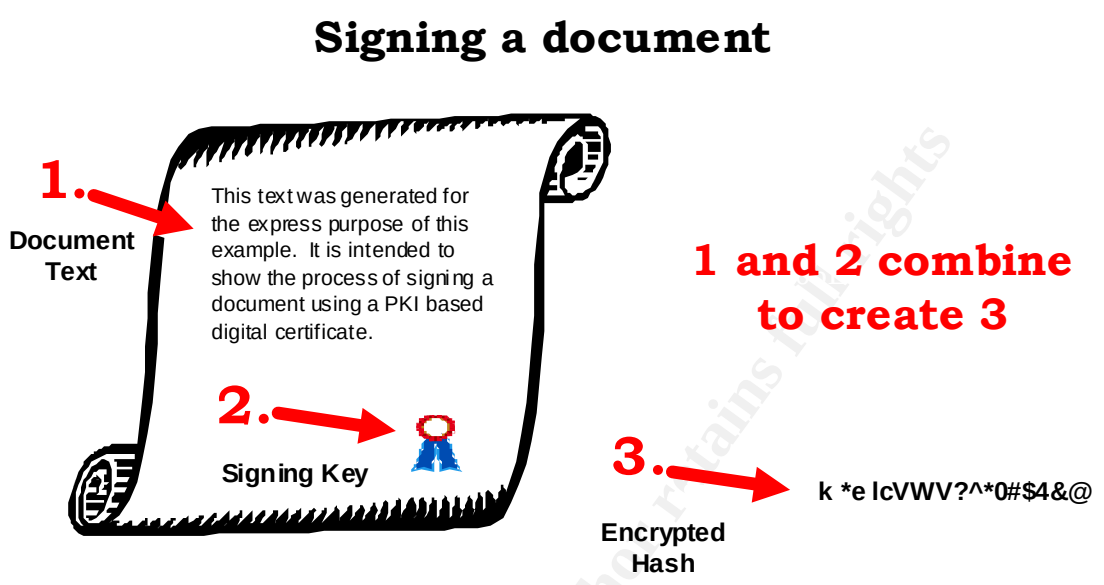

figure 3

(Encryption)

Some security technologies are used to encrypt data in transit while others are use to encrypt the data at rest. Both can use PKI as an enabling component to get the job done. Encrypting data at rest with a PKI-enabled digital certificate is the act of using an encryption algorithm to bind a person's certificate credentials with the object being encrypted. Unlike signing, however, the certificate credential used is the public key of the intended recipient. Functions enabled by PKI include encrypting objects such as documents, electronic forms, files and data. For this encryption function only a very few implementations of client-side PKI software provide this ability out of the box. Encrypting an object typically requires the use of third party software with a user interface that has been PKI enabled. The diagram in figure 4 depicts a document encrypted by the encryption public key of the party targeted as the receiver.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

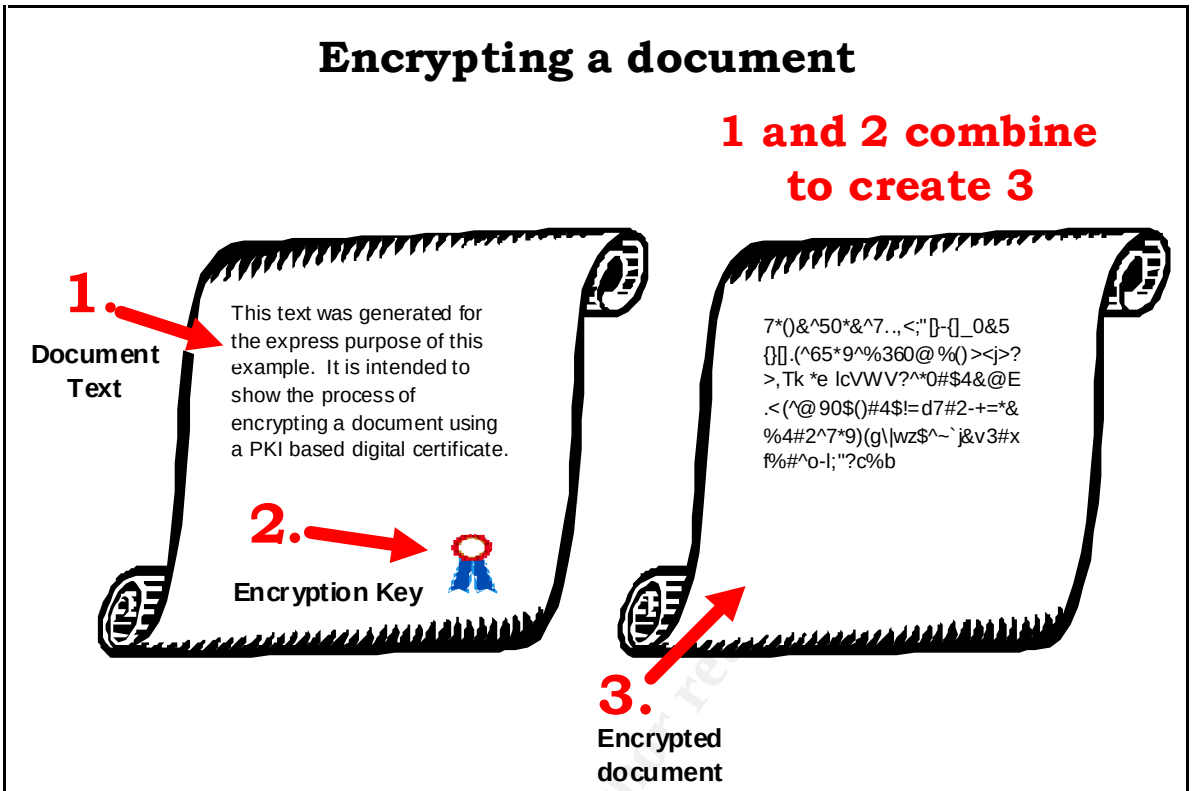

figure 4

Encryption methods that protect data during transit use a different approach. Descriptions of this type of encryption function sometimes use an analogy of a protective tunnel or pipe through which data travels, although a better analogy might be a stream of encrypted capsules flowing between two end points. In this category, PKI can enable such technologies as SSL/TSL, S-HTTP, SSH, and VPN. In addition to the encryption components, PKI also enables the authentication function to verify one or both end points or users prior the creation of the tunnel. With VPNs, the PKI-enabled handshake can authenticate between two servers or a server and an individual, and the authentication can be either one- or two-way. With SSL/TSL, the authentication handshake is typically one-way. The client's web browser uses PKI verification to recognize the credentials of the web site, before the protective tunnel can be created. Depending on the specific method and configuration settings, the data traveling inside the protected tunnel can be encrypted or not. Business requirements relating to confidentiality and privacy should drive the level to which encryption is deployed. For data requiring the highest levels of protection, both encryption techniques can be used. This would produce an encrypted tunnel with encrypted data traveling through it.

The concept of encrypting E-mail has some unique challenges. At different stages of its life, E-mail messages fall into both categories, data at rest and data in transit. The scenario that works best for both categories is to encrypt the E-mail envelope. That way the data is unreadable while being transmitted or when it is at rest sitting in an in-basket,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

on an E-mail server, or on the unknown number of servers on the paths between the sender and receiver. S/MIME is the most common E-mail encryption function that uses PKI. Most mature E-mail clients are already S/MIME enabled. The function to do S/MIME exists in the client. A user needs only to possess and have installed a PKI-enabled digital certificate to call the embedded S/MIME function. S/MIME implementations within most E-mail clients usually group a signing and an encryption function into one package. They are, however, separate functions and each one works as I have described above. When invoking S/MIME within a single E-mail the user can choose to sign, encrypt or combine the two functions.

Other electronic messaging services have been introduced to the market in recent years that offer secured delivery of messages, documents and files. Secure messaging services, such as Tumbleweed® Secure Messenger (IME) and ValiCert's SecureTransport™, integrate with existing E-mail for notification of intent to deliver a secured message. The messaging service lives on a secured web site typically SSL enabled. The message delivery is secured by requiring the intended recipient to visit the secured site for retrieval. Other PKI functionality sometimes available with these types of messaging services includes authentication and signing.

(Nonrepudiation)

According to Webopedia.com, the term nonrepudiation has the following meaning:

> In reference to digital security, nonrepudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.[4]

I concur that nonrepudiation can be engineered to encompass the bi-directional guarantees brought out in this definition. It is not uncommon, however, that the implementation design only supplies nonrepudiation for one party. The emphasis is usually on keeping the sender from denying he or she was the originator. In any case, nonrepudiation within PKI enables two interconnected functions, transaction integrity and data integrity.

Transaction integrity involves verifying the identity of the person who authorized a transaction and verifying the legitimacy of all components of that transaction. The PKI functions of signing and workflow verification come together to support transaction integrity and enable the signer to say and the receiver to verify, "I and no one else, authorized this transaction by my electronic signature." The workflow example in figure 2, above, can also be used to represent a sample of transaction integrity for a two transaction process. Transaction one is the actual travel reimbursement request.

[4] Jupitermedia Corporation. Webopedia.com. "nonrepudiation".

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Transaction two is represented by the signature from the approving manager. I will use transaction one to explain the concept of transaction integrity. When the requestor signs the signature field, the algorithm runs against his or her private key and the data values in the four required fields to produce a unique hash outcome.

The validation process is the vehicle that provides both transaction and data integrity. The transaction has integrity because the signature can be validated as being the digital signature of the requestor. The validation process can prove the certificate was not expired or revoked at the time of signing. Data integrity for this transaction is achieved through the same validation process. Any time the signature is validated, a reciprocal algorithm is applied against the signer's public key and the current values in all of the required fields. If the value in any one of the required fields changes the outcome of the hash values will no longer match. If the hash values do match, the process both verifies the signer's credentials and proves the values in the data fields have not changed since the signature was applied.

Issues to address

As stated earlier, there are a series of issues that an organization must address to do complete justice to the implementation of a security strategy that incorporates PKI. These can be grouped into several areas including technology, certificate architecture/policy, legal and people issues. One of the biggest lessons learned from five years of involvement with PKI technologies, is the significance of these issues and the value that internal and external partnerships offer in seeing the toughest to resolution. Organizations driven to resolve everything their way and on their own will face a much harder struggle. Many of the issues are larger than one organization. Independent solutions can be more detrimental to the effort at large.

(Technology)

PKI can be an invasive technology. Its applicability can be extended across many areas and can be incorporated within many security technologies. To get the most value, an organized approach needs to integrate well with existing infrastructure. Organizations must not, however, underestimate the visibility, hype and resistance that come as baggage with the technology. Years of hype and propaganda campaigns waged by real and would-be vendors have left many battle scars. Many business managers and IT professionals have sharpened their defenses against PKI based on overload from this hype. As a result, it can be a significant struggle to present valid arguments about the true benefits of the technology.

The approach an organization chooses to implement PKI-enabled technology can create its own problems. An integrated approach will bring greater benefits than any single solution effort. One of the largest benefits offered by PKI is as an enabler technology. Organizations looking to implement PKI as the primary solution to their problems have an uphill struggle, especially if they do not have a vision for how PKI integrates with their technology strategies. A long-term strategic vision will also help ease organizations

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

over that first PKI implementation hump. As the title and opening paragraph of this practical suggests, there is "no single killer application for PKI". From the perspective of a single application, much of the hype has validity. Implementation costs are high, infrastructure impacts are large and learning curves are significant. In this context, PKI is a hard sell. If all the organization gets for struggling through the gamut of PKI-related issues is a strong authentication method to a single application, the question of whether or not it was worth it would appear very valid. Many organizations unfortunately have a function-by-function, application-by-application or a business area-by-business area approach. Using this approach, they may never choose to undergo their first PKI implementation and therefore, never see the cumulative benefits of the second, third or fourth PKI-enabled business functions.

There may be two notable exceptions where PKI can make sense to enable a single function. It would be relatively easy to successfully argue the merits of SSL or TSL enabling a web server that houses applications with security requirements. With SSL and TSL the benefits are easily understood and the impact is relatively hidden outside of a few key network support staff. Assuming organizations make the right choice of vendor to provide their public SSL certificate, the PKI components are already available to most browsers. In addition, there are little to no customer impacts or learning curves. They go to the SSL-enabled website and the technology works. Another PKI-enabled technology that could possibly be implemented as a non-integrated effort is in the area of VPN connections. In some corporate strategies VPN connections are used for site-to-site secure batch transfer processes and to enable remote connectivity for IT support staff. With SSL/TSL and VPN, the footprint of impact is typically small as is the visibility of any issues outside of IT technical support staff.

An organization that takes an integrated approach to PKI will need to seriously address whether or not it should retrofit PKI into existing infrastructure. If it makes sense to replace an existing solution or to integrate a PKI-enabled technology into an existing solution, include in the decision process an assessment step for the appropriate timing. If an application is targeted for replacing its authentication mechanism with one that is enabled by PKI, it might make sense to coordinate the change with the next release of the application or, for example, when the application is being web-enabled.

In a systematic approach to sensible PKI-enabled security architecture, an organization should perform analyses in the following areas:

- A privacy/confidentiality assessment of the organization's data
- A profile of its applications' security requirements and clients
- The organization's strategic directions for security architecture
- Current access profiles into the network

After these assessments, the following business questions can be answered:

1. Does the organization have any data that requires a high level of protection? If the answer is yes:
   - Which of our applications house or manage any of that confidential data?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Who accesses them and how?

2. What are the business and legal requirements for securing or protecting this confidential data?
3. Where are the appropriate target areas and where does it make sense to incorporate a PKI-enabled solution?
   - Does the organization allow remote connectivity for its support staff?
   - Does the organization have web-enabled applications with sensitive or confidential data?
   - Does the organization have web applications and data that need to be protected against unauthorized access (modification or disclosure) from the Internet?

Once these questions have been answered, and once an organization makes the choice to include PKI-enabled technologies, especially personal digital certificates, they are ready to begin tackling the important PKI architecture and policy related issues.

Does it make sense to contract an external CA or provide CA services internally? The answer to this question goes hand-in-hand with this one, "Is the company totally independent, or does it have any external business partners with which it must collaborate?" Unless authentication and connectivity requirements are now, and forever will be, internal, an internal CA service will at some point become an albatross. If organizations do have or ever expect to have external trading partners, they should think seriously about contracting for external CA services. External certificate authorities have all but solved the issue of interoperability. Running a CA service well is a complex business utilizing elaborate equipment, sophisticated security protection and many formal policies and practices. If organizations expect business partners to trust their own internal certificates, those certificates must provide the same formality and level of assurance to which their business partners' certificates conform. The concept of home-grown does not typically carry that implication.

Making a decision to contract an external certificate authority does not yet answer all the questions. There are choices about which model fits an organization best. Does one use a simple model where the CA does the identity proofing, certificate issuance and certificate management? How about using a CA/RA (Registration Authority) model of which there are several varieties? An RA typically does the identity proofing and possibly some in-house certificate management like registering, revoking and sometimes hosting a copy of the certificate revocation list (CRL). If an organization is distributed across large geographic boundaries, there are models that support multiple RA functions. Again, the key to the right answers involves knowing how the organization relates to its business partners and what makes sense for all organizations involved. Do some of the business partners already have a CA model? If so, what does it look like? What kind and quality of PKI policies do they enforce? All of these issues are important considerations.

Either during or after the CA model is finalized, an organization will have to address the look and feel of the certificates it will employ. Does one certificate fit all uses across the organization? Is an assurance level important? Many implementations offer certificates choices with multiple levels of assurance. For example, Washington State offers three

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

assurance levels for their PKI-based digital certificates sold through its licensed certificate authority, Digital Signature Trust[SM]. Figure 5 details the certificate offerings from this CA.

Digital Signature Trust[SM] Washington State Certificate Authority Certificate Options		
Certificate level	**Characteristics**	**Implementation options**
High Assurance	• Online registration • Third-party verification of the applicant's identity • Face-to-face authentication notary public • Identity reliance limit $50,000 / transaction • Signing and Encryption key pairs	• USB token • Smart card • Software
Intermediate Assurance	• Online registration • Third-party verification of the applicant's identity • Identity reliance limit $10,000/transaction • Signing and Encryption key pairs	• USB token • Smart card • Software
Standard Assurance	• Online registration • Third-party verification of the applicant's identity • Identity reliance limit $1,000/transaction • Signing key pair only	• Browser-based
figure 5		

Many other certificate options exist. The Federal Bridge Certificate Authority, which was designed as a guide to facilitate CA interoperability between federal agencies and has a stated goal towards interoperability between other non-federal agency CAs, defines five assurance levels for certificates including a test, rudimentary, basic, medium, and high.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

What digital certificate choices make sense for any given organization should primarily be driven by the confidentiality and sensitivity level of the data being accessed, whether or not the data is being accessed from inside or outside the organization's physical networks and the risk or consequence of unauthorized disclosure.

Again, these choices become more crucial as an organization interfaces with external business partners, especially if they have contracted with a different external CA. The issue of cross-certification is not an easy one to solve. Many policies on how certificates are generated, protected, issued and managed must be mapped between an organization's CA and those of its partners. These sets of issues were the main drivers involved in creating the Federal Bridge Certificate Authority effort. When choosing the certificate model(s) and assurance level(s) that fit an organization best, a good principle to keep in mind is one of the highest common denominator. An application designed for authentication with standard or basic assurance certificates will almost always accept validated users who hold high-assurance certificates. The same is not true from the other direction.

(Certificate Architecture and Policy Issues)

This area of certificate architecture and policy will also be of significant importance to organizations that interface with external partners. It may not seem so important, how an organization generates and manages PKI components for its own internal uses. If, however, a business partner is interested in trusting the staff of an organization by accepting their PKI credentials it matters a great deal. Issues regarding how formal the Certificate Policy (CP) is, become very important. Exactly how formal a CA is at generating, distributing, accounting, recovering and administering the business' digital certificates, dictates what level of trust business partners can place in the use of those certificates. Of equal importance to business partners is the Certificate Practice Statement (CPS), the formal practices a CA uses to issue, suspend, revoke and renew certificates including how the organization provides access to them. In situations where time is critical, the practices and frequencies that drive when a CA updates its Certificate Revocation List (CRL) are also important. Consider an example in the medical world. A pharmacy is bound by law to honor prescriptions issue by licensed medical doctors. Let's say the pharmacy uses a web-based system that allows registered doctors from medical facilities to enter and electronically sign prescriptions for his or her patients. If a doctor was dismissed by the medical facility because of legal or policy issue, and the facility revokes the certificate they provided to that doctor, it would be important to that pharmacy and to the medical facility for the update to that CRL to happen as close to real-time as is feasible. How frequently this update happens is a component of the CPS. Not all CAs provide near real-time service. If this is a legitimate business requirement for an organization, knowing what the practice is becomes very important.

Trust is a two way street. The formality, with which the certificate architecture and policies are implemented within one organization, should matter as much to that organization as it does to its external trading partners. The reverse statement is also true.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The formality with which the certificate architecture and policies are implemented by an organization's external trading partners should matter a great deal to that organization.

The issue of cross-certification of certificates between two trading partners is no small matter. Some progress is beginning to be made at the federal level, but there are still many issues to tackle. The work of the Federal PKI Steering Committee (FPKISC) and the Federal PKI Policy Authority (FPKIPA) with two affiliated efforts, the Access Certificates for Electronic Services (ACES) and the US Federal Bridge Certification Authority (US FBCA), has provided quality groundwork in this area. Although the primary target of these efforts was interoperability between different CAs at the federal level, there is a stated commitment for considering cross-certification of non-federal CA models. Illinois and Washington are among the states that have already begun formal discussions or submitted proposals.

With wide acceptance of the X.509 and X.500 standards, most PKI technologies are interoperable. A lower assurance certificate signs and validates in the same way as the highest assurance certificate. A browser-based certificate works technically the same as a token-based certificate that incorporates biometrics in the place of a password. The biggest challenge in interoperability between organizations is in the policy area. Many ask, "Are all of the PKI practices and policies of my trading partners as detailed and formal as mine?" This is a very important issue to address as organizations begin to interface their PKI solutions with the outside world.

(Legal)

There are a growing number of laws addressing PKI. At the federal level in the U. S., enabling legislation came first from the Privacy Act of 1974 and its accompanying System of Records, as well as the Government Paperwork Elimination Act (GPEA), October 1998 and Electronic Signatures in Global and National Commerce (E-Sign) Act of 2000. These laws lead or aided such federal efforts as ACES and the FBCA. Several states enacted PKI or digital signature laws including Utah (1995), California (1995), Washington State (1996) and Florida (1996). According to Thomas J. Smedinghoff and Ruth Hill Bro in the Chicago Office of Baker & McKenzie, by the spring of 1999 "Forty-nine states, the U.S. Federal Government, and the governments of over 15 countries have enacted or are currently considering some form of electronic signature legislation."[5] A guidelines document for digital signatures was published by the American Bar Association in 1996. So what is the big issue here? The strength of any law is indicated by how well it stands up in the courts against legal challenges. To this date, precious few (if any) court cases to challenge any of these laws or the legal use of an electronic or digital signature has been filed or tried. My research in this area failed to turn up any.

[5] Smedinghoff, Thomas J. Ruth Hill Bro. Baker & McKenzie, Chicago Office. "MOVING WITH CHANGE: ELECTRONIC SIGNATURE LEGISLATION AS A VEHICLE FOR ADVANCING E-COMMERCE". The John Marshall Journal of Computer & Information Law. Vol. XVII, No. 3, Spring 1999 at 723

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(People)

The above issues are significant and should not be taken lightly. The biggest challenges to embracing PKI-enabled solutions, however, are people-oriented. Many IT professionals are against the technology for one reason or another. Years of PKI vendor wars and industry hype, have left them deeply entrenched in opposing camps. Many CIOs entangled with ever-shrinking IT budgets have to account closely for every dollar. Any amount of controversy can kill executive IT endorsement of any technology.

In many cases, the value of PKI as a security technology can be sold more easily than the cost and complexity to do the job right. With today's fiscal drivers, many businesses equate the best strategic business decision with the lowest cost. For most security technologies, the continuum of cost to security typically finds low cost and low security on one end of the scale with high cost and high security on the other. The key to a complete cost benefit analysis making the case for any security strategy that includes PKI is its scalability. The technology, infrastructure and learning curve costs of the initial implementation will be a hard sell on their own merit. Long term vision for strategic benefits after the second or third reuse of a technology is an intangible concept for some business executives unless the organization has an integrated vision from the beginning.

From the user community, there are different issues to address with PKI. The use of digital and electronic signatures involves a total paradigm shift for most people. From the time they learned how to write, they have been dealing with their own personal signature. They know what it looks like, know what it feels like and know how to use it. Methods of proving a signature belongs to an individual are tangible and have been in use for years. With digital certificates, the challenge is to give people software (in some cases may be a piece of hardware as well) and a pin, password or pass phrase. After they learn how to use the technology, they are told this has the same equal weight in the electronic world as their hand written signature does in the paper world. The problem is they can't see it, feel it and at first don't have very many uses for it. It looks and feels like a complex version of a user-ID and password. They are very familiar with that. Regardless of how much advice they have been given about good user-ID and password management practices, these are the credentials many of them have been abusing for years. They write them down, share them with others, and they choose passwords that are easy to remember (and guess). With digital certificates, organizations will have to deal seriously with this issue. The consequences of abuse are not only a business risk, they can also pose a legal risk.

Another people challenge is that of cultural acceptance. To the average individual, the technology behind digital signatures is invisible. How do they know all those technical things they heard are really happening to bind their "signature" with the data they are signing or the electronic signature they are applying? They don't have that paper to touch. Even if they print the document or electronic form off upon completion, at most they may see their name in the signature field. It will probably appear in block text and look nothing at all like their hand written signature. Now on top of all this new

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

technology organizations have imposed on their staff and trading partners, they are told they can be held legally liable for certain types of misuse. This is a big pill for them to swallow. Organizations must not dismiss this issue too easily and should be well prepared for this learning curve challenge.

Conclusions

(The real value of PKI)

All of the issues and challenges of PKI mentioned above are real. Organizations that embark on an IT security strategy that includes PKI as a component can expect to address all or most of them. The hypothesis that there are no killer applications for PKI is also true. With few exceptions, the nature of a PKI-enabled strategy carries with it complexities and significant costs and implementation challenges. Undertaking these issues and challenges to the extent it takes to correctly implement PKI-enabled security technologies is a hard sell for one application or business function. The real value in PKI lies in two very large areas:

1. PKI as an enabling technology
2. The scalability of PKI

Many of those who fought the vendor battles trying to raise PKI as the Holy Grail failed to achieve the right focus. The technology components of PKI are not it. The ability to enable the four major functions of encryption, authentication, signing and nonrepudiation should be. These functions combine in various ways to provide the many services available through PKI. The scalability of these PKI-enabled functions and services gives organizations with strategic vision the ability to use PKI to help deliver a broader scope of solutions than any other security technology. Let's look at some of the individual components within these two areas.

(PKI as an enabling technology)

Is PKI the great enabler of E-Commerce? Some resources say that E-Commerce is already flourishing, why do we need PKI? These same sources don't typically mention that most E-commerce sites are already PKI-enabled with SSL. Will other PKI-enabled resources emerge to assist E-Commence? I believe they will. For over a year, American Express blue card users have been able to use PKI-enabled authentication and encryption between the buyer and the credit card vendor to secure a one-time transaction number which in turn can be used to purchase goods online. Visa has recently announced a pilot using the same type of technology.

As explained above, PKI can be used to enable encryption techniques for data in motion or data at rest. Digital certificate technology can play a critical role in the creation of an SSL, TSL or VPN connection for enabling a protective tunnel for data during transit. That same technology can also allow the encryption of data at rest protecting it from unauthorized viewing.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Strong authentication can be supported by the same PKI technology. When enabled with digital certificates, especially hardware-based certificates, it falls in the category of two or three factor authentication. Something one has (the digital certificate) and something one knows (the password or passphrase). In high security environments, biometrics can be combined with the same PKI technology to introduce the third factor of something one is (a finger print, voice print, etc.). As long as an organization addresses the associated policy and contractual issues, the mechanics are available for extending that strong authentication to its external trading partners who require access to internal systems.

PKI combines its encryption and signature capabilities to enable the signing of objects such as documents, files, E-mails E-forms. Signing capabilities are already built into a growing number of vendor software products. For example, most full functional E-mail services are already enabled to do S/MIME, which provides for both signing and encryption. Some of today's electronic messaging systems combined to allow both SSL protection and PKI enabled authentication. E-forms development suites from several vendors can enable the use of most implementations of PKI-enabled digital signatures and nonrepudiation.

(The scalability of PKI)

It is the scalability of the technology that provides the most mileage for PKI. Benefits gained by PKI enabled functions can be leveraged across applications, environments, networks and organizations with an investment in one set of CA policies, practice statements and PKI support infrastructure. For example, the infrastructure built to enable PKI authentication for a single application can be duplicated with no additional costs. The cost per application of a personal digital certificate purchased by an individual is cut proportionally when the same certificate is used to authenticate that person for application number two, three and four.

The size and scope of PKI can grow easily as an enterprise grows. The same CA, CP, CPS and CRL mechanism that supported 100 clients can easily support 1,000 or more. The growth capacity for PKI can easily grow from a one-to-one implementation to an implementation that accommodates one-to-many. If built as part of a strategic vision, a single PKI structure can easily and economically grow as organizations add more applications, networks, operating systems, physical locations or external trading partners. PKI functionality is being enabled across a growing set of technologies. More and more vendor security solutions are enabling the use of PKI. In most cases, the well-planed PKI solution already in-house can be incorporated as the enabler of these technologies. SSL, VPN, directory services, Computer Operating Systems, E-mail/E-messaging and application development tool suites are some examples. Scalability also is a factor across the PKI functions themselves. The same PKI functions that enabled the simple signing and encrypting of a file or document is growing to include many flavors of authentication, authorization, credential verification, process validation and concepts such as single sign on.

(Closing observations)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

OK! So "There is no single killer application for PKI." If, an organization believes that, then I agree with them. If they use that premise as one of the driving business reasons for avoiding the technology, this is where we part company. I believe organizations that are dropping or avoiding PKI as a technology for this single reason have missed the point.

The use of PKI is optimized if done within an enterprise and strategic vision. Organizations struggling with the question of PKI for a single application or function face an uphill battle. In a cost benefit analysis of this approach, organizations may discover that cost and complexity do not bring enough return on investment to make it worth their while.

However, more and more vendors, including Microsoft in its Windows 2000, .Net and XP products, have incorporated functions that enable the use of PKI for authentication, encryption and other functions. As security and privacy concerns continue to grow with more and more state and federal regulations, the need for flexible but scalable IT security will also grow. More than any other security technology, PKI can provide this ability across one or more business enterprises.

If an organization has made a decision that includes PKI as an integral component in its strategic direction, a few suggestions will help pave the way. They must:

- Prepare to face some legitimate issues.
- Refuse to underestimate the size, complexity or seriousness of the issues related to technology, policy, legality and people
- Reject reliance on the technology alone to support business policies
- Back up business policy with a combination of technology as well as contractual and legal documents as the world waits for court cases and legal decisions to pass judgment on PKI as a security technology. This is important for in-house staff as it is for an organization's external trading partners.
- Keep a long-term strategic vision for IT security in focus
- Target the smaller applications with the highest degree of confidential or sensitive data for PKI implementation first.
- Form partnerships both internal and external. With PKI all of the struggles and issues are the same. For trading partners, the more each organization resolves these issues with comparable or compatible outcomes, the easier scalability across enterprises becomes.

Finally, the greatest merits of PKI are realized when it is viewed as an enabling technology and when the scalability of PKI are realized to their broadest extents. If an organization is waiting for the quintessential killer application for PKI, they cannot expect to see it anytime soon.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Washington State, PKI Early Adopters Program. Washington State, Department of Information Services. Washington State, Secretary of State. Washington State, Department of Health. Department of Labor and Industries. Department of Retirement Systems. Digital Signature Trust, Inc. Foundation for Health Care Quality. March 2000 – Dec 2000

Williams, Ian. Securing Your E-business.
"Is PKI the solution your business needs to secure its online activity?"
Business Communications Review International. March/April 2002. Vol 2 * No 2
Reprint available at URL http://www.bcrinternational.com/3_4epki.html

Rainbow Technologies. "Public Key Infrastructure - Securing the Future of Communication". White Paper. Rev: 1.1 10/27/00
Reprint available URL http://www.rainbow.com/library/8/PKI_Paper.pdf (4 August, 2002)

RSA Security Inc. 174 Middlesex Tumpike. Bedford, MA 01730. "RSA secure ID hardware and software authentication tokens".
hardware - http://www.rsasecurity.com/products/securid/hardware_token.html
software - http://www.rsasecurity.com/products/securid/software_token.html
(30 August, 2002)

Moulton, Bruce. Vice President - Infrastructure Risk Management. Fidelity Investments. "Expert Predictions for Security Trends In". SANS SECURITY ALERT. December 2000
URL http://www.sans.org/SANSSecAlert2_102000.pdf (19 July, 2002)

Ellison, Carl and Schneier, Bruce. "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure". Computer Security Journal. Volume XVI, Number 1, 2000
Reprinted at URL http://www.counterpane.com/pki-risks.html (15 June, 2002)

Armstrong, Illena. "PKI: Has It Truly Arrived Yet?". SC Magazine. August 2000.
Reprinted at URL: http://www.scmagazine.com/scmagazine/2000_08/cover/cover.html
(3 August, 2002)

Cooper, Daniel K.US General Services Administration. "ACES - Access Certificate for Electronic Services". http://gsa.gov/aces/privacy_act.htm (16 August, 2002)
"ACES – Who We Are". http://gsa.gov/aces/who_we_are.htm (16 August, 2002)

Loeb, Edward C. General Services Administration. "US Government Paperwork Elimination Act. Federal Register:" February 16, 1999 (Volume 64, Number 30). Notices. Page 7650-7651. Summary.
http://gsa.gov/aces/paperwork_reduction_act.htm (16 August, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Cooper, Daniel K.General Services Administration. "US Government Privacy Act of 1974; System of Records. Federal Register:" May 28, 1999 (Volume 64, Number 103). Notices. Page 29032-29034. Summary.
http://gsa.gov/aces/privacy_act.htm (16 August, 2002)

National Office for the Information Economy. © Commonwealth of Australia 2002. "online authentication, a guide for government managers".
http://www.noie.gov.au/publications/NOIE/online_authentication/onlineguidefinal.pdf (23 August, 2002)

Treuhaft, Jeff. Netscape Communications Corporation. "CS1: Overview of SSL 3.0". SSL History slide.
http://developer.netscape.com/misc/developer/conference/proceedings/cs2/sld004.html
Full presentation available at URL
http://developer.netscape.com/misc/developer/conference/proceedings/cs2/index.html (23 August, 2002)

DevEdge Online Documentation. Netscape Communications Corporation. "Introduction to Public-Key Cryptography"
http://developer.netscape.com/docs/manuals/security/pkin/index.htm (23 August, 2002)
"Introduction to SSL"
http://developer.netscape.com/docs/manuals/security/sslin/index.htm (23 August, 2002)

Patel, B. Intel; Aboba, B. Dixon, W. Microsoft. Zorn, G. Booth, S. Cisco Systems. Internet draft. Category: Standards Track. "Securing L2TP using IPsec". VPN Consortium. November 2001
http://www.ietf.org/rfc/rfc3193.txt (23 August, 2002)

Berinato, Scott. "Only Mostly Dead - RIP PKI. Why a security platform never took off". CSO online, Alarmed column. May 23, 2002
URL http://www.csoonline.com/alarmed/05232002.html (22 July, 2002)

Simon, Ed. Madsen, Paul. Adams, Carlisle. O'Reilly & Associates, Inc. O'Reilly "An Introduction to XML Digital Signatures". August 08, 2001
URL http://www.xml.com/pub/a/2001/08/08/xmldsig.html (23 August, 2002)

Ford, Warwick. National Institute of Standards and Technology (NIST) PKI Program. "Public-Key Infrastructure Standards". October 1996
URL http://csrc.nist.gov/pki/panel/warwick/sld001.htm (23 August, 2002)

National Institute of Standards and Technology (NIST). "X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)". Version 1.12. December 27, 2000.
URL http://csrc.nist.gov/pki/fbca/FBCA_CP_20001227.doc (23 August, 2002)

University of Michigan, project, Information Technology Division Distributed Directory Services project. "Introduction to slapd and slurpd". section 1.2 "What is LDAP?".

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

URL http://www.umich.edu/~dirsvcs/ldap/doc/guides/slapd/1.html#RTFToC1
(30 August, 2002)

Taylor, Paul. "Introducing LDAP". Windows NT Systems magazine. December 1998
URL http://www.ntsystems.com/db_area/archive/1998/9812/212fe3.shtml (30 August, 2002)

Microsoft Product Support Services. Microsoft Knowledge Base Article - Q196455. "Introduction to Lightweight Directory Access Protocol (LDAP)".
URL http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q196455&
(30 August, 2002)

Vlerken, Van. The Information Management Forum. Treasury Board Secretariat and National Archives of Canada. "Message Authentication, Integrity, and Non-repudiation from Paper to PKI". pg 2. 02/09/2002.
URL http://www.imforumgi.gc.ca/new_docs/authentic_e.doc (7 September, 2002)

Gonsalves, Royce. Information Technology Services, Monash University, Australia. Case "Study of Virtual Private Network (VPN) Implementation at Monash University".
URL: http://questnet.scu.edu.au/uploads/39.pdf (7 September, 2002)

Mitchell, Bradley. About, subsidiary of PRIMEDIA Inc., New York, New York. "Basic Network Design - The OSI Model".
URL http://compnetworking.about.com/library/weekly/aa052800a.htm (7 September, 2002)

Silverman, Mark L., CISSP. "Nuts and Bits of PKI. Center for Information Technology, National Institutes of Health". CENDI Symposium on PKI and Digital Signatures. June 13, 2001. Republished at
URL http://www.dtic.mil/cendi/presentations/silverman_pki_05-13-01.ppt

Tumbleweed Communications Corp, Redwood City, CA 94063. "Tumbleweed® Secure Messenger (IME)".
URL http://www.tumbleweed.com/en/products/solutions/extend_network/messenger.html
(7 September, 2002)

Valicert, Inc., Mountain View, Calif. "ValiCert SecureTransport™, Secure Document and Data Delivery over the Internet".
URL http://www.valicert.com/products/secure_transport.html (7 September, 2002)

Jupitermedia Corporation. Webopedia.com. "nonrepudiation".
URL http://www.webopedia.com/TERM/n/nonrepudiation.html (7 September, 2002)

Angel, Jonathan. "PKI and the Law". Network Magazine. October 2000.
reprinted at
URL http://www.networkmagazine.com/article/NMG20001004S0010/2

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(7 September, 2002)

Clark, Elizabeth. Special Report: "Unlocking PKI". Network Magazine. October 2000. reprinted at URL http://www.networkmagazine.com/article/NMG20001003S0003 (7 September, 2002)

Digital Signature Trust. State of Washington, "Types of Certificates" http://www.digsigtrust.com/state/wa/swa-offerings-main.html (15 September, 2002)

Edfors, Patricia N. Former Chair, Federal PKI Steering Committee. James J. Flycik. CIO Council, Federal PKI Steering Committee. "Charter Statement". URL http://www.cio.gov/fpkisc/charter.htm (30 August, 2002). [no longer available] Full charter available at Federal Public Key Infrastructure Steering Committee. Federal PKI Policy Authority, "Charter For Operations". URL http://www.firstgov.gov/fgsearch/resultstrack.jsp?sid=15504220&url=http://www.cio.gov/fpkipa/documents/fpkipa_charter.pdf (29 September, 2002)

Kahn, Rebecca. Marsh, Georgia K. Federal PKI Steering Committee. Meeting February 06, 2001. Minutes February 22, 2001. URL http://www.cio.gov/fpkisc/state/2-6-01.htm [no longer available] (30 August, 2002)

Internet2 website. Certificate Policies. http://middleware.internet2.edu/certpolicies/ (15 September, 2002)

Security Group of the Politecnico di Torino. The EuroPKI Top Level Certification Authority. http://www.europki.org/pki/en_index.html (15 September, 2002)

Smedinghoff, Thomas J. Ruth Hill Bro. Baker & McKenzie, Chicago Office. "MOVING WITH CHANGE: ELECTRONIC SIGNATURE LEGISLATION AS A VEHICLE FOR ADVANCING E-COMMERCE". The John Marshall Journal of Computer & Information Law. Vol. XVII, No. 3, Spring 1999 at 723
Reprint available at URL http://www.bmck.com/moveart.doc (15 September, 2002)

Scheier, Robert. "PKI complexities, cost hold promising technology back". Security Tips & Newsletters. 18 September, 2001.
URL http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci770681,00.html (30 August, 2002)

Schlumberger Information Solutions, Houston, Texas. "Worldwide Corporate Directory Connects People to People for Communication and Collaboration". © 2002 Schlumberger Information Solutions. April 2002
URL http://www.sis.slb.com/media/services/info_mgmnt/ldap_cs.pdf (15 September, 2002)

Kahn Consulting, Inc. ("KCI"), 157 Leonard Wood North, Highland Park, Illinois 60035. "Implementing Electronic Signatures: Technical, business and legal considerations". URL http://www.kahnconsultinginc.com/library/KCI%20Whitepaper-PE%20Implementing%20E-Signatures.pdf (15 September, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced