GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

What happened to PKI?
Chandler Davis
January 5, 2003
Version 1.4b

Abstract

Many information security analysts in the mid to late 1990's agreed that Public Key Infrastructure (PKI) was an investment that many companies were going to need to consider if they plan on doing business across the Internet. PKI was suppose to be an integral part of most companies information security infrastructure. It was also suppose to be simple to use and almost seamless to the end user. So now it's 2003 and why are so many security analysts hanging their heads when someone mentions the company's PKI effort?

The infrastructure piece of Public Key technology requires many different components in order to provide authentication and authorization services that PKI offers. Implementing these components is a complex assignment that has turned out to require an extensive amount of time and money. It is hard for many companies to calculate the return on investment for PKI, which will continue to make it hard to get funding and support year after year. With the recent economic downturn, many companies have decided to drastically cut back the funding for PKI, if not discontinue it altogether.

Why PKI???

In the 1990's there was an explosion of dot-com companies. Many investors were looking toward the Internet as the next big break-through market. It was believed that the Internet and dot-com companies were going to be the cash cow that many investors could make millions on. This lead to an explosion in the information technology area, not only in the number of dot-com companies, but also with a number of new technologies that were being experimented with.

PKI was one of the technologies that many Fortune 100 companies were a little hesitant on using. Information security consultants and vendors were telling companies to rely on a relatively young security infrastructure that had not been widely developed, but was suppose to allow companies to safely expose their network and data to millions of home users and rival companies on the Internet. The fear of exposing the companies network to the Internet, kept companies relying heavily on private phone lines to connect them to their business partners and suppliers, while limiting the functionality of their website. Many of Fortune's top 100 did use the Internet to provide some information about the company and/or their products, but in most cases the companies were not willing to sell their products online. The inability of the traditional brick and mortar companies to be able to provide products and services across the Internet allowed smaller virtual companies to infringe on some traditional businesses. Some of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the newly founded dot-com companies did not put the same importance on information security as compared to traditional companies that already had name recognition. This allowed many of the startup dot-com companies to quickly create computer systems that give customers the ability to purchase products and services online, but in some cases it allowed personal information such as credit card data to be disclosed to unauthorized individuals. Larger traditional companies were slower to react to needs of Internet customers because most computer systems were intentionally built to not allow access to data when the requesting individual was outside of the physical building.

Traditional companies did see the advantages of the Internet as a possible way to reduce the cost of doing business, but the lure of the Internet was not as enticing, due to the fear of becoming the featured story on the nightly news. If it were revealed that a large traditional company had its computers compromised because it was accessible to the Internet, the consumer confidence in that company could have devastating consequences.

During the 1990's when companies began selling products online, many consumers were fearful of the Internet. This fear came from dealing with the unknown. Purchasing merchandise online exposed consumers to a new form of communication (electronic-business or E-business) that does not require any type of human interaction. Many consumers had come to rely on some type of human interaction (whether it was in person or over the phone) in order to achieve a trustworthy feeling during the transaction. For instance, when a consumer purchases an item at a store, they physically pick up the merchandise they want to buy and paid for it with a credit card. The credit card company acts as a trusted third party that promised to pay for the merchandise purchased by the customer. In this case both the consumer and the seller are happy to do business since the customer walks away with the merchandise and the seller has received a promise from the credit card company to pay for the merchandise. When a consumer purchases an item over the phone or through the mail, the fear of making the purchase is higher than making a purchase at a physical store, but in many cases, not to the point that the purchase will not happen. In this case, many consumers rely on the ***source*** of the advertisement instead of the advertisement itself. Items being advertised on a local radio or television station, or in a well known publication such as "PEOPLE" magazine, may help increase the comfortable level of consumers. This is because the consumer may feel they can trust the ***source*** (a radio station, TV station, or national magazine) would have already done some research on the companies and products they are advertising. On the other hand, merchandise purchased over the Internet requires consumers to use the relatively new E-business form of communication that does not allow for any type of human interaction. This is not the only reason consumers experience fear when shopping over the Internet. According to Alex van Someren, chief executive at security specialist nCipher, one of the most common concerns about shopping online is, "The perception is that some 14 year-old on the other side of the world has crocodile clips attached to the Internet wires, and is stealing your credit card number."**(1)** With the perception and fears of the Internet growing as the year 2000 approached, many consumers remained hesitant about shopping online until they felt that websites have taken the necessary steps to protect

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

them during the transaction.

As many companies began finding out, trying to create a foothold on the Internet was proving to be somewhat more challenging than they had anticipated. Companies large and small had the same fears as many consumers did about doing business over the Internet. Important security questions like the following, still needed to be answered.

1. How do you keep someone else from ease dropping on a communication?
2. How do you tell if someone had tampered with the data they have received?
3. How do you validate a person identity online?
4. How do you get a physical signature on the electronic data?

During the Internet boom, some companies spent time and money to research and development, new ways of securing online transactions. Vendors such as Baltimore Technologies, were telling companies that they needed PKI in order to accomplish a wide variety of online transactions. "PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

1. **Confidentiality** - to keep information private
2. **Integrity** - to prove that information has not been manipulated
3. **Authentication** - to prove the identity of an individual or application
4. **Non-repudiation** - to ensure that information cannot be disowned"**(2)**

While not many of the dot-com companies decided to embark on the challenges of PKI, some did. Many of the smaller companies decided not to create their own PKI, but to purchase only as many certificates that they needed from PKI certificate vendors such as VeriSign. The price per certificate is high compared to those issued by someone owning their own CA, but the infrastructure cost associated with buying certificates is almost nothing since that is the responsibility of the certificate vendor. Certificate are good for a certain amount of time before they expire, at that time the owner of the certificate can choose whether or not to pay for a renew. While on the other hand, some companies on Fortune's top 100 decided to create their own PKI. Companies like Entrust and Baltimore Technologies provide a key piece of software that is needed for companies to create and manage their own PKI solution. In order for PKI companies to continue receiving revenue, the software requires a license code in order to create certificates. Just like VeriSign, these companies would also charge for each certificate and the price per certificate would be even lower depending on the number of certificates that were purchased. The more certificates you buy the lower the cost per certificate. Many times this price negotiation would take place before a company had it's PKI in place and working. Although creating a PKI is very costly in the short run, it was believed that within a few years the company would begin to save large amounts of money, compared to buying their certificates from a PKI certificate vendor.

Year after year, it was always going to be the year for PKI to break out and capitalize on it's much awaited success. In 1997, PKI was called the "silver bullet" and a "guarantee" for secure online transactions or the "high-tech bug spray" to stop "viral warfare". When that didn't materialize, in 1999 PKI was being pitched as the safest way to conduct

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

online business. Of course that wasn't PKI's year either, so in 2000 it was going to be great for the wireless market. (3)

It was also hoped that when President Clinton signed the digital signature act into law on October 1, 2000, it would help boost the economy by making goods and services more available through E-business as well as breathe new life in PKI. The law was to provide a uniformed standard for doing business across state lines so companies would not have to follow multiple electronic signature laws. It was also hoped that with a uniformed standard it might make some of the technologies seem the same, which would make it easier for the consumer to understand what is happening. If the consumer had a better understanding of what was happening, perhaps the fear of doing business online would subside.

The year 2000 also brought the beginning of the end for the economic boom in dot-com companies as well as the stock market. Dot-com after dot-com began to fail and fewer and fewer dot-com's were being created, while others began to see their funding start to dry up. Larger companies started to notice the economic downturn and began cutting back on development and testing of projects that had not shown signs of financial benefit to the company. With no killer applications waiting for PKI and most companies stuck in the pilot stage, PKI turned out to be one of the projects that began to see it's funding reduced or cut all together. In many cases the mention of PKI left executives wondering what happened to this promising technology and most importantly, "Where did all the money go?"

Where did all the money go?

As with any new technology, people with experience are at a premium. Many of the large companies that decided to purchase the software and the tens of thousands of certificate licenses wanted to take advantage of the purchase as soon as possible. One of the first problems that companies ran into was the lack of people that were extremely familiar with the technology. While some companies decided invest more money into PKI by hiring consultants to help develop their PKI direction, other companies decided to develop PKI skills in their own employees. The education process needed to train employees has proven to be expensive, as well as time consuming. Many of the PKI vendors had training classes available that taught students how to install and operate the vendor's software. Companies supplying directory software had their own training classes. One of the best sources of learning about PKI came from the many PKI conferences that were available. Although many conferences required time and a considerable amount of money, in most cases is was a great place to learn about the successes and pitfalls experienced by many different companies. They also allowed employees and consultants to get together and discuss their specific concerns.

The cost of physically building a Public Key Infrastructure can be somewhat overwhelming. A large amount of equipment and software is needed in order to create a production PKI that can be rolled out company wide. Some of the major investments

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

in equipment include the following:

- the Certificate Authority software and the server to run it on
- the directory software and a server to run it on
- a server for the RA and maybe software (the RA could be developed in-house or package solution can be purchased)
- firewall software and server(s)
- additional network equipment
- maybe even a web server depending on the design

Multiples of the above equipment may also need to be purchased depending on the company's philosophy. All of the above equipment needs to be sized in order to provide the desired performance according to the amount of traffic that is anticipated. The cost of availability may mean that many of these servers will need a fail-over or load sharing server in addition to more networking equipment and availability software. The company philosophy may also dictate that multiple environments need to be created. Such as a development environment that is separate from the production environment. It would allow PKI application developers a place to experiment with different code without being held to the same standards as the production environment. A testing environment may also need to be created. This environment would be setup very close to the specifications as the production environment and would allow developers to test their application in a production "like" environment to make sure it will perform as expected once it is put into production. Each environment will require almost the same amount of equipment as the production environment and would double or triple the cost of using PKI.

Once all the servers and network equipment has been identified and purchased, another major investment in PKI is the physical location of the equipment. This location will need to have many of the same features of normal data centers including; temperature control, humidity control, security controls, fire/smoke controls, and redundant power supplies. Unlike many data centers, the security controls needed for the location that will house the Certificate Authority (CA) should be stricter than normal. Frequently a specially designed room would house at least the CA, if not most of the PKI equipment. This room would be located inside an existing data center. The physical security system would require multiple authorized individual be authenticated at the same time before allowing the door to open into the CA room. A common approach to authenticating to the physical security system would require at least one of the individuals to use a biometric device. In many cases closed circuit television cameras normally monitor the doors leading into the data center as well as the doors leading into the CA room. In some cases cameras are also placed inside the CA room in order to preserve a video record of the events that occurred. These video records would show who is interacting with what piece of equipment and when, but not necessarily in such detail that someone could tell what information was being displayed on the monitor or what keystrokes were made.

The creation of a PKI does not only take time and money from the IT department. It also takes a considerable amount of time from the company's law department. A

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

company issuing PKI certificates wants some kind of legal understanding between the company and the entities that received the certificate. A Certificate Policy (CP) is a document that tells the legal liability that the issuing company is willing to accept as well as the intent of the PKI certificates that are issued. In many cases the company's lawyers supervise the construction and content of this document. An accompanying document called the Certificate Practice Statement (CPS) tells how the policies are being interpreted and how they will be implemented. Entrust created a white paper dated February of 1997 that talks about what should be covered in Certificate Policies and Certificate Practice Statements and how they interact with one another.

Perhaps the most significant cost for many companies is the expense associated with the amount of time it takes to get a basic PKI up and running. Creating the infrastructure piece of PKI requires many different pieces of equipment working together seamlessly in order to provide a service. This infrastructure will require the skills of many different individuals. Systems designers, operating systems specialists, network specialists, directory specialists, hardware specialists, and security specialists, just to name a few, will all need to work together for a considerable amount of time in order to provide a basic PKI when they are finished.

So what takes so long?

Once a company had made the decision to implement PKI, one of the next questions becomes, "How long will it take?" The main components include the Certificate Authority, a Directory, and the Registration Authority. Each of these three components performs a specific job.

There is not a lot of customizing available for the Certificate Authority (CA). For example, when installing the Entrust Certificate Authority software, the installer is asked less than twenty-five questions. Many of the companies that create CA software work closely with directory software companies to help make the integration of the CA and the directory as painless as possible. Installing the directory software is almost as simple with the exception of how the directory information tree might look.

On the other hand, the Registration Authority (RA) can be one of the most confusing components to implement. Since the CA may have a copy of all the keys it issues (including it's own) it is considered the crown jewels of PKI. It is critical to maintain a high level of security around the CA to ensure that PKI is not compromised. In order to maintain a high level of security, in many implementations no PKI users are allowed to directly communicate with CA. Instead, a limited number of devices are allowed to communicate to the CA on the user's behalf. One such device is the RA. One of the jobs of the RA is to communicate the needs or wants of PKI users back to the CA in a secure manner. Another function of the RA, is to authenticate each user that wants to interact with the CA. It is this authentication process that determines the level of trust that can be placed in the certificates that are issued by the CA.(2) Creating a customized RA that requests and provides information in a way that is suitable to the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

company, can be a very time consuming process. Part of the reason is because of the number of questions that are raised during its design. Questions like:

- How are you going to authenticate the person identity before a certificate is issued to the person?
- Will the CA issue graduated certificates? Some operations may require different level of authentication, say for instance, someone wanting to get a quote for a life insurance policy may not need the same level of authentication as someone wanting to purchasing a life insurance policy.
- What actions will users be able to do with the Registration Authority? Such as reset their certificate pass phrase, expire their certificates, change their share secrets, or request a new set of keys.
- How will the Registration Authority interact with the user? Will it supply all the needed information to the requester in real time, will it e-mail some of the information to the requester, or will it send some of the information to another authorizing authority to act as a final check of the person identify?

Many of these questions can be easily answered if there is a specific business case or purpose for PKI. A specific business case helps in overall design of a company's PKI and helps deduce the guesswork of analysts trying to predict the future uses for PKI. Guesswork, uncertainty**,** and confusion all lead to a longer time line for during implementation. Longer time lines and unclear direction begin to create doubt in everyone's mind if PKI is worth the continued financial support. Without seeing any short-term financial benefits to PKI, some companies have decided that PKI is not a good fit within their company while.

Who claims PKI is/has failed?

According to an article entitled "IBM Backing Away From PKI Software" written by Dennis Fisher of eWEEK, IBM will slowly remove it's self as a supplier of PKI software. IBM is starting to back away from PKI by cutting back on promoting their PKI software called Tivoli SecureWay. Although the company continues to make the product available, it is believed that IBM has no further plans to develop the software. Instead, IBM will start urging current customers to consider using VeriSign as their PKI supplier. In mid January of this year IBM announced a partnership with VeriSign where the two companies will work together to develop a set of services based on VeriSign's PKI. IBM is repositioning its self to promote PKI services, much like Entrust and Baltimore Technologies plc., have already done. Fisher points out, "Vendor are finally listening to customer complaints that there are few applications and services designed for use with PKI, something that has hampered deployment and use of the technology."**(4)**

The Royal Mail in the UK announced that it will shutdown its digital certificates business called ViaCode. On August 31, 2002, ViaCode PKI ceased operation and revoked all of the digital certificates it had issued. The demand for digital certificates placed the company in an "… unsustainable financial position caused by the slow development of the market …". **(5)** This has caused problems for the National Health Service that used

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Digital Certificates to electronically transmit pathology results within the NHS. Electronic Data Systems Corp (EDS) is trying to take over where ViaCode left off, with the help of Entrust. The EDS system was suppose to being running August 19, but due to the complexity of changing from one PKI to another have delayed the startup for over a month.

During the RSA Conference 2002 held in Paris from October 7 - 10, it was discussed why PKI is failing. Two major factors limiting the deployment of PKI are cost and complexity. The chief technology officer for Microsoft, Craig Mundie, mentioned that if cost or complexity is too high users shy away from the technology. Whitfield Diffie, chief security officer of Sun Microsystems promises that the use of PKI will expand, but slowly. He noted that the value of PKI is more apparent when everyone else is using it. "When only a few people have it, it is not worth adopting"[(6)]

Conclusion

PKI's history and possibly it's future could be compared with the history of heart transplant surgery. Learning heart transplant surgery and learning how to create a PKI are both time consuming and expensive. Many trials and pilots were used to prove that the concept was sound. The history of heart surgery and PKI are much the same, not all attempts resulted in favorable results, although something was learned during each attempt. There is a great deal of fear involved with both, whether it is a person receiving a heart transplant, or customer trusting a security mechanism that they don't understand, they both can create anxiety. An individual doesn't need to be able to understand transplant surgery or PKI, all they need to know is it works with a great deal of success. A very low success rate for PKI, coupled with the fact that PKI is very expensive and complex, have lead many companies to shutdown their PKI operations.

Does this mean that it is time for Doctor Kevorkian to help step-in and finish off PKI? No. PKI has had its successes. But in order for PKI to become all that was promised in the late 1990's and early 2000, implementer and software designers will need to find ways to reduce the cost and complexity of PKI. In turn it is hoped that companies and investors will return.

1 - Nash, Emma. "E-business players fight the fear factor." 31 October 2002. URL: http://www.vnunet.com/Features/1136435 (5 Jan 2003).

2 - Baltimore Technologies. Executive Briefing, "An Introduction to PKI based e|security." 2000. p. 6. URL: http://download.baltimore.com/download/pdf/BaltimoreGuideToPKI.pdf (5 Jan 2003).

3 - Berinato, Scott. "Only Mostly Dead." 23 May 2002. URL: http://www2.cio.com/research/security/edit/a05232002.html (5 Jan 2003).

4 - Fisher, Dennis. "IBM Backing Away From Software." 28 January 2002. URL:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://www.eweek.com/print_article/0,3668,a=21765,00.asp (5 Jan 2003).

5 - ViaCode, URL: http://www.consignia-online.com/portal/default/all/home?paf_gear_id=100002&paf_gm=content&paf_dm=full&paf_gear_state=con_content&xmlPath=/docContent/xml/generalContent/viacode/viacode.xml (5 Jan 2003).

6 - Judge, Peter "Sun, Microsoft: PKI is failing." 9 October 2002. URL: http://xdnet.com.com/2100-1105-961350.html (5 Jan 2003).

Additional resources contributing to this paper include:

Richards, Asha. "E-Sign and State Electronic Signature Laws: What Comes Home in The Sea of Legislation?" 16 April 2001. URL: http://www.tilj.com/content/ecomarticle04140101.htm (5 Jan 2003).

Boeyen, Sharon. Entrust White Paper, "Certificate Policies and Certificate Practice Statements". February 1997. URL: http://www.entrust.com/resources/pdf/cps.pdf (5 Jan 2003).

Leyden, John. "NHS PKI project in sick bay." 9 September 2002. URL: http://www.theregister.co.uk/content/archive/27196.html (5 Jan 2003).

Leyden, John. "Royal Mail pulls plug on ViaCode digital certificate." 29 May 2002. URL: http://www.theregister.co.uk/content/archive/25496.html (5 Jan 2003).

Chen, Anne. "Prescription for PKI Success." 5 November 2001. URL: http://www.eweek.com/article2/0,3959,47940,00.asp (5 Jan 2003).

Scheier, Robert. "PKI complexities, cost hold promising technology back." 18 September 2001. URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci770681,00.html (5 Jan 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: April 30th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS