Building a Successful PKI

By Arshad Noor

Contrary to what you might have heard, or read in the Information Technology (IT) press, companies have built **Public Key Infrastructures (PKI)** successfully, and use them daily to solve day-to-day business problems. What is little known, however, is the magic potion used by these companies to make their PKIs successful. This article will attempt to demystify some of that magic.

Public Key Infrastructures are the term given to the aggregation of policies, procedures, and technology to manage **Digital Certificates**. These are the visible part of credentials issued by the PKI to manage **Access Control**, which in turn, are the rules defining how a resource within a computing infrastructure may be accessed, and once accessed, what can be done with it.

Invented more than two decades ago, and commercialized over ten years ago, there is no denying the business benefits of public-key cryptography—the technology underlying PKIs. **Encryption** for confidentiality, **Digital Signatures** for authentication and message integrity, and, when combined with external cryptographic tokens and strong business processes, **non-repudiation** of transactions.

With these kinds of benefits, many technology leaders jumped into PKI—and almost drowned! With some exceptions, many PKIs failed to meet expectations, or are currently on life-support—waiting for something that will pull the plug on them. A report[1] by the US GAO indicates little progress on PKIs amongst major US Federal agencies, even after spending US $1 Billion over the last three years.

There is no single reason attributed to their failure; more a collection of reasons—the high cost of deployment, complexity of the technology, poor understanding of operational and business requirements, excessive focus on technology rather than applicability, and others—all contributing to the failure rate.

However, between the birth of this technology and its presumed death, some companies have deployed PKIs successfully, and continue to use them to solve their business problems. You won't read about them in the press—since it is a security technology, most companies don't want to tout their defensive counter-measures as an invitation for attacks. Secondly, the press is not in the habit of writing about corpses, so there is little incentive to sell the merits of a technology proclaimed dead many years ago.

Having been involved in PKI deployments for the last five years—some successful, and some not—we believe we understand the reasons why some PKI projects are successful while others flounder. We hope these lessons will be of benefit to you.

Lesson 1: Define your objectives realistically

When sold a PKI, you are provided a vision of the fully-integrated, PKI-enabled IT infrastructure. However, what you're not told is that the PKI is just a foundation, and that applications are incapable of using it unless they're designed to do so. Between the deployment of the PKI and the first application that can use it, a lot must happen:

- Certificate life-cycle procedures must be created;
- Business processes must be created or modified to support the certificate life-cycle;
- One or more applications must be created or modified to use certificates;
- An Operations and Support infrastructure must be created or modified, to deal with new requirements;
- Users of PKI credentials must be trained to use them effectively;

Most deployments under-estimate the scope of activity that precedes a "production-ready" PKI. The deployers get overwhelmed by the workload, while the consequences are delays, and cost-overruns for unplanned, or inadequately budgeted activities.

What can you do about it?

Recognize that a fully-integrated, PKI-enabled IT infrastructure is a multi-stage effort, and set your expectations accordingly. The duration to accomplish the task will depend on the size of your deployment and the scope of integration desired for your existing environment. However, by defining clear boundaries for each stage, you can improve the probability of success significantly.

Stage 1

In the first phase of this effort, focus on building a PKI pilot that takes no more than one person-month of effort, and no more than US $25,000 for hardware, software and services. It is possible, within this time and amount, to evaluate a PKI that represents an enterprise PKI scale model, with a **Certification Authority (CA), Registration Authority (RA), Validation Authority (VA), Publishing Directory (PD) and Enrollment Directory (ED)** including FIPS-certified external cryptographic tokens. If it takes more time or money than this, you're already in trouble.

Within such a pilot, evaluate all the business benefits that PKIs deliver—strong authentication, message integrity, confidentiality and non-repudiation. Use this scale model to understand the PKI—architecture, technical capabilities, operational and support requirements, impact on business process and applications, etc.

Stage 2

When you've been funded to build an enterprise PKI, commit to accomplishing only the following in Stage 2:

- Architecting and designing the enterprise PKI;

- Acquiring the hardware, software and services to deploy the PKI;
- Creating detailed certificate life-cycle processes;
- Creating and training the PKI Operations and Support infrastructure;
- Creating end-user training modules; and
- Creating the core business processes that support the certificate life-cycle;

This stage should **specifically not include** the enterprise-wide roll-out of certificates or PKI-enabling applications. The risks increase dramatically with such dependencies, at this stage.

Stage 3

In the third stage of the PKI project, perform a limited deployment, starting with the IT department, "power" users and potential RA Agents in business departments. Turn on **Secure Multipurpose Internet Mail Extensions (S/MIME)** and **Client Secure Socket Layer (SSL)** authentication to a test intranet site for these initial users. Besides getting them familiar with the technology, it will facilitate application developers and business users thinking about certificate-enabling their applications, business processes and systems.

Stage 4

In this final stage of deployment, issue certificates based on priorities established by the business. By now, the PKI will have worked out its rough edges, and will provide a smoother experience to users.

Lesson 2: Use the right technology

While there are industry standards around digital certificates, there are also differences in how vendors support them, and the capabilities they offer to make your PKI easier to use and operate. Unfortunately, the wrong product can add hundreds of thousands of dollars in costs and many months of additional effort to deliver the PKI.

Vendors generally focus on ensuring correct execution of the PKI-enabling software, with operations and support for business processes being of secondary concern. However, some vendors are better than others in this regard. Some of the more important differences we've seen amongst products are, how they handle:

- **Preauthorized issuance of digital certificates.** Some have out-of-the-box support, while others expect you to write your own modules to enable this. This feature can add 3-6 person-months to the project, and additionally, impact the cost of operations;
- **Ease of use in the Issuance part of the certificate life-cycle.** Some allow you to enable users to perform many business-related operations easily, while others bog you down with cumbersome detail irrelevant to the business process;
- **Support for Disaster Recovery and High Availability.** Some have this capability out-of-the-box so that, when configured, fail-over is automatic. Others require you to execute many manual steps, thereby severely impacting availability and the cost of operations;
- **Cost of deployment.** Some vendors sell the software modules piecemeal and charge a per-seat licensing fee per certificate. One gives you the PKI software for "free" in its server operating system, but charges a higher price per seat for the OS, than what it might cost to build equivalent capability on an alternative OS with reasonably-priced components. A third charges you a flat, per-seat fee and gives you all modules in the software at no additional charge.

Choosing the right product can determine the success or failure of your PKI. Unfortunately, the trick is knowing the right selection. Using industry analysts is not very helpful in this case, since industry analysts do not build and operate PKIs, and therefore, have no real-world experience on what makes a successful PKI.

What can you do about it?

Unless you take the advice of someone who has built real-world PKIs successfully, the only way to mitigate this risk is to evaluate at least 3 contenders yourself, and make the decision based on your experience. While giving you first-hand knowledge, it will take at least 4-6 months for a high priority project, 9-12 months otherwise. Additionally, the evaluation team must include an Application Architect and a senior Systems Administrator to evaluate the application integration and operations issues respectively.

Lesson 3: Know the technology

A major reason PKIs fail is, people responsible for deploying them have an incomplete understanding of the implications. It isn't enough to understand the mechanics of public-key cryptography or the minutiae of certificate extensions. The person responsible for PKI deployment must have sufficient knowledge about network routing, DNS capabilities, packet-filtering firewalls, cryptographic tokens, web technologies and architectures, the mechanics of Client Secure Socket Layer (SSL) authentication, etc. Part-time team members from these areas only have a little understanding of PKI, and cannot volunteer information that would optimize the PKI in the IT infrastructure.

As a result, the architecture typically deployed is needlessly complex; too many machines are purchased, too many firewalls are established, improper fail-over strategies are implemented, processes are designed with latencies built-in, etc. Again, the complexity leads to delays and cost overruns, putting the project on shaky ground.

What can you do about it?

The more knowledgeable and experienced the PKI deployment manager is in operations and applications development, the greater the probability of success. Why? PKIs are demanding in their operations requirements. Availability, recoverability, security and performance requirements for PKIs are higher than for standard transaction-oriented applications. People with strong operations experience have a focus that optimizes operational activities without compromising the other demands of the PKI. The background in applications development is essential to understand how developers will build applications to use the PKI. If the PKI deployer misses on simplifying either of these goals, the PKI is sure to fail.

Lesson 4: Define your architecture before deployment

Most technology projects have some flexibility to maneuver around errors or missed requirements. A database schema can be modified to include a new column without impacting existing application code. New software libraries, with additional capability, can be deployed without affecting existing applications.

While PKIs are flexible, there are certain qualities that make them difficult to change once deployed. For example, the algorithm and key-sizes used to create the CA's signing keys are fixed. Once the CA starts issuing certificates, recreating keys due to changes in requirements will invalidate all certificates issued upto that point, unless a more complex activity is pursued—key-rollover.

Once certificates have been issued with specific extensions in them, adding, deleting or modifying certificate policies and extensions impacts all new certificates. If any previously configured policies and extensions are incompatible with current business requirements, then all previously issued certificates need to be reissued.

PKIs implemented without Online Certificate Status Protocol (OCSP) Responders, automated Disaster Recovery or High-Availability have a major impact on the physical, network & firewall environment, and on operational & support processes if deployed after going live. Even the choice of hardware, the operating system used to deploy the PKI can be a factor in their success.

What can you do about it?

Once you know you're building a PKI, don't order any hardware or software until you've created a detailed blue-print of every major facet of the PKI. Consider alternative architectures and debate the merits/demerits of each, until you're satisfied you have the optimal architecture. This can take a month or two, but is time well spent. Every minute spent defining detailed architecture up-front, will save days, if not weeks, over how things should be retrofitted into a partially-built PKI.

More often IT management may make the wrong decision in a difficult situation, to give the impression of a project under control rather than accept the delays to fix the problems. Or they will throw more money at it, in the hope that it will solve the problem. Unfortunately, these decisions usually exacerbate the problem, leading to a meltdown of the project at a future date.

Lesson 5: Pay attention to business and support processes

PKIs are technical and complex beasts. Much of it is new to most people on the deployment team, and consequently, the team is usually busy figuring out the technology, or working the implementation details. This, inadvertently, leads to little attention being paid to business and support processes—critical elements of a PKI's success.

The certificates issued to users are only as trustworthy as the business process that issued them. Without appropriate risk-management in the process, the certificates provide a false sense of security. At the same time, the business processes cannot be onerous, or users will reject it—or worse, quietly find ways around it.

Similarly, the support infrastructure needs to deal with different types of users—employees, partners, developers, administrators, customers, etc. Not factoring the different communities and their demands causes support delays and complex procedures leading to higher costs.

What can you do about it?

PKI deployment teams must consist of at least one individual whose focus is on business and support processes. This individual must have deep technical knowledge, as well as strong business and communications skills. Aside from the PKI deployment manager, this individual will most impact how the PKI is perceived. As such, companies deploying PKIs should give this position great attention, and bring him/her on the team, even before the PKI architecture is finalized.

Lesson 6: Build the right operations infrastructure

PKIs require a counter-intuitive approach to operations and systems management. Many large companies organize their operations around specializations, such as Firewall, Network, DNS, Hardware, OS, Applications, etc. PKIs introduce many new layers of technology and dependencies, making it inefficient, as well as insecure, to distribute operations functions amongst multiple groups. Each unique pair of hands on a narrow segment of the PKI adds potential delays and miscommunications.

In our experience, successful PKIs created a dedicated operations group with people possessing a broad range of capabilities, whose responsibilities covered every aspect of PKI operations—managing hardware, operating system, network, DNS, firewall, LDAP, clustering (if any), and all PKI-related hardware and software. This PKI Operations group would be responsible for all activities within the PKI stack, while still coordinating with the larger Operations group in the company.

The advantage to such a model is a cohesion and efficiency in operations, not achievable in "distributed operations". The PKI Operations group will know everything about their infrastructure, and be fully responsible for all activities within it. Secondly, there will be minimal latencies to problem resolutions, since any individual within that group is capable of troubleshooting any problem within the PKI, as opposed to depending on multiple people to determine the problem and solution.

What can you do about it?

If your organization uses the distributed operations model, consider creating a "consolidated PKI Operations Group" on a trial basis, to validate the model before rejecting it outright. Establish and track operations metrics that indicate the relative efficiency of each model. After the trial period, finalize the model that works better for your company. While it might appear that establishing a dedicated PKI Operations group is more expensive in the near term, over a longer horizon, it will result in lower costs and greater efficiencies for the company, so be sure to make the trial period of sufficient duration to show the benefits.

Lesson 7: Communicate, communicate, communicate

This may be the most important reason for the failure of PKI projects—lack of communication! PKIs have an enormous impact on many aspects of IT and business infrastructure. Users have to learn new skills, understand new capabilities, incorporate new functions into business processes. Developers and System Administrators have to incorporate new technology into applications and systems, rethink IT architecture and accommodate new capability in the computing environment.

PKI deployers are, typically, so immersed in implementation details, that they tend to overlook communicating to affected groups of people, other than project and executive management. Lack of information about the project, its technology, progress and impact creates uncertainty, and eventually, resistance.

What can you do about it?

Setup an internal website as soon as the decision is made to build a PKI. Make sure everyone in the core team uses this site as a warehouse for PKI-related documentation—architecture, diagrams, Certificate Policy, Certification Practices Statement, business & support processes, training materials, Frequently Asked Questions, progress reports, etc.

Establish internal PKI-newsgroups for developers, administrators and end-users to facilitate discussions amongst those communities. Use it as a forum to answer questions and provide visibility into the technology and the deployment effort. Executives need their own one-on-one presentations to ensure they get pertinent information.

Successful PKI projects, not unlike any large IT projects, eliminate uncertainty and rumors when authoritative information is readily available. By ensuring that information about the PKI is available to all employees, a huge barrier to the success of PKIs is eliminated.

Lesson 8: Work with someone who has built successful PKIs before

If your company were building a complex web application for the first time, there would be an enormous learning curve for developers and deployers of the application. New programming languages, tools, application servers, directories, security modules, etc. would introduce technologies that were unknown to people on the project. Despite the complexity, IT organizations recognize this is an investment. They definitely need to evolve the application to meet changing business needs and will probably build new applications using the same, if not a more refined, application model. Companies, therefore, plow through the challenges, knowing the investment will provide commensurate returns on future applications.

However, with the right architecture, companies will **never need to build another PKI after the first one**. The company must, therefore, invest an enormous amount of time and money, getting the project team familiar with PKIs, and then architect, design and build a complex infrastructure **just once**. When placed in this context, its obvious that companies are throwing away large sums of money for non-reusable knowledge. (Maintaining a PKI is nowhere as complex as architecting and building a PKI from scratch—especially if it is your first time). Thus, anyone that can help the company eliminate the learning curve, in getting the PKI initially architected and deployed, while navigating them around the road-blocks, will save the company large sums of money—as long as that someone prices their services reasonably.

However, the person who's helping you must have built and operated a successful enterprise-scale PKI before. Any smart guide can tell you that they can get you from point A to point B. A guide that has made that trip more than once successfully, has their own map that avoids the pitfalls, while ensuring that you have a pleasant journey.

What can you do about it?

Ask yourself if your company's core competency includes architecting, building and operating PKIs. If it does not, seek out a guide that can help you achieve your goals. Ideally, your guide should have the following qualities:

- Led—not just participated in - multiple successful PKI implementations;
- First-hand knowledge of multiple PKI products;
- Hands-on application development experience using digital certificates;
- Hands-on operations experience, preferably with PKIs;
- Solid understanding of business and support infrastructure requirements;
- Strong project management and communication skills;
- Multiple references from companies with PKIs of your size and scope;

Conclusion

Most PKIs have have gone through hyped expectations, naive adoptions, disappointments and rejections as a security technology. However, objective analysis and our own experience, indicates that PKIs—when architected and built correctly—can solve more than just security problems. They can improve user, developer and administrator productivity[2], while also playing a role in helping companies deal with Compliance Management issues associated with IT regulations such as SOX[3], GLBA[4], HIPAA[5], California's SB 1386[6] in establishing tighter controls through strong authentication, digital signatures, data-at-rest encryption, etc.

While many PKI projects have resulted in failures and disappointments, it is our experience that it is possible to build successful PKIs. The lessons we've learned over the last five years have been synthesized in this white paper in the hope that it will help you avoid the pitfalls of failed PKI implementations. While heeding the advice in this paper cannot guarantee success for your PKI, applied diligently, it can significantly improve the probabilities for its success.

Arshad Noor is the Founder & CTO of StrongAuth, Inc., a Silicon Valley company providing PKI-based Consolidated Identity Management and Compliance Management solutions.

Arshad is currenly Co-Chair of the Access Control Principle working group in the GAISP initiative, managed by the ISSA. He is the Chair of the Application Guidelines sub-committee of the OASIS PKI Technical Committee. He represents StrongAuth, Inc. in the Technical, and the Public Policy working groups of the Online Identity Theft Prevention Council, managed by ITAA. He is also a Working Group member on Information Security Guidelines for Lawyers, managed by the Information Security Committee of the Section of Science and Technology Law of the American Bar Association

[1] US Government Accounting Office report on **Status of Federal PKI Activities at major Federal Departments and Agencies**—December 2003; http://www.gao.gov/new.items/d04157.pdf
[2] **Network Identity Management System—The Final Architecture?**—May 2002; http://www.digitalid-world.com/modules.php?op=modload&name=News&file=article&sid=62
[3] The **Sarbanes-Oxley Act of 2002**—http://thomas.loc.gov/i107/i107SAN.html
[4] The **Gramm-Leach-Bliley Act**—http://thomas.loc.gov/j106/j106GRAHAM.html
[5] The **Health Insurance Portability and Accountability Act**—http://www.hhs.gov/ocr/hipaa/
[6] California's Breach Disclosure Law (**Senate Bill 1386**)—http://www.strongauth.com/regulations/sb1386/sb1386Index.html

StrongAuth, Inc.

Need to be SOX-404 compliant?

Better get a PKI!

Single-factor authenticators - such as user IDs & passwords - cannot distinguish between authorized users, and an attacker - or even an unauthorized insider - using a compromised ID. As such, they would fail to meet the definition of an "effective internal control" for your financial reporting systems, as required by Section 404 of the Sarbanes-Oxley Act.

What would qualify? A PKI with 2-factor authentication tokens. StrongAuth, Inc. can establish a ***PKI-based solution in three months*** to help you address this part of your SOX compliance strategy. We have the know-how. We have the experience!

Call us today to get your Access Control under control.

issa@strongauth.com

(408) 331-2000 **www.strongauth.com**