PKI Deployment – Business Issues

Table of Contents

Abstract

Deploying a successful Public Key Infrastructure requires a great deal of analysis, planning and preparation. The purpose of this document is to provide readers with information that may help organizations prepare for their pilot project or testing phase of implementing PKI.

This document is by no means a comprehensive guide to a PKI deployment. Rather, it is intended to serve as a guide on how to adequately prepare for some of the challenges that may be encountered.

Topics such as business analysis, risk assessment, policy creation, deployment strategy, and audit considerations will be discussed. This document assumes that the reader is already familiar with PKI theory and understands how public and private keys work. In addition, the role of a certificate authority in providing a viable trust model should be understood.

Establishing the Business Case – Security and Business Requirements

PKI is a robust technology that provides a complete security solution to a company. It delivers **strong authentication, data confidentiality** and**, data integrity.** It enables **non-repudiation** and facilitates **centralized privilege management.**

When establishing the business case, it is important to ask:

- What functionalities do the current technologies lack of?
    - o For what applications do you intend to use PKI?
    - o Are all 5 of the above properties equally important for the applications?
- How well do you know your users? Are controls already in place to establish identity for strong authentication purposes?
- How well do your users adapt to new technology?
    - o Will changing existing mechanisms become a barrier to the success of your applications?
- What are the current risks associated with identity fraud in your applications? Carefully evaluate the risks associate with not using a technology like PKI to secure your enterprise.
- How onerous is the current development process for securing applications?
- Will digital signatures play an important role in the eBusiness strategy of your organization?
- PKI may require the storage of sensitive information about people. Will your organization be able to adhere to any applicable privacy laws?

It is important to note that technologies other than PKI can often be adequate for most security needs. The power of PKI comes from the fact that all 5 of the essential security requirements can be fulfilled with a single technology rather than with multiple solutions. In addition, a common security infrastructure is easier to administer and cheaper to maintain. The primary challenge is to determine if change is needed and how to implement that change in a cost-effective manner.

Devise a medium and long-term plan for the infrastructure. It should be clear how new and existing applications would be engineered to take advantage of the new security mechanisms and how eBusiness strategy of your organization will be enabled. Be careful of the "chicken-and-the-egg" syndrome. You do not want to create a solution looking for a problem. If you are unsure as to the availability of PKI applications once the infrastructure is in place, consider creating a focus group of your peers or customers to manage expectations and to get a level of commitment to the initiative. Obtaining early support of your internal IT and business units, as well as third parties will improve your chances of success.

The selection of a suitable vendor for your PKI is extremely important. The decisions you make at the initial stages will have a significant impact on your PKI strategy. (Refer to PKI technical questionnaire) Consider the following issues when talking to vendors:

- How robust are the products. Will they support the types of applications that you wish to secure? These could include web applications, secure network connectivity, file and desktop encryption, digitally signed forms, privilege management and registration. Look for a vendor that has strong partnerships with other software companies. This will give you flexibility and choice when implementation time comes around.
- What is the current market share of the vendor? It obviously helps if other companies are using the vendor's products successfully. Get as many references as you can, but focus on organizations that mirror your planned implementation as close as possible.
- The relationship with your vendor of choice will hopefully be a long term one. They should have a proper support structure that will meet your expectations. If you will have users all over the world and your vendor does not have 24 by 7 coverage, then negotiate that at the beginning.
- If your vendor prefers to use a value-add-reseller (VAR) then you must ensure that the VAR thoroughly understands your requirements.

Determining Technical Requirements

Once the pilot infrastructure has been established and a business decision has been made to implement PKI in production environment, it is important to understand that an infrastructure that is set up for a proof of concept will almost never serve your needs in a full blown production environment, especially if that environment is expected to pass any stringent audit requirements. Let's consider the following components that you may need in a minimal implementation:

- Certificate Authority software
- Directory
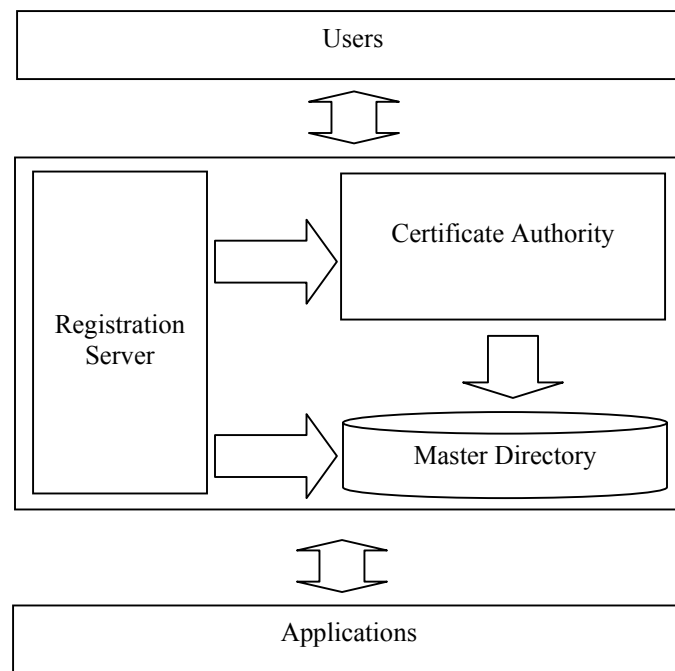- Registration software
- Test applications

Figure 1 – Basic PKI Components

While Figure 1 shows a very simple PKI, a real world implementation can be extremely complex when you start peeling away the layers. See Figure 2.
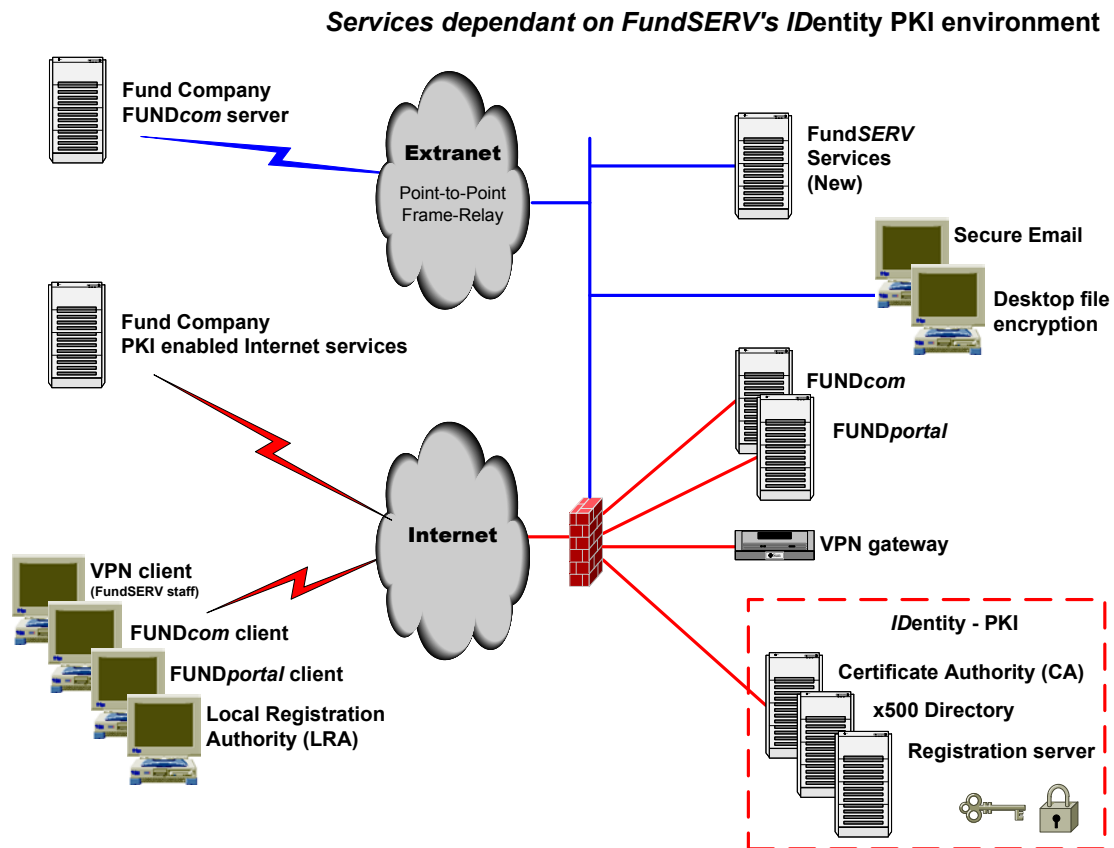
Figure 2 - PKI in the real world

When you consider the infrastructure in Figure 2, the list of components to be supported could include items like:

- Certificate Authority software
- Master directory
- Shadow directories
- Registration software
- Certificate recovery applications
- VPN gateway
- Firewalls
- Application programmers interface for PKI enabling applications
- HSM modules for secure CA key storage
- Secure computer room

As part of your technical analysis consider the following:

- Do you have the technical skills within your organization to support a complex PKI? If not, consider outsourcing its implementation and maintenance.
- If you have internal standards for hardware, ensure that all components of your PKI will be compatible.
- Do you have an adequate business recovery plan to ensure that PKI services are unaffected in the event of system failures?

The decision whether or not to outsource your PKI operations should be one that is made at the start. Do not conduct a pilot in-house if a third party will be providing

hosting and maintenance. Talk to the third party provider about creating an appropriate test environment that will meet your needs, a pilot should attempt to mirror your production implementation as close as possible.

Developing Effective Policies, Practices and Procedures

Robust policies, practices and procedures are integral to a successful PKI deployment. A certificate authority's purpose is to issue digital certificates under a trust model that allows 2 entities to communicate securely with each other. Appropriate controls must be established to create the required level of trust. Refer to the PKIX Internet X.509 Public Key Infrastructure Certificate Policy and the Certification Practices Framework (RFC 2527) for more detailed information on creating policy documents.

PKI policies refer to the business rules that will be used for the PKI implementation. These can be listed in a number of different documents, the most important of which are the Certificate Policy (CP) and the Certificate Practice Statement (CPS). The CP provides an overall business view of how your PKI will operate and the CPS serves as an interpretation of PKI polices according to established standards within the organization such as system design and architecture and operating principles.

If you consider policies to be the "what", practices would be the "how".

Here is a statement that could be made within a CP:

A request for a certificate shall be made directly to the CA by a Registration Authority (RA) or a Local Registration Authority (LRA). Such an application shall be verified with the signature key of the RA or the LRA

The corresponding CPS could elaborate on this statement as follows:

Prior to certificate issuance, a user must apply to a Registration Authority (RA) or Local Registration Authority (LRA) by completing a Certificate Registration Form. Upon satisfactory completion of the defined authentication procedures, the RA or LRA shall provide the user with a reference number and an authorization code, which is used to create the individual profile. A secure digital signature key pair is generated and the certificate request is sent to the CA using the CMP or SEP protocol

Consider the following when you are developing your CP and CPS:

- Create a group of individuals that will be responsible for the maintenance and approval of your PKI related policy documents. This group should serve as the Policy Authority.
- Determine in advance whether you will make the CP and the CPS public. If they will be accessible by your users, ensure that the information contained within does not compromise the security of your implementation. One common practice is to make the CP a public document but keep the CPS internal.
- Establish procedures to ensure that the 2 documents are aligned when changes arise. Components of the CPS should reflect the statements made in the CP.
- The CP will need to include sections addressing the authorized use of the certificates and the liability for the CA in the event of abuse. Get a proper

legal opinion on these sections to ensure that you are protected against damages.

Key elements of the CP and CPS would include elements such as:

- CA liability, obligations, policy enforcement publication of CA information, compliance and data protection
- Authentication, authorization and issuance policies for certificates
- Operational requirements
- Physical, procedural and personnel security controls
- Technical security controls
- Policy administration

Other documents can also be created to support the CP and CPS as required. These could include:

- Sensitive password policy – describes the controls to ensure that passwords required for sensitive PKI operations are protected.
- Disaster recovery procedures – formal description of procedures to recover PKI operations
- Emergency physical access – Policy regarding the admission of emergency support personnel into secure PKI areas
- Audit logging policy – Describes how PKI related logs will be reviewed
- Registration software policy – Polices regarding the use of certification registration software
- Security clearance policy – describes the procedures required for the hiring of PKI staff
- System backup policy – Defines how backup media for PKI systems will be handled
- Visitor policy – Describes the procedures to be followed when visitors require access to secure areas.
- PKI policy authority charter – A formal mandate for your PKI related policy makers
- Incident reporting policy – Any action that goes against defined policies may need to be formally reported to management. This policy would outline the procedures involved.

Internal Operating Procedures

When creating internal operating procedures, ensure that you balance the requirements and procedures. It is important to develop proper policies and procedures to facilitate daily operations; however, it is equally important to ensure that they are realistic to implement and adhere to.

When designing access specifying the number of individuals requires carrying out a certain act or entering a certain area (M of N rules), ensure that it is practical and meets the requirement at the same time. Keep in mind that in the event that you have to access the CA at three in the morning, all of the people involved are readily available. When creating the matrix for PKI assets, go through every operation and scenario carefully to avoid situations where one or two custodians can compromise your CA.

When selecting Master Users, carefully consider their job functions and responsibilities. For example, travel schedules and the inability to be physically present may negatively impact the operation of the CA.

Creating a Successful Deployment Strategy.

Deployment strategies will vary from PKI to PKI. They are largely dependent on the level of security that needs to be attained for applications and the demographics of the community of application users. It is important for the users to understand the reasons behind selecting the PKI technology, the procedures in obtaining certificates and the advantages in using PKI.

It is important to have an organized plan outlining the necessary steps and requirements to obtain a certificate.   Training material should be simple and easy to follow. Advise users in advance if software is required to install on their desktops.

Consider the following when developing your deployment strategy:

- Ensure that you have established an adequate education and marketing plan well in advance of rollout.
    - People do not like sudden changes in technology. Making modifications to the security infrastructure will affect the way users conduct their daily business.
    - Keep your message simple. Avoid unnecessary technical details about how PKI works. Focus instead of the benefits of a robust security infrastructure that protects your users and reduces time, cost and risk. For example talking about the benefits of single sign-on to various applications may be understood better than details about data encryption.
    - Talk about the security requirements necessary to enable a successful eBusiness strategy and how PKI can meet those requirements. [1]
    - Increase security awareness in general. Help your users understand the need for PKI and how it will protect them.

- Be prepared to encounter resistance to your PKI policies. If your infrastructure reaches out to other organizations, their security polices may be different than yours.

- One size may not fit all. You may encounter organizations within your user base that already have their own internal PKI implementations. They may not be eager to give up their own investment. Cross certification should be considered.
    - Create flexible policies that can be modified as required. Consider your CP and CPS to be evolving documents. The challenge will be to address the needs of your users without compromising the security standards that you set out to attain.

- Don't create a trust model that cannot be realistically implemented. For example, if you require face-to-face authentication for certificate issuance, ensure that this is feasible from a business and financial perspectives.

- If your PKI includes other organizations, be prepared for scrutiny from their legal teams. If your PKI requires legal documents to be signed, your users will

---

[1] PKI Basics - A Business Perspective

think twice about clauses regarding terms and conditions of use, most importantly liability in the event of certificate abuse.

- Make it easy for your users to sign up. Don't tie them up in unnecessary paperwork. Electronic agreements are a viable alternative and don't take up precious shelf space.

Resource Planning

A key component of your infrastructure will be technical support services. Requirements will be different depending on the type of implementation. If your PKI simply serves internal users, then existing support structures can be leveraged. However, if you have to support users in other organizations, you may require a more formal plan.

If you plan to outsource the implementation and the maintenance of the PKI, consider outsourcing the helpdesk as well. However, bear in mind that while the third party will most likely have the required PKI skills, they may not possess the business knowledge for application support. Another option would be to split support addressing technical and business issues separately.

If you decide to keep support in-house, you will need to consider the type of support structure that you would like to create as well as the level of support that the users require.   In addition, you have to evaluate the importance for the support staff to pose business vs. technical knowledge. Depending on the complexity of your business area, it might be easier to train an individual who does not have in-depth technical knowledge. You might also want to develop an in-house guide to explain to the employees what this new project is all about and why does the support staff locate in a locked down area.

Take the following items into consideration:

- Training requirements:
  If you plan to certify your personnel, budget accordingly for the appropriate courses and examinations.

- Skill levels:
  Will your helpdesk staff be expected to solve most problems by themselves, or will they escalate technical issues to the IT department or vendor support?

- Hiring practices:
  It may be difficult to hire new people that have adequate PKI related experience. Experienced individuals may be over qualified for a helpdesk role. You can always combat this with an aggressive training plan.

- Security checks:
  Since PKI operations are usually considered to be sensitive, you may need to periodically perform background checks on your PKI staff periodically. Ensure that your human resources department is aligned with such policies.

Auditing Considerations

Before beginning the process of deploying a production PKI, it is essential to take into consideration future auditing requirements.   It is simpler and often considerably less expensive to build the system from the ground up in accordance with best practices and audit requirements rather than to retrofit everything later.
Consider which audits you are likely to require in the future, such as Web Trust or ISO5900, and review the respective criteria for successfully completing these audits. Having a good understanding of audit requirements improves the ability to deliver a scalable compliant solution.

The following issues should be taken into account during the planning stages:

- Plan to conduct an audited Root Key Generation Ceremony for the initial production CA, as this is far more disruptive to do after the fact.
- Plan to use a FIPS 140-1 Level 3 certified hardware key storage device. Migrating keys from software to hardware later will require another audited ceremony.
- Develop CP and CPS documents that are clear and concise, while also covering all required operations aspects. Quality should take precedence over quantity, as concise documents are easier to implement, easier to enforce and easier for auditors to review.
- Develop supporting policy and procedure documents as the system is being built and the support systems are being implemented. This should result in a situation where, on the day the CA goes live, realistic policies and accurate procedures are already in place and staff is already familiar with them.
- Re-visit any existing corporate security related policies and procedures and ensure that they are updated to reflect the addition of the CA infrastructure.
- Consider having PKI Administrators use FIPS 140-1 Level 2 certified hardware tokens for storage of their identities.
- Consider redesigning physical security to be compliant with audit requirements. This generally involves building additional secured areas with electronic access control mechanisms and the installation of a wide range of additional devices, such as biometric readers & cameras.
- Give a lot of careful thought to your M of N rules. The goal is to make it impossible for any one person to complete an end-to-end penetration of the PKI environment and systems.
- Consider implementing a disaster recovery or business continuity strategy. This includes not only a replicated PKI environment at another site, but also the installation of additional monitoring devices at the main site, such as heat detectors and water leak detectors. If linked to a monitored security system, such devices are cheap insurance against a disruption of service.

Conclusion

Deploying a Public Key Infrastructure project is no different than other business/IT project. However, the perception that PKI is a complicated technology can sometimes make deployment challenging. It is important to establish a business case that includes business needs, the scope of the initiative, and the related business, security and technical requirements. Be sure to carry out a risk assessment of not implementing PKI as well.

A set of sound policies and procedures must be created and maintained in order to deploy a successful PKI. It is also critical to review current policies of the company and decide if additional policies and practices have to be established and implemented.

Increase your users' security awareness by continued marketing and education. The success of deployment lies in gathering feedback, listening to the user community, and providing for their business needs.