



ROBERT FRANCES GROUP
Business Advisors to IT Executives

120 Post Road West, Suite 201, Westport, CT 06880 Phone: 203-429-8950 Fax: 203-429-8930

Picking up the value of PKI:

Leveraging z/OS for Improving Manageability, Reliability, and Total Cost of Ownership of PKI and Digital Certificates

Jerald Murphy
Senior Vice President and Service Director
Robert Frances Group



Executive Overview	3
Business and Technology Scenario	4
Why PKI?.....	5
The Importance of Digital Certificates	5
Options for Managing Certificates.....	6
Second Party PKI Services	6
Be Your Own Certificate Authority.....	6
IBM Heritage: Trust and Security.....	7
Centralization.....	7
Virtualization	8
Processing	8
Security	8
Control	8
The Flexibility of PKI Services for z/OS.....	9
Step up for PKI Enablement: a Template for Success.....	10
Risks for IT Business Today.....	10
Business Risk	11
IT Risk	11
Security	11
Complexity.....	11
Operational Risks.....	12
Value of PKI Solutions	13
Value of IBM PKI Solution	13
Value calculation	13
Consideration Factors	13
Costs.....	13
Value Calculation.....	15
Risk Mitigation	16
Business Value Creation	17
Putting PKI to Work Practically: Use Case Scenarios.....	18
Conclusion	19

This report was developed by the Robert Frances Group with IBM assistance and funding. This report may utilize information, including publicly available data, provided by various companies and sources, including IBM. The opinions are those of the report's author, and do not necessarily represent IBM's position.

Executive Overview

With the never-ending increase in security exposures in companies, as well as the resultant publicity associated with compliance audits and public notification of identity theft, IT executives are very concerned that customer data and intellectual property be adequately protected. In addition, the range of attacks designed to fraudulently pose as legitimate users is driving business environments to demand better identity management and transactional security. Robert Frances Group has found through its clients that Identity Management is one of the top three items IT executives are concerned about and plan on focusing resources to address in the coming year.

Public Key Infrastructure (PKI) is a set of technologies and services that helps to address the issue of identity management, especially for helping to certify the identity of external as well as internal resources (people, as well as systems and applications). The advantage of stringent certification of identities is that it protects sensitive data and verifies the data was received, in a way the end-user cannot deny.

Effectively implementing PKI on distributed systems tends to be complicated and costly. There are multiple systems and data stores that get involved in sophisticated PKI infrastructures involving databases to store certificates, processing costs, operating system and database support, and the personnel costs associated with the maintenance and processing of the PKI transactions. Many of these issues are mitigated through a mainframe based implementation. Databases dispersed across distributed platforms are consolidated onto a single footprint. Keystores can work with the existing external security manager to associate certificates and key pairs, and management of security resources can be integrated. The PKI Services component of z/OS is integrated into the mainframe operating system; thereby further reducing cost of ownership. PKI Services on the mainframe leverages the strengths of the platform for full lifecycle management, automated certificate approval, PKI process integration, and interconnection flexibility.

Perhaps most important, in this environment of increased threats, is the long-standing reputation for security and trust that is a fundamental strength of mainframe computing. While this paper cites some specific cases of operational efficiency and business value, the total value of increased business operations security will continue to increase. The dynamic nature of the automated, integrated, virtualized business processes of tomorrow will place even more value on strong identity management, which will continue to add value to mainframe-based PKI solutions.

Business and Technology Scenario

Companies are currently faced with a divergent IT challenge. On the one hand, companies look to information technology to lower operational costs by automating more business processes. On the other hand, the ever-growing complexity of enterprise infrastructure as a result of increased automation increases the enterprise exposure to attacks on sensitive business information. Recent public announcements of information theft only raise the concerns of business unit managers. At the same time, external audits that verify the compliance of companies to information protection statutes make the IT and security managers' burdens seem never-ending.

While the threats to business information continue to increase, so does the cost to the business for lost downtime. Companies can ill afford to ignore the risks to the business brought about by system vulnerability and compromised data.

Figure 1 Cost of downtime by industry segment

Industry/Sector	Revenue/Hour
Energy	\$1,468,798
Telecommunications	\$4,611,604
Financial	\$8,213,470
Information Technology	\$3,316,058
Insurance	\$2,582,382
Pharmaceuticals	\$2,058,710
Banking	\$1,145,129
Consumer Products	\$989,795
Chemicals	\$1,071,404
Transportation	\$1,463,128

Source: Robert Frances Group 2006

IT executives must balance the need to integrate these complex environments with the requirements for efficiency and security. RFG believes companies will need to rely on trusted partnerships with companies that have a strong track record with security process and technology, in addition to understanding management of complex business environments.



Why PKI?

The public key infrastructure (PKI) provides applications with a framework for performing the following types of security-related activities:

- Authenticate all parties that engage in electronic transactions
 - As users enter the computer system their identity must be verified through the use of some mechanism which assures the system that the user is indeed who they say they are.
 - Digital certificates, provided by the PKI, contain the information necessary to prove the authenticity of a user's identity. Because the digital certificate is encrypted by a trusted entity, such as a Certification Authority, the authenticity of the certificate itself is not suspect.
- Verify the author of each message through its digital signature
 - Companies making use of unsecured networks such as the Internet for business-to-business transactions, or single-owner networks such as a corporation's intranet, can be assured that the data will remain intact and unread while in transit.
 - The sender can't repudiate or deny sending the data as long as his/her signature is included.
- Encrypt the content of all communications
 - Data flowing across unprotected networks should be encrypted to prevent unwanted viewing and alteration. PKI provides the keys necessary to protect the digital conversations between two entities. A simpler session key is used to protect the actual data, but the exchange of the session key is protected with a public/private key pair.

The Importance of Digital Certificates

One of the areas of technology that is helping companies protect critical corporate data is the use of digital certificates. A digital certificate is a combination of an entity's public key, used for encrypting information, along with a signature from a trusted agent verifying the authenticity of the entity's credentials.

The combination of encryption and identity verification is increasingly essential to business transactions. Encrypting information protects the information from being seen by unauthorized people or tampered with by them. Verifying the identity prevents users from getting forged information from people pretending to be someone they are not. With the increased oversight on data privacy from regulations such as Gramm-Leach-Bliley and HIPAA, companies need to make sure they are properly protecting sensitive information.

Since certificates verify a person's identity as well as encrypt information, businesses can also verify that a person actually saw data or performed a transaction. This is critical for businesses such as financial services, where a broker wants to be able to prove a client authorized a financial transaction on his behalf. When a company uses a digital certificate to authorize a transaction, it can legally prove that the authorized account holder was, in fact, the person who executed a transaction.

As more business processes become automated, the number of use cases for digital certificates will continue to increase, which will increase their importance and visibility. Several groups RFG interviewed said they were planning on growing their use of certificates by over 300% in the coming year.

Options for Managing Certificates

Since it is clear that the value and need for digital certificates will only increase, IT executives should examine the options available for managing PKI environments. Today, there are essentially two options available to businesses: buying PKI services from second parties, or building and managing their own PKI.

Second Party PKI Services

The first option IT executives can consider is to use a third party for digital certificate management. Companies such as Verisign, Cybertrust, GoDaddy, offer companies the option of issuing and managing digital certificates for them. While an advantage of having a third party manage certificates is offloading the management of PKI, the cost of doing this can be significant. The cost is going to vary by individual versus application/server certificates, and the price will increase as the company increases its use of certificates. As business process automation continues to accelerate, these service costs will certainly rise.

Be Your Own Certificate Authority

Another option available to companies is to build their own certificate authority. Historically, this option has had its own costs and complexity. Companies such as Entrust make software that companies can use to build a PKI. However, these solutions can be expensive to buy and complex to operate and maintain.

An alternative companies have is to build their PKI using PKI services that come with the IBM z/OS operating environment. The central use of PKI services can reduce management complexity. The bundling of PKI services with the OS eliminates separate acquisition costs, while the use of certificates carries no unique additional cost, regardless of the number of certificates managed. With this option, companies have the flexibility of growing the use of certificates, without a concomitant increase in the cost of using PKI.

We will now look into some of the factors to evaluate when considering the use of IBM PKI Services

IBM Heritage: Trust and Security

One of the biggest concerns IT executives and security managers have about distributed systems is the large security risk that exists with most computing environments¹. Distributed systems by their very nature are not typically in a centralized location. This places the systems at risk physically, since there are more places where they can be accessed and exploited.

Even when these systems are located in a data center, they are logically separate, which makes them more vulnerable to attack. System administrators and security managers have more places to check for exposures, more systems to look at for security updates, and more steps to go through to fix vulnerabilities when they occur.

Most of these problems are avoided with a centrally managed mainframe environment. IBM systems have a long, ongoing reputation for security, where it has been built into the earliest system designs with concepts such as logical partitions (LPARs), and customer information and control systems (CICS). Additionally, physical security has historically been much stronger in mainframe environments. Even when there are multiple systems, system complex processing (SYSPLEX) gives the effect of operating with one logical processing environment.

As companies increase their focus on identity management, PKI protection places a premium on protecting root certificates. Most companies RFG has interviewed actually place these systems in a physically locked environment, requiring the highest level of trust for business critical data. Since mainframe environments are almost always in a central data center environment, they are typically in a better position to be physically secured.

Natural Location for PKI: The Mainframe

The combinations of centralization, virtualization, processing, security, and control are what IT managers have come to expect and rely on in mainframe computing environments, which makes the environment a very natural one to place business critical security processes like PKI on.

Centralization

In order to effectively manage PKI, root certificates should be centrally managed. If the certificate management were distributed, there would be more places that need to be physically secured. Additionally, it would be more difficult to manage the certificate lifecycle, such as coordinating revocation lists, renewals, etc. Additionally, organizational control of certificates is ideally done by one authority; keeping the system and the group

¹ Conclusion is consensus of CIOs and CISOs from RFG roundtable discussion during RFG Risk Management Summit, Nov 2005. Summary of findings contained in Challenges and [Best Practices for Enterprise Data Protection](#)

together can reduce complexity. All security managers that RFG speaks with agree that reduced complexity directly corresponds with increased security. Centralization of PKI services via a mainframe can directly reduce complexity.

Virtualization

Mainframes have specialized in virtualization for a long time. Logical partitioning has been a fundamental attribute of mainframes, where the operating system allows strict control of the workload scheduled for each processor. As business requirements for certificates increase, it is a very straight forward process to increase the resources dedicated for managing certificates on the mainframe. Resources can be dynamically added as needed, while maintaining logical separation and control.

Processing

In addition to partitioning, the mainframe job schedule similarly allows strict control of what processes get executed on an engine in what order. In this way, work can be performed in priority order according to strict business requirements. Processing dedicated to a task can be modified as needed to fit both the workload as well as the business priority.

In current distributed environments, additional resources needed for processing PKI would have to be physically assigned. Since distributed PKI services are managed in secure facilities, IT managers cannot simply add these processes to free systems if those free systems are not in the physically secure facility. Internal management of PKI with distributed systems will incur increased server costs, as well as operational costs for move, add, and change (MAC), even when these servers exist for reuse.

Security

One of the biggest requirements for a PKI solution is the security of all the components, especially for the root certificate store. Since the root certificate authority is responsible for validating all the certificates it issues, its own private key must be well-protected. Encryption solutions must be robust, and protection of the PKI environment is essential. Mainframe systems are designed with these attributes. Mainframes have built-in hardware encryption engines, strict control and process compartmentalization.

Control

To guard the security of a PKI solution, tight control of all the elements of the solution must be established and maintained. Private keys must be protected and not allowed to be compromised. Management control must be managed for certificate issuance, renewal, and revocation. Revocation lists must be maintained to verify the validity of certificates. The business environment must be tightly controlled in order for a high level of trust to be established. Mainframe environments provide this level of control and trust.



Large companies have been relying on IBM mainframe environments for years for their most sensitive data and business applications. It is natural to extend this trust for PKI solutions.

The Flexibility of PKI Services for z/OS

PKI Services allow security managers to establish a PKI infrastructure and serve as a certificate authority for their internal and external users, issuing and administering digital certificates in accordance with your own organization's policies. Users can use a PKI Services application to request and obtain certificates through their own Web browsers, while authorized PKI administrators approve, modify, or reject these requests through their own Web browsers. The Web applications provided with PKI Services are highly customizable, and a programming exit is also included for advanced customization. Systems Administrators can allow automatic approval for certificate requests from certain users and add host IDs, such as RACF user IDs, to certificates you issue for certain users to provide additional authentication. Several notification options can be configured, including notification that the user's certificate is ready to be picked up, the certificate request has been rejected, and that the certificate is expiring. Administrators can also issue their own certificates for browsers, servers, and other purposes, such as virtual private network (VPN) devices, smart cards, and secure e-mail. PKI Services supports Public Key Infrastructure for X.509 version 3 (PKIX) and Common Data Security Architecture (CDSA) cryptographic standards. It also supports the following:

- The delivery of certificates through the Secure Sockets Layer (SSL) for use with applications that are accessed from a Web browser or Web server.
- The delivery of certificates that support the Internet Protocol Security standard (IPSEC) for use with secure VPN applications or IPSEC-enabled devices.
- The delivery of certificates that support Secure Multipurpose Internet Mail Extensions (S/MIME), for use with secure e-mail applications.

Step up for PKI Enablement: a Template for Success

Setting up a public key infrastructure is a complicated endeavor. A typical PKI set up involves coordinating several elements, as shown below:

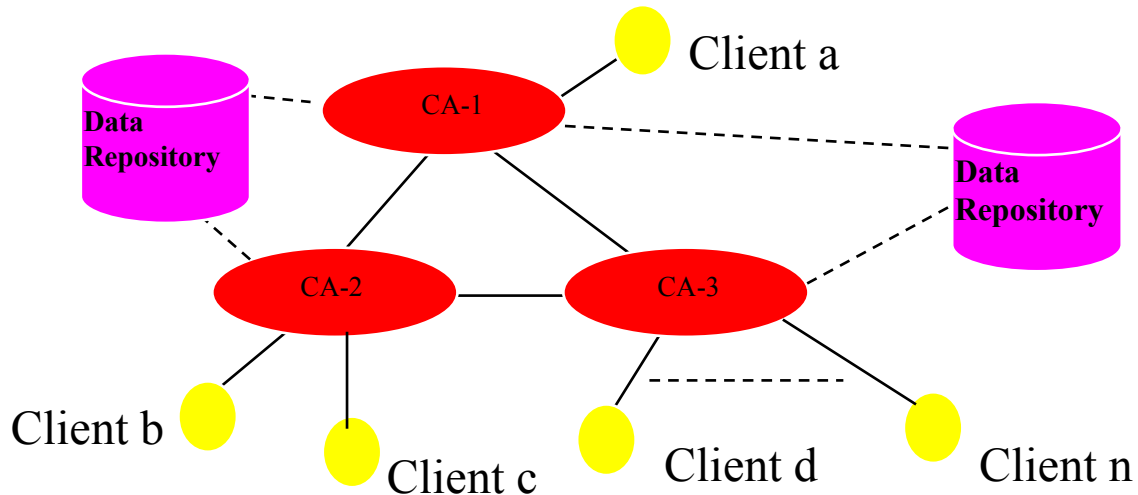


Figure 2 Typical PKI Setup

Source Robert Frances Group

IBM mainframe PKI service has a template that companies can use to start the PKI process. While the systems may need some modifications to work in environments, the modifications are not complicated, since all the components of the service reside in the same location. Many companies find that the templates provided help a great deal in starting the process.

The biggest challenge in setting up a modern PKI is the difficulty in managing the potentially multiply-nested certificate authorities, in conjunction with the certificate lifecycle, including certificate issuance and revocation. With all the complexities that are involved in establishing and maintaining PKI, most IT executives agree that heading off problems before they occur in the first place dramatically improves operational efficiency and security.

Risks for IT Business Today

Risk for business is increasing on a daily basis. Not only is the number of threats increasing, but also the types of attacks are becoming more sophisticated, including multi-vector attacks. Identity information is not just stolen by hacking into central computer data stores, but is obtained when people pose as imposters to get information, and or when imposters pose as legitimate public service institutions. Both the business and the individual consumer need to be able to verify the identity of the other to mitigate risk and ensure the integrity of every business transaction.



Business Risk

Business risks for identity theft and fraud are certainly financial. When identities are stolen, all of the financial resources associated with that ID are at risk. Equally problematic to the business is the reputation risk as a result of damage to the corporate image. These are difficult to measure directly, but most business executives would agree the exposure to companies from loss of reputation can be in the millions of dollars.

IT Risk

IT risks associated with PKI systems exist in the area of security, complexity and operations. IT executives must pay attention to risks in all these areas in order to have a scaleable, reliable PKI system.

Security

Encryption, theft of data – In order to protect sensitive data, companies need to protect this data from access by unauthorized people. Not only is data exposed while it is at rest in the data store, but it is also exposed during transmission from one system/person to another. Best practice is to encrypt data in both scenarios. PKI systems encrypt data in transit from one person to the next, so any agency that interrupts this information in flight (for example, in the air when the information is going over a wireless network) will not be able to read it. PKI systems also encrypt the keys stored on systems, so that the key itself cannot be stolen and used to decrypt classified information. IT executives must ensure PKI solutions tightly control both types of encryption.

Physical security – IT executives can minimize risk by reducing the number of sites that need to be physically secured. This is challenging in distributed environments, since the different application tiers are not always in the same location. Mainframe environments tend to be centralized, and they are usually already part of a physically secured facility.

Viruses – IT executives see viruses as an ongoing, constantly changing threat to the business environment. Security officers see largest risk to end-user systems, followed by Microsoft-based operating systems. Distributed systems in general offer multiple points for virus attack. Mainframe based systems are viewed as the least at risk for compromise via viruses, worms, etc.

Malware – In addition to viruses, which seek to destroy operating systems and alter/erase data, malware's goal is usually to surreptitiously gather sensitive information by passively collecting user information (key loggers, cookies, etc.) and sending or selling this information to unauthorized third parties. Similar to viruses, Mainframe systems are far less susceptible to such infiltration and misuse.

Complexity

Distributed systems make it difficult to coordinate solutions. As companies move from N-Tiered to service-oriented architectures (SOAs), this problem will become more complex. The problem with complexity in systems is that once one piece changes, the

rest of the infrastructure will likely need to be rearranged to account for changes in another area. Modeling what will happen when one element changes becomes more difficult.

This complexity increases the probability that some unknown behavior will creep into the system. More ominously, it provides more opportunities for data to become compromised or otherwise exploited. Some of the elements that are directly linked to complexity and security include operating system (OS) patches, application updates, database patches, and hardware compatibility.

Additionally, version control between hardware, OS, database, middleware, applications, multiple business partners, etc. makes it very difficult to know for certain that all elements of risk have been removed from the system. In reality, it is impossible to remove all risk from the system, and cost prohibitive to eliminate most of it, especially in a complex, distributed environment. Mainframe systems can mitigate much of this risk, with standardized operating environments and centralized management.

Operational Risks

IT executives are always trying to minimize operational costs. The natural complexity of PKI solutions has a tendency to carry increased operational risks. The costs around PKI that impact operational costs include the processes around PKI management, systems costs, and personnel costs. These are briefly reviewed below:

More steps involved for PKI management – Typical PKI lifecycle includes approving and issuing new certificates, updating and changing certificates, reissuing certificates, revoking no longer approved certificates, and managing the certificate revocation list.

Systems costs for PKI include the hardware to run the PKI software, encryption hardware, hardware for key management (if not all included on the same system), the costs of the software to run the PKI infrastructure, and maintenance costs for this hardware and software. Personnel costs include the cost of the people dedicated to running the PKI infrastructure (if not outsourced), and the incremental headcount associated with hardware and systems management for those systems dedicated to PKI.

For PKI on the mainframe, many of the costs may be dramatically reduced. Since PKI software and services come built into the mainframe operating system, additional incremental hardware costs are not incurred. Incremental maintenance costs may be limited to the MIPS associated with the LPAR running PKI. Finally, there is usually no additional systems management when PKI is run in the mainframe environment, although there is usually someone with overall responsibility for PKI administration.

Value of PKI Solutions

While IT managers tend to focus on the technical details of solutions such as PKI, the business usually doesn't care about the technical details. Whatever systems are implemented, the business wants IT to be able to address business-oriented issues: How much does the solution cost? Does the action need to be performed? What is the risk to the business if I don't perform the function? How scalable is the function? Will it grow with the company? Can this solution integrate with other systems the business is already using?

RFG believes IT executives should look at both the business risks and the value to the business to better communicate with management and to make decisions that best support the business.

We will now walk through some considerations that will help IT managers look at the risk and benefits of PKI solutions in ways that can be explained to management, ending with a value calculator that can be used to help automate this analysis.

Value of IBM PKI Solution

Value calculation

When calculating the value of a solution, IT executives must measure the cost of implementing a solution against the risks associated with not having it, as well as the business (and, to a lesser extent, technical) benefits of such a solution. RFG often finds that these considerations are evaluated subjectively. When IT executives can evaluate these various factors in as objective a manner as possible, they are in a better position to make realistic tradeoffs, and present this analysis to business managers in terms they are more likely to understand and support.

Consideration Factors

RFG believes the following set of factors should be used to perform a PKI benefit analysis. After the factors are reviewed, we will show a sample template that can be used to perform a detailed benefit analysis.

Costs

The first, and often most important, factor to consider is the cost of a PKI solution. Cost is usually high on the importance scale for two reasons: costs can be objectively quantified, and they can often be directly incorporated into budget planning. The costs associated with PKI implementations include:



Certificates

Most implementations of PKI include a direct cost per certificate managed or issued. These costs can be \$5 for individual certificates and up to \$500 or more per server or application certificate. This is one of the biggest potential benefits of IBM PKI on the mainframe. Since the PKI software is an integral part of z/OS, the purchase costs of the certificates are eliminated. Prices for individual certificates will vary with the size of a given PKI implementation, and very large implementations can drop the per-certificate cost. However, all of these external certificate costs are eliminated with a mainframe-based PKI solution. Since it is entirely likely that the number of uses of digital certificates will increase over time, the cost of outsourced PKI services will continue to increase. Using PKI on the mainframe may help dramatically reduce the cost per certificate, which could increase the number of types of applications with which a company can consider using certificates.

CPU Costs

There is a certain amount of CPU that gets used to manage a PKI. In the case of a mainframe solution, very few MIPS can support thousands of certificates². While MIPS calculations don't directly apply for outsource services (these are rolled into the per-certificate costs), non-mainframe solutions almost always have dedicated hardware to support the PKI implementation. Therefore, IT executives should compare MIPS used against hardware, operating system, and application costs for a relative comparison.

PKI Support

This is the cost for dedicated full-time engineers (FTEs) that are experts in the PKI software to manage the PKI environment. This number tends not to vary from distributed to centralized systems, and this number is rolled into the price of an outsourced PKI service. However, even with an outsourced certificate service, the company must still have someone that is responsible for managing the relationship with the service provider.

OS Support

This is the incremental FTE cost associated with supporting the operating system and the server on which PKI solution runs. In the case of the mainframe, this is subsumed by overall platform management. In the case of distributed systems, those PKI elements will run on separate platforms and have a measurable FTE number. For these types of applications, the typical FTE ratio is 1 FTE per 15-20 systems³.

² Results found in interviews with financial institutions interviewed by RFG in 2006, with measurements performed for operations in both Europe and North America.

³ Numbers obtained as a result of RFG interviews with North American IT and Security systems managers, 2006.



Database Support

In addition to the operating system, separate database support is needed to support the data repository (ies). In some cases, the PKI information is linked with X.500 or, more likely, LDAP or Active Directory identity management systems. However, there is additional policy information and keys that need to be managed that are typically stored in separate data stores. Database administrative ratios are similar to OS administrative support ratios for application servers. While these ratios tend to be similar, RFG often finds that the responsibility for key management is not with the database administrator, but with the security group. In this case, additional personnel need to be included for key management

Manual Approval Cost

Even when distributed computer systems are built for PKI, the issuing and approving of certificates can still be a manual process. Most of the companies that RFG talked with that are using PKI systems have a significant portion of certificate management that is still done manually. When this is the case, FTE load for this manual process needs to be added to the PKI operational costs. With mainframe-based PKI, the approval process is automated, so these costs are eliminated.

Value Calculation

Once the PKI costs are considered, IT executives should then evaluate the value of implementing these systems. While the value may be subjective, a relative ranking should be assessed. First, the assessment should be done in qualitative terms. Next, a relative value should be associated with the ranking of a category, so the alternative solutions can be evaluated on a relative basis. RFG recommends the following value areas be considered:

System Scalability

System scalability is important, since it can influence the additional incremental cost that will be needed to support future certificate growth. If the number of certificates needed is dynamic or growing rapidly, building a system that supports high scalability can lead to lower operational costs, and put off future capital expenditures.

Full Certificate Lifecycle management

If the PKI system implemented can cover the full certificate lifecycle, operational costs are likely to be less than if different systems or groups manage different parts of the solution. Additionally, a solution that manages the full certificate lifecycle will be less complex, requiring fewer disparate system interfaces. This will increase the security of the system, which is of critical importance to sensitive information such as key management.



Automated approval

Not only can automated approval help reduce operational costs, by reducing the number of FTEs required to support the system, it can also improve the quality of service to end users, by minimizing the time required to obtain and renew certificates.

Revocation list integration

Active maintenance of certificate revocation lists (CRLs) is a critical part of PKI management. This is also an area that can create security gaps, since a person that is using an expired/invalid certificate (such as a lost certificate or a terminated employee) can be a serious security exposure if allowed access to unauthorized data as a result of not getting CRL updates. PKI systems must have tight integration with revocation lists to ensure system integrity and security.

Interconnect Flexibility

Regardless of how well a PKI system is built, it will have to integrate with other systems. Most companies RFG has spoken with about PKI have needed to integrate with external certificate authorities, even when they are managing their own PKI. Partners will have their own certificate authorities, requiring cross-certification. Additionally, companies will need to work with partners who use outsourced solutions from management security services. Applications and people will need to integrate with an enterprise that has certificates registered with other domains. This requires a proper PKI system to be able to cross-certify with other independent domains. The system should be based on open standards that will allow maximum flexibility while maintaining control within its own trust domains.

Risk Mitigation

In addition to looking at the costs of PKI solutions and their value to the company, IT executives should also look at the risk to the environment that is mitigated (or increased) as a result of implementing a given PKI solution. Key factors to evaluate for risk mitigation include:

Compliance

Optimal PKI solutions for compliance should be easy to audit and achieve guidelines for data protection and privacy.

Identrus

Identrus is a company founded by a consortium of banks that wanted an independent agency to ensure the authentication of identity of the partners and their clients. Having a PKI solution that is certified to work in this framework is of significant value to the constellation of financial institutions that participate in this community.



Data Security

The most important requirement for many companies is the security of corporate information: financial, intellectual property, and employee and customer data. PKI solutions should be evaluated for their fit into the overall data security framework that protects these key assets.

Fraud Reduction

Identity theft and data theft are becoming huge problems in the industry. Evaluate the proposed PKI solution on its ability to reduce or eliminate fraud for the enterprise applications that are using PKI.

Business Value Creation

When PKI solutions are evaluated against cost, business value, and risk reduction, the overall comparison of these components will reveal a total business value for the PKI solution. Ideal solutions should not only be economical, but also decrease risk and increase the actual value of the business applications to the clients, which ultimately can increase company credibility, raising the overall brand value of the company.



Putting PKI to Work Practically: Use Case Scenarios

RFG talked with several companies that have implemented PKI solutions in order to determine what they see are the costs, values and risks associated with their own PKI environments, including distributed PKI systems, mainframe-based PKI systems, and outsourced PKI solutions. The chart below is a summary of the information collected from those interviews.

Figure 3 Sample PKI Value calculation

PKI Value Calculation	Total Service Cost	Total Distributed cost	Total Mainframe cost	Service unit Cost ⁴	Server Unit Cost	Mainframe Unit cost	Total Units
Costs							
Certificates	\$75,000	\$ -	\$ -	\$5.00 indiv. \$500 svr/app	\$	\$	10000 50
CPU Costs		\$ 30,000	\$20,000	\$ -	\$15,000	\$ 10,000	2
PKI Support		\$ 40,000	\$40,000	\$ -	\$ 80,000	\$ -	0.5
OS Support		\$ 18,750		\$ -	\$75,000	\$ -	0.25
Database Support		\$ 20,000		\$ -	\$80,000	\$ -	0.25
Manual Approval Cost	\$20,100	\$ 10,050		\$ 2.00	\$ 1.00	\$ -	10000 50
Per transaction costs	\$12,500	\$ 12,550		\$ 0.25	\$ 0.25	\$ -	50000
TOTAL COST	\$ 102,600	\$131,250	\$ 60,000				

Figure 4 Comparison of the risk and value associated with different PKI service alternatives

Value and Risk	PKI Service	PKI on Distributed Platform	PKI on Mainframe
<i>Scalability</i>	5	3	5
<i>Lifecycle Management</i>	4	2	4
<i>Automated Approval</i>	3	2	5
<i>Revocation List Integration</i>	5	3	4
<i>Interconnection flexibility</i>	5	3	4
<i>Overall Risk Mitigation</i>	4	3	5
TOTAL Value	4.33	2.66	4.50

⁴ Unit costs defined as the element being measured. In most cases, the unit is a digital certificate per individual. Where noted, unit may be a server or application, which have higher per-unit certificate costs.



Conclusion

As businesses become more automated, they have more opportunities for growth, yet more risks for fraud and theft. PKI is a security method designed to validate the identity of the parties involved in transactions, help protect the confidentiality of the information, and nonrepudiation of the business transaction. In this era of increased complexity and risk, PKI systems are becoming an increasingly essential element to every business.

However, PKI systems are inherently complex, and implementing a PKI that can scale to a large, dynamic user base, while integrating with existing and future infrastructure elements can be expensive. Improperly implemented or managed, a PKI system can bring its own risk to the IT infrastructure. While outsourcing these tasks can eliminate some of the infrastructure development risks, outsourcing may have its own limitations, and it certainly has its own costs.

IBM mainframe systems have built-in PKI software. This software is designed to work with existing systems infrastructure, with built-in templates to speed the development and deployment process. Since the software is built into the operating system, there are no additional software or maintenance costs associated with its use. This combination of low cost and built-in integration can help reduce complexity, and potentially lower operational costs. Additionally, mainframe-based PKI has the added benefit of the reduced risk associated with the well-known reliability and security of mainframe systems.

IT executives should evaluate the need for PKI systems in their enterprise, and consider costs, value, and risks associated with distributed solutions, services, and mainframe-based solutions to arrive the optimal solution for their business environment. While buying a mainframe system for the purpose of building PKI is not likely to make economic sense, leveraging existing mainframe systems can be an economic, secure, and reliable way of establishing and expanding a company's PKI services.