



# Data Security Mythbusters:

---

## Public Key Infrastructure (PKI)

TECHNICAL WHITE PAPER

## Table of Contents

Executive Summary	3
Symmetric vs. Asymmetric Encryption	4
What is PKI?	4
What are Public Keys and Private Keys?	4
What is X.509?	5
What is a Certificate Authority?	5
Myths Busted	5
Myth one: To manage digital certificates a public-key must be deployed, including certificate authorities and other complex processes	5
Myth two: Managing keys and certificates requires a lot of people and a lot of time	6
Myth three: To manage keys, expensive software must be purchased with high ongoing maintenance costs	6
Myth four: The only way to manage keys successfully is by placing them in hardware	6
Myth five: Managing keys requires a data center with robust physical security	7
Conclusion	7

## Data security mythbusters: Public Key Infrastructure (PKI)

In today's business environment, enterprises must work even harder than before to protect one of their most valuable assets – their information. When facing the pressures of regulatory oversight, email security, business-to-business requirements, and increased threats to networked environments, organizations must be proactive in protecting their data. A single loss or breach of information can have a severe impact on an enterprise's brand and public image, on customer retention, new business attraction, and the tangible bottom line. It is these factors that are driving enterprises to understand how they can address these issues, immediately, diligently, and cost effectively.

---

Even in the current risk environment, many organizations have failed to adopt public key infrastructure (PKI), a necessary component for truly durable data protection. Stories of failed PKI projects, cost overruns, and lack of efficacy of the solutions have created a perception that key management is too difficult to implement. Many of these perceptions are based on the painful experiences of early adopters during the neophyte days of PKI. PKI excels in the facilitation of digital signing and encryption in an enterprise environment while providing centralized management for corporate security policies. PKI-based data encryption strategies that are well implemented meet enterprise requirements for speed of deployment, ease-of-use, application integration, and return on investment (ROI).

This document will provide a review of PKI concepts and terminology and summarize the five primary myths associated with PKI management, while placing them in the context of today's marketplace in terms of available technology and genuine business value.

The five myths surrounding PKI management addressed in this paper include:

**Myth One:** To manage digital certificates, a complete public-key infrastructure must be deployed.

**Myth Two:** Managing keys and certificates requires a lot of people and a lot of time.

**Myth Three:** To manage keys, expensive software must be purchased with high ongoing maintenance costs.

**Myth Four:** The only way to manage keys successfully is by placing them in hardware.

**Myth Five:** Managing keys requires a robust, secure data center.

## Symmetric vs. Asymmetric Encryption

**Symmetric Encryption** Password-based encryption is an example of symmetric encryption – both the person encrypting the data and the person for whom the data is encrypted must know the same password to access it. In symmetric cryptography (a.k.a., secret key cryptography), an algorithm is used to scramble the message using a secret key in such a way that it becomes unusable to anyone who does not have access to that secret key.

Symmetric cryptography works well only if encryption and decryption are eventually performed by the same individual or entity. When 2 or more parties become involved, there is the question of how to exchange the passwords without it being intercepted, copied, or breached by “man-in-the-middle” attacks.

A symmetric key is created during the encryption process and is generated via a password. Both the sender and the receiver must have access to the same password (symmetric key). The greatest challenge with symmetric cryptography is how to securely distribute the secret key to the involved parties. Another issue is that since both parties have the same key, it makes the data more vulnerable to attack.

**Asymmetric Encryption** In asymmetric encryption, also known as public key encryption, algorithms use two different keys: a private key and a public key. A message encrypted with a public key can be decrypted with its private key. The owner of the key pair holds the private key and may distribute the public key to anyone. Someone who wants to send a protected message uses the public key of the intended recipient to encrypt it. Only the person who holds the private key can use it to decrypt the information.

The difference between symmetric and asymmetric encryption can be illustrated with a lock and key analogy. A lock with a single key is analogous to conventional, or symmetric, cryptography. Alternatively, public key or asymmetric cryptography is like a different kind of lock that uses two keys; one can secure the lock, but not open it, and the other can open the lock, but not secure it. The key that can open the lock is kept securely, but an infinite number of copies can be made of the other key to support broad distribution of the public key.

For example, if Pat, Doug, or Susan want to send a secret message to Bob, they will encrypt it with Bob’s “locking” key, or public key. When Bob receives the encrypted message he will decrypt it with his private key.

## What is PKI?

PKI is an acronym for Public Key Infrastructure, a method for issuing and managing digital certificates. Digital certificates bind an identity, including name and associated data such as email address, location, etc., to an electronic public key. A single public key is uniquely assigned to a single individual or entity. A public key is paired with a corresponding private key to produce a unique key pair.

## What are Public Keys and Private Keys?

Public/private keys are used to encrypt and decrypt data and are issued to individuals or an entity, such as an Information Security Department, when a digital certificate is obtained. The digital certificate verifies the identity of an individual or entity and the key pair is bound to the identity associated with that certificate. Public/private keys are used to encrypt and decrypt data, and enable the encrypted data to be shared with others without having to first exchange some other “shared secret,” such as a password.

PKI provides stronger security than passwords because passwords are prone to being intercepted or to inherent weakness if they are short, easy to guess, or written and stored inappropriately (such as writing the PIN number

on the back of an ATM card). Using a conventional password-based encryption scheme, the password must be exchanged between everyone that wishes to share encrypted data by a secure method such as face to face meetings or via a trusted courier. These options are very expensive and do not scale to the level of enterprise needs.

Using PKI, the encryption and decryption keys are different for each user and it is impossible for anyone to convert one type of key to the other. This allows the encryption key (public key) to be accessible by the public. It can be posted to a website and emailed without concern that it will be intercepted or copied because it can only be used to encrypt data; it cannot be used to decrypt data. In a PKI environment, users share secured data by obtaining the recipient's public key from the web or an email and encrypt the data using that key and an appropriate encryption application. Because information cannot be decrypted with the public key, no one other than the intended recipient of the protected information can decrypt it. Even the person who encrypted it cannot reverse the process. To decrypt data, the recipient uses the private key that corresponds to the public key. This key never leaves the recipient's possession, residing securely either on a computer or a smart device (card, USB drive, etc.).

### What is X.509?

X.509 is the name commonly applied to an international standard for the format and information contained in a digital certificate. X.509 is the most common type of digital certificate. A digital certificate is a digital document that contains a public key signed by a trusted third party, known as a Certificate Authority (CA).

### What is a Certificate Authority?

A Certificate Authority (CA) is the application for security professionals that issues public/private key pairs and binds the identity of an individual (name, email address, and/or other demographic elements) to the public key by means of the certificate. Popular CAs include VeriSign, RSA, Comodo, and Entrust.

## PKI Myths Busted

**Myth one:** To manage digital certificates, a public key infrastructure must be deployed, including certificate authorities and other complex processes.

When asked by senior management to protect sensitive information while reducing business risk and meeting regulatory expectations, most IT organizations review available options and determine that PKI encryption satisfies these requirements.

After reviewing publicly available information about PKI encryption, an assumption may be made that in order to have appropriate control of the organization's public key infrastructure, an entire certificate authority must be implemented that is tied to an existing global root authority. "Global root authorities" require thorough background checks, attestations regarding intended use, and reviews of processes and procedures related to issuing subordinate end user certificates. Working from this assumption, an organization begins to isolate the requirements for implementing such an infrastructure and determines that this solution is too expensive due to the cost of software, equipment, and personnel.

The conclusion is based on a false assumption. Any public/private key pair can be used for encrypting sensitive data if encrypted with a key of sufficient length (1024 bits or longer suggested) and an algorithm of sufficient strength (Advanced Encryption Standard [AES] suggested). This will protect information from risk as long as the private key is held securely and managed with appropriate diligence.

**Myth two: Managing keys and certificates requires a lot of people and a lot of time.**

A common misperception of PKI is that the durability of the data protection resulting from PKI key-based encryption is associated with complexity. Many organizations believe that managing PKI keys requires a number of highly specialized resources to be focused solely on PKI infrastructure management. Many organizations feel they can't afford several full time equivalents just to establish and maintain a certificate authority to issue keys.

In reality, setting up an in-house certificate authority and using them to issue hundreds, even thousands of certificates and public-private key pairs, does not require a dedicated resource. Depending on the certificate authority vendor, configuring the application and establishing self-service key issuance web interfaces may take as little as a day and seldom more than a few days. Once the application is configured and the web forms published, administration consists primarily in monitoring exceptions reports and helping users learn when encryption should or must be used.

**Myth three: To manage keys, expensive software must be purchased with high ongoing maintenance costs.**

The way PKI key management applications (certificate authorities) have been sold to the market has resulted in a strong perception that software licenses and ongoing maintenance can be extremely expensive.

Below are three low-cost, simple to deploy alternatives to buying the more expensive PKI application licenses.

1. Use what is already available: SSL certificates. Most organizations are familiar with obtaining, managing, and using SSL certificates for encrypted server connections. This same type of certificate (or even the same certificates, depending on your security policies) can be used for other data encryption operations, such as file encryption in support of exchanging sensitive data.
2. Purchase end-user digital certificates from a managed service. Verisign, a leading provider of PKI out-sourced services, has offered a pay-as-you-go option for buying end-user certificates for some time and other vendors are entering the market. For a minimal fee, an end-user can be provisioned with a valid digital certificate and public/private key pair suited for encrypting sensitive data.
3. Leverage existing Operating System. Microsoft® Certificate Server is included as part of every Microsoft Server 2003 license and can be used to generate volumes of certificates and public/private key pairs for no additional charge. Microsoft Certificate Server comes with generic web forms that allow end users to obtain the encryption keys completely through self-service, decreasing labor support costs.

**Myth four: The only way to manage keys successfully is by placing them in hardware.**

There is a purist segment of the security community that supports the position that private keys used for decryption in PKI should only be managed in hardware to ensure that they are appropriately protected. This references the use of expensive computer cards or other peripherals that are dedicated to managing and protecting private keys so that once a private key is placed inside the hardware, it can never be removed. Such practices are appropriate when the private key is being used to digitally sign electronic files for the purposes of making legally binding commitments.

However, if an organization's goal is to protect information through encryption, such an approach is not necessary and could actually create complications. When public key encryption is used to facilitate exchanging data between organizations instead of individuals (as with large file tapes or transmissions), a "separation of powers" strategy is deployed. In this deployment, the private key is placed in a file or dataset location and is restricted to limited read/write access. Automated processes that must receive and decrypt the data for further processing are configured to find the private key in the specified location, and only a limited number of security professionals have access to the keys. These keys are audited frequently to ensure no inappropriate transactions are applied.

### Myth five: Managing keys requires a data center with robust physical security.

As referenced in Myth one, digital certificates and private keys can be used in processes wherein a digital signature becomes a legally binding authorization. In those situations, a high degree of diligence and protection for private keys is required to prevent cybercriminals or thrill-hackers from obtaining a private key for fraudulent purposes. Within this limited use, private keys may only be maintained in data centers that are manned 24 hours a day by human security guards, constant video surveillance of both those human guards and all entry/egress points, and other expensive physical safeguards.

This robust physical security may not be necessary for a certificate authority that is generating public/private key pairs intended for use by processes or individuals exchanging protected information. For this type of use, the recommended level of security for protecting certificate authority servers is commensurate with the same degree of diligence given to database or network operating system servers in order to prevent misuse. In addition to this level of security, audit processes are recommended if a Key Recovery Module, the secure repository that keeps copies of the private keys issued, is installed.

**Conclusion** An overview of the myths commonly associated with PKI reveals that there is more than sufficient evidence to persuade organizations that the barrier for adopting PKI for encryption purposes is much lower than previously identified. A review of PKI concepts also demonstrates that it provides much more durable security than passwords and is not nearly as complex as it is perceived to be. Considering both the myths and the durability of the security it provides, it is clear that using PKI and public/private key encryption is a data security best practice can be pursued by an organization without encountering high costs or over-use of valuable resources.

---

**About PKWARE** PKWARE, Inc., the largest global software company providing ZIP solutions, is the creator and continuing innovator of the ZIP standard. PKWARE products are used to ensure the security and portability of data internally, as well as with partners, across all major platforms. Hundreds of global organizations in financial services, banking, retail, healthcare, government, and manufacturing use PKWARE services daily. PKWARE products provide unmatched scalability, ease of use and deployment, making them the most cost-effective means of securing data and complying with industry regulations. PKWARE, a privately held company, is based in Milwaukee, WI with additional offices in New York, the United Kingdom and Japan.

© 2009 PKWARE, Inc. All rights reserved. PKWARE, PKZIP, SecureZIP, and SecureZIP Mail Gateway are trademarks or registered trademarks in the U.S.A. and other countries. Any other trademarks are used for identification purposes only and remain the property of their respective owners.

United States  
648 N. Plankinton Ave., Suite 220  
Milwaukee, WI 53203  
1.888.4.PKWARE  
www.pkware.com

UK/EMEA  
Crown House  
72 Hammersmith Road  
London W14 8TH  
United Kingdom

