Entrust® Securing Digital Identities & Information

3 elements that comprise a high quality PKI

…and how you can get it for less

November 2009

Documentation issue: 2.0

retweet this
Click here to post this on Twitter

Table of Contents

1 Introduction

Do you need to exchange information online securely? Do you need to turn on the security inherent in your existing applications? Do you need to authenticate users, devices, or applications? If so, you need a certificate.

Certificates, which contain a user's public key and identity, are issued and managed by an entity called a Certification Authority (CA). A CA is a component of Public Key Infrastructure (PKI)—the technology behind public-key encryption, authentication, and digital signature services—and is necessary to establish and maintain a trustworthy networking environment using certificates.

PKI systems, however, can be complex and time-consuming to deploy as well as expensive to operate and maintain. Furthermore, individuals with the necessary skill set required to run a CA are scarce, making it difficult to obtain and retain PKI-savvy staff. A PKI system also consists of many different features (often misunderstood), which organizations must decide to include or exclude, as they affect both PKI cost and quality.

So how can you obtain the services of qualified PKI staff, at a cost-effective rate, to quickly deploy security for your organization? Outsource your CA to Entrust Managed Services PKI.

This white paper examines the elements that comprise a high quality PKI and the advantages of outsourcing to Entrust Managed Services PKI.

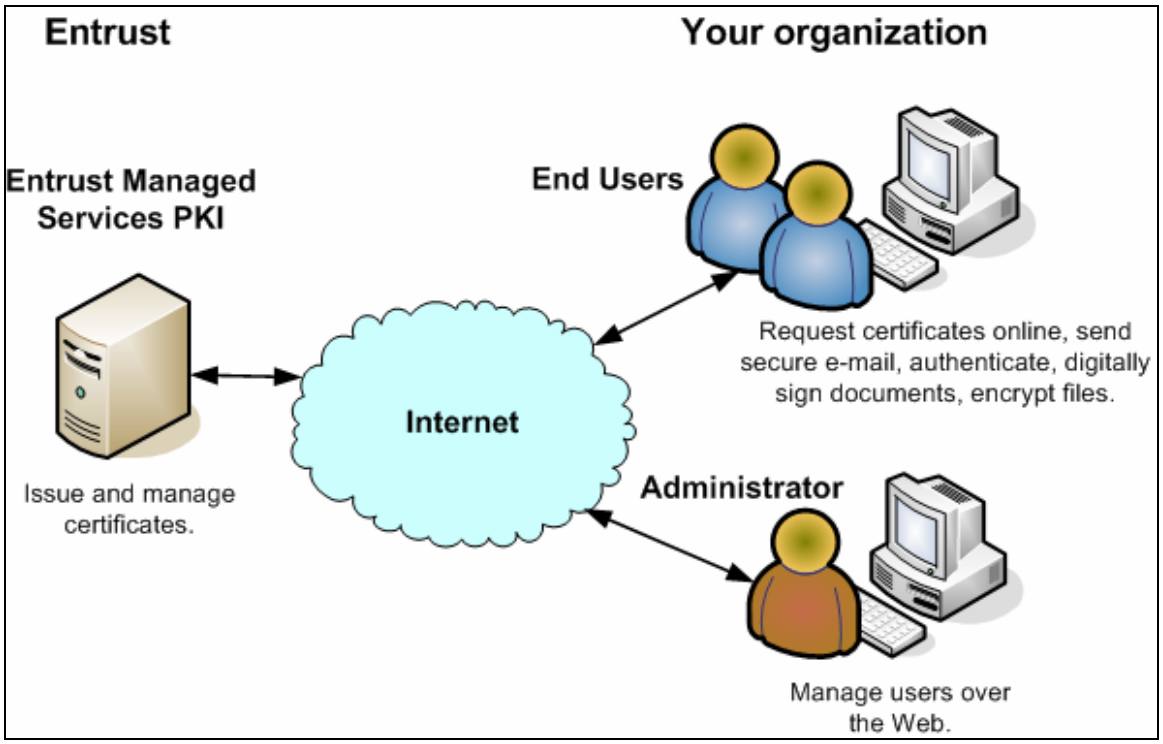
2 What is Entrust Managed Services PKI?

Entrust Managed Services PKI is a hosted certificate service that enables customers to quickly and easily request and manage user, application and device certificates over the Internet. The install, operation, maintenance, and monitoring of the PKI are handled by Entrust out of state-of-the-art secure facilities. With certificates users can secure applications such as Microsoft Office, Microsoft Outlook, remote access VPN and Adobe PDFs without requiring organizations to manage a PKI.

Flexibility of scale and certificate delivery options give you control to customize the solution. You can also configure the security policy for the initial and ongoing definition of various security parameters, such as key length, certificate lifetime, expiry, revocation, and recovery procedures, as well as manage the full lifecycles of certificate-based digital identities online.

As data breaches, identity thefts, and information loss continue to become commonplace, Entrust Managed Services PKI enables you to solve security challenges quickly, easily, and in a cost-effective manner.

Figure 1: Managed Services PKI architecture



3 What makes a PKI successful?

Certificates are used to deliver strong authentication, data confidentiality, and data integrity to a wide variety of organizations, from e-commerce to those just looking to streamline internal security. As a result of the medley of organizations using certificates for different purposes, needs and requirements in a PKI system vary.

However, regardless of differing PKI system needs and requirements, there are a number of key elements that all companies must consider when implementing a PKI. These key elements are what comprise a high quality PKI.

Key elements include:

- **System features**

  The following PKI system features are essential to implementing a high quality PKI solution:

  - High availability (HA) including monitoring
  - Secure facilities
  - Disaster recovery (DR)
  - Backups
  - Hardware Security Module (HSM)
  - Audits
  - Root key generation (RKG) ceremony

- **Solution features**

  The following solution features are essential to implementing a system that is effective, efficient, and easy to operate. Solution features make a PKI more valuable as a result of its increased usability: the solution is more scalable for future requirements and the system is easier to operate and maintain.

  - Cross-certification to establish trust relationships between multiple CAs
  - External certificate issuance (issuing certificates outside of your firewall)
  - Integration with existing applications
  - Scalability

- **Cost**

  Regardless of the number of certificates your organization requires, implementing a PKI system requires PKI-savvy resources, feature-rich PKI software as well as facilities that are appropriate for the level of risk you are trying to mitigate. To save money, many companies elect to exclude certain system features, such as disaster recovery or HSM private key storage. This cost-cutting practice, however, can drastically reduce the quality of a PKI.

  To save money without forfeiting quality, you should consider alternative PKI deployment options, such as outsourcing your PKI. Outsourcing your CA to Entrust Managed Services PKI provides significant cost savings benefits. In addition, the system features included in the Entrust Managed Services PKI base offering far exceed what many companies would be willing to spend if implementing their own CA in-house.

4 System features

To have a high quality PKI—one that is continuously operational, secure, redundant, tamper-proof, accountable and trustworthy —the following system features are necessary:

- High availability
- Secure facility
- Disaster recovery
- Backups
- Hardware Security Module
- Audits
- Root key generation ceremony

The importance and value of each system feature is described in detail below.

4.1 High availability (HA)

An important factor in operating a PKI solution is to ensure the system is reliable and continually operational over a specified period of time. This is called high availability (HA). Incorporating a HA strategy ensures your business is not affected due to hardware or software failures. Any system downtime can cost money in lost business or increased security risk. HA is essential, especially during peak hours when there is an increased load on the system.

Costs attributes of HA include:

- Secondary servers for high availability of the CA, database, and directory
- Configuration possibilities include two servers and one Storage Area Network (SAN).
- Training courses to devise an HA architecture
- Operating system
- HA software
- Redundant Hardware Security Module (HSM) to allow operation in the event of a single HSM failure

The Entrust Managed Services PKI includes a high availability strategy within its base offering. At Entrust, HA consists of 99.5% uptime and 24/7 operation. This includes multiple secondary servers (two at the main site and one at the disaster recovery site): CAs, networks, Internet links, hardware security modules, and databases.

HA is a feature that companies tend to overlook solely as a result of the expense. However, HA is indispensible to keeping your system continuously operational and at maximum efficiency, which is why it is included in the Entrust Managed Services PKI base offering.

4.2 Secure facility

Physical security is another crucial element in deploying a successful PKI solution. This involves separate and secure facilities to house one or more certification authorities (CA).

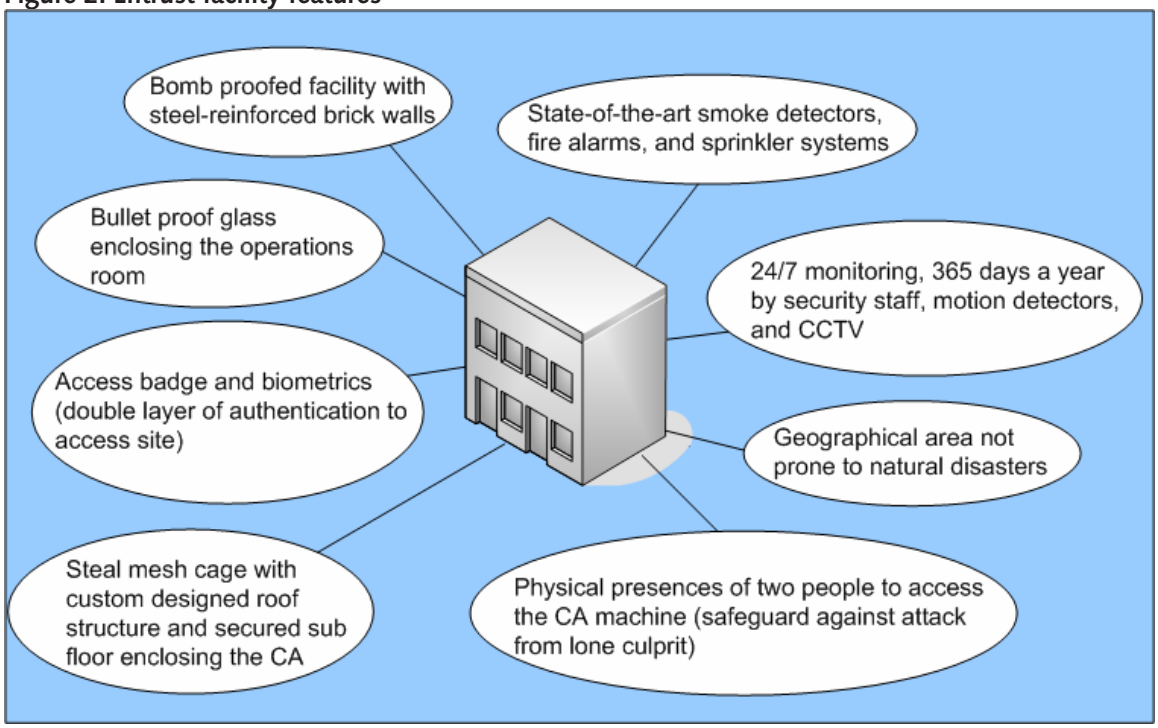
The CA issues certificates and securely binds the names of users to their public keys, so it must be kept in a secure facility to prevent fraudulent creation of certificates. This involves secure physical access to the facility (card reader access), fire and alarm systems, a safe for key information, and bonded security staff. A document outlining all procedural controls, such as the role and authentication requirements required to perform sensitive CA functions, is also necessary for the security of the CA.

Costs attributed to secure facilities include:

- Finding a location
- Electricity
- UPS
- Backup generator
- Air conditioning
- Card reader for securing the server room
- Racks, wiring, servers, phone
- Fire and alarm systems
- Safe for key information storage

The Entrust Managed Services PKI includes secure facilities within its base offering. Entrust has partnered with Savvis, a leading hosting provider worldwide, for secure infrastructure facilities, allowing Entrust to provide unparalleled physical security.

Figure 2: Entrust facility features



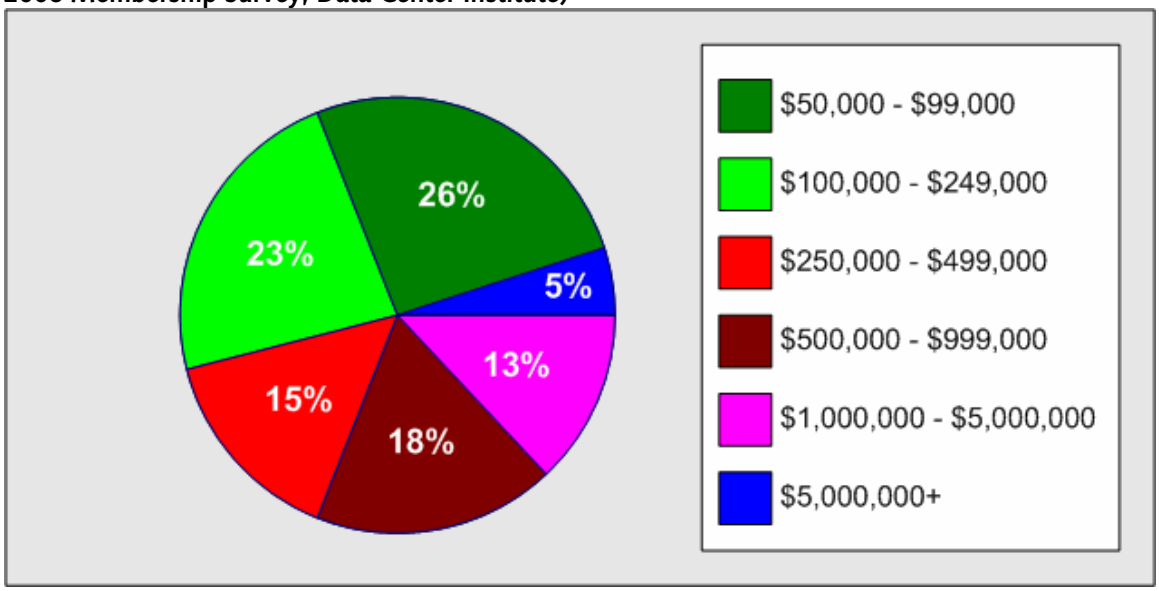
4.3 Disaster recovery (DR)

Disaster recovery (DR) is a crucial element of a successful PKI, as it ensures that your system can continue to operate in the event of a catastrophe affecting the building housing the CA at the primary site. A Disaster Recovery Plan (DRP) establishes procedures to recover a PKI following a disruption. This is achieved through backup systems, which are configured to assume the duties of the original server when required. Without a DR strategy, a system failure leads to unplanned downtime, which can cause revenue losses, reduced productivity, and compliance and/or reporting penalties. It can also damage partner relationships and organization reputation (Forrester Research, Inc., 2007).

A DRP establishes procedures to recover the data, hardware, and software critical for business operations after a catastrophic disruption. According to the AFCOM 2006 Membership Survey, 77.4% of companies have declared at least one business disruption affecting the organization's ability to continue business-as-usual in the past 5 years (such as loss of power or cooling, fire or water damage, natural disasters, bomb threat, terrorism, employee error or sabotage, data loss, or security breach).

As Figure 3 illustrates, the cost of downtime is staggering and therefore dictates the importance of a DR strategy.

Figure 3: Hourly cost of downtime (source Association for Computer Operations Management 2006 Membership Survey; Data Center Institute)



Costs attributed to DR include:

- Replication of all facilities expenses (DR requires a separate location)
- Hardware expenses for servers and networking gear

Entrust provides disaster recovery as part of the Entrust Managed Services PKI base offering. This includes redundant servers, database, ISPs, telecommunications, and 24/7 disaster recovery backup at remote secure site. In addition, Entrust validates DR capabilities through testing and audits to ensure that your sensitive data remains secure should a disaster strike.

4.4 Backups

Database backups ensure that data is never lost in the event of a total failure. A loss of database information would be catastrophic for the following reasons:

- Loss of archived decryption keys

  Without a decryption key, you cannot decrypt past encrypted data—the information can never be accessed again.

- Loss of CA key use

  Without use of the CA key, you cannot issue revocation lists, leaving relying parties to either ignore revocation lists, which is a security issue, or not accept signatures and encryption certificates (client dependent).

- Loss of the CA

  The loss of the CA means the CA has to be recreated, thus incurring the cost of another CA setup, key generation ceremony and associated audit cost—approximately $90,033. In addition, all users, as well as applications using certificates such as VPN devices, will have to

be re-enrolled into the new CA. While this is all occurring, your service is down and, as discussed in the Disaster recovery (DR) section above, downtime is extremely costly.

The cost of implementing backups must be included when building your PKI solution.

When considering implementing backups into your PKI system, you should ensure your backup solution meets the following requirements:

- The backup system takes scheduled (periodic) snapshots of the database and logs so that you can recover as much as your data as possible.
- The backup system takes incremental backups and/or logs to ensure no data is lost in the event of a failure between scheduled backups.
- The backup is restored to the repaired hardware.
- The backups are tested on a periodic basis to ensure the backups are usable and not, for example, an empty file.
- The backup system should be automated to avoid human error in missing a backup.

You should also store your backups in an offsite location, in the event of a disaster at the main site.

With Entrust Managed Services PKI, all the above requirements are satisfied and are included in the base offering.

4.5 Hardware Security Module (HSM)

An HSM is used to provide a secure location to generate and store the CA signing (private) key in an encrypted state (unlike server software storage, where the private key is in active memory and in an unencrypted state, making it more available to tampering). The private key used to sign certificates never leaves the HSM. Rather the CA sends the HSM the certificate to sign with the CA private key. Protecting private keys in specialized, tamper-resistant hardware provides increased protection against unauthorized issuance of fraudulent certificates.

With Entrust Managed Services PKI, your CA keys are stored in a tamper proof hardware security module as part of the base offering.

4.6 Audits

Auditing is an integral part of any PKI system. Regular audits are a way to determine whether policies and procedures established by an organization are being implemented as outlined in the Certificate Policy (CP) and Certificate Practices Statement (CPS). Any recommendations received from audits allow companies to adjust policies and practices to improve their security framework.

Entrust Managed Services PKI includes external third-party audits as part of the base offering to verify the CP and CPS are followed and that customer data is protecting as per established policies.

4.7 Root key generation (RKG) ceremony

The secure creation of the root key, or private key, is an integral part of the entire PKI system, as it ensures the digital certificates, which it signs, are trustworthy. If absolute trust in the root CA key does not exist, the PKI system cannot be trusted either. A root key generation (RKG) ceremony affirms that an organization's policies are followed and that no anomalies occurred that might later impugn the integrity of the root CA key. This ensures that the root key cannot be stolen to sign fraudulent certificates by someone posing as someone other than themselves.

A RKG ceremony is an important step in establishing trust with another organization's CA through a cross certificate.

Costs attributed to an RKG ceremony include:

- RKG scripts (detailed procedural steps that are executed and audited)
- Auditor costs to witness the generation and HSM storage of the CA private keys
- People costs for testing the RKG, running through the scripts, and conducting a smaller RKG at the DR site

Entrust Managed Services PKI includes the execution of a RKG ceremony within a secure vault in the base offering.

5 Solution features

Another aspect of a high quality PKI is its solution features. These solution features increase the value of the PKI by increasing its usability.

A highly usable PKI system involves one that allows you to easily:

- Cross-certify with other Certification Authorities, including those outside of your private domain
- Issue certificates outside your firewall, including external employees or business partners
- Integrate with existing applications to turn on security features inherent to the applications
- Scale your solution to respond to organization growth

Each solution feature is explored in detail below.

5.1 Cross-certification

Cross-certification extends trust relationships between different Certification Authority (CA) domains. To accomplish cross-certification, two CAs securely exchange and sign each other's verification keys, which are used to verify the CA's signatures on end-user certificates. Then, during an exchange between users on different CAs, the cross-certificate is used to verify the trustworthiness of a user certificate signed by the cross-certified CA.

However, prior to cross-certifying, organizations must thoroughly investigate each other's policies to ensure they are meeting legal standards and can therefore be considered trustworthy. This includes, but is not limited to, examining the following:

- Certificate Policy (CP) and Certificate Practices Statement (CPS)

  You must examine the organization's CP—a high-level document that describes how the CA operates, what a certificate should be used for and the responsibilities for requesting, using, and handling the certificates and keys—and CPS—a document that describes how a CA implements a specific CP in the context of the operating policies, system architecture, physical security, and mechanisms and procedures used to achieve the security policy. It is also important to determine whether these documents meet the RFC 3647 standard.

- Pre-issuance identity vetting policies

  You must examine the organization's policies, rules, and mechanisms surrounding identity authentication and verification of potential credential recipients.

- Private-key protection policies

  You must examine where the organization stores their CA's private key, as well as the keys of any subordinate or trusting CAs, and determine whether it meets FIPS 140 and, if so, at what security level.

- CA and directory architecture

  You must examine the organization's CA architecture (this includes any subordinate or trusting CAs of the principle CA) and directory architecture for interoperability purposes.

- Auditing practices

  You must examine the organization's auditing practices for the principle CA or any subordinate or trusting CA, including who performs the audits and the audit frequency. You must also obtain the latest auditing report to verify compliance.

Individuals representing the different CAs must also sign legal agreements, which state the domain security policy and provide assurance that all outlined security policies will be followed.

Cross-certification can be very time consuming as it involves investigation of another CA's trustworthiness as well as information gathering to satisfy requirements of the cross-certifying CA organization. It also requires an audit. Third-party audits cost $90,033 per year (see True cost of PKI ownership for more information). Furthermore, the owners of the CA with which you want to cross certify may impose policies on your operation that can be expensive to rationalize with your existing operation.

Entrust Managed Services PKI can handle the burden of investigating another CA for cross-certification, and modifying your policies to meet the demands of the owners of the other CA. For example, your Certification Authority can be cross-certified with Entrust's public trust networks such that certificates issued under your CA are trusted by Web browsers without any pop up security dialogs.

5.2 External certificate issuance

With an internal CA, digital signatures, authentication, and encryption work effectively within the organization, because internal users have ready access to the CA through the internal network. However, in order for extranet users, such as partners or citizens, to decrypt documents or verify signatures from your organization, they need the following:

- Access to a User Interface (UI) to enroll for a certificate
- Access to other users' certificates to encrypt data for them
- (optionally) Access to PKI software for certificate management

The cost required to configure external certificate issuance is considerable due to its complexity: significant effort is required.

Entrust Managed Services PKI provides the ability to issue certificates outside of your firewall quickly and easily. External users navigate to an Entrust Web application where, with the click of a button, they can obtain the certificates necessary to communicate with your organization securely. There is no learning curve and no technical knowledge required. Best of all, the required certificate is obtained quickly so as not to upset business continuity.

5.3 Integration with existing applications

A revealing measure of PKI usability is the ability to seamlessly integrate your certificate with your existing applications. In order for an in-house CA to accomplish this, proprietary PKI software may be required on each desktop and may be limited to integrating with vendor-specified software applications.

With Entrust Managed Services PKI, no client-side software is required. Certificates seamlessly integrate with the majority of commercial off-the-shelf (COTS) applications, such as Microsoft Office and VPNs, using Microsoft's crypto framework. There is no need to invest in additional resources or alter current practices.

Note: For applications not part of the Microsoft framework, Entrust provides toolkits to reduce the cost of building your own fully automated solution. For more information on toolkits, see http://www.entrust.com/pki/toolkits.htm.

In order to create an account and enroll for a certificate without installing client software, Entrust Managed Services PKI provides access to two flexible, zero footprint Web-based applications: one for administrators and one for users. Your organization can decide how much control to provide users over their Entrust digital ID enrollment and account management; for example, new users can enroll for a certificate with or without administrator approval.

Administrators and users can perform the following tasks through the Web-based applications:

Table 1: Entrust Authority Administration Services Web-based applications

User Management Service (Administrators)	***User Registration Service (Users)***
Approve pending requests	Register for a digital ID
Create accounts (individual and in bulk)	Create a digital ID
Edit accounts	Recover a digital ID
Reset accounts	Manage account -Reset account -Revoke account -Put account on hold -Remove hold -Change registration password -Show activation codes for digital ID enrollment
Deactivate and reactivate accounts	
Search accounts, requests, and audits	

Entrust Managed Services PKI does offer the Entrust Entelligence Security Provider client (for Windows and Mac), should you desire fully automated certificate enrollment. Security Provider provides additional features and benefits, thereby providing significant value to your organization.

In addition, Security Provider also offers a plug-in for Microsoft Outlook. Entrust Entelligence Security Provider for Outlook delivers capabilities that simplify the delivery of secure messages from the sender to the recipient's desktop, over what Microsoft provides in Microsoft Outlook.

Table 2 shows how Security Provider adds value to your PKI:

Table 2: Security Provider benefits

Benefits	*Description*
Automatic certificate renewal	Provides automatic certificate renewal before expiry and silently updates desktop applications using the new certificate. For users, there is no downtime or confusion about expired keys.
Certificate management	Manages user's certificates on a desktop or smart card.
Key history management	Provides an independent key store for improved user experience. As keys are renewed or changed, the old keys are securely kept so that documents encrypted with old digital IDs can be decrypted months or years later.
Permanent decryption of Oulook email	Gives users the option to permanently decrypt files in their Outlook inbox for easier viewing and searches.
Recipient certificate caching	Caches recipient certificates on the local computer so users can still compose e-mail offline.
Portability	Users can easily export their certificate and copy it to a laptop or home computer for temporary use.
Password protection for certificates	Protects certificates with a password so that no one else can use them.
Secure connection with Entrust Managed Services PKI	Opens and maintains a secure connection whenever it needs to communicate with Entrust Managed Services PKI.
Support for non-repudiation	Generates the key pairs used for digital signatures and ensures that the signing keys are never backed up and remain under the users' control at all times.
Automatic update of key pairs	Automatically updates the certificate on the user's computer if you change the user's distinguished name (DN) by creating new key pairs.
Automatic certificate association	Automatically associates keys and certificates with various applications, including Microsoft Outlook and a variety of VPN clients, so users do not need to manually set up certificate association after initial enrollment or subsequent key updates.
Certificate revocation	Includes a built-in Online Certificate Status Protocol (OSCP) client to check the revocation status of digital certificates; so there is no need to purchase, deploy, and maintain a separate OSCP client. The Entrust OSCP client provides logging across Windows XP and Vista to help with troubleshooting.
Full certificate path validation	Provides NIST approved full certificate path validation in a bridged or cross-certified PKI environment. You can trust that the identity claimed in a digital signature is authentic, and that the identity was issued by a trusted authority and is valid for the intended use. This reduces risk and ensures the trust required for PKI-secured transactions.
Automatic key association	Automatically associates keys and certificates with various applications, including Microsoft Outlook and a variety of VPN clients so users do not need to manually set up certificate association after initial enrollment or subsequent key updates.

5.4 Scalability

From an efficiency standpoint, scalability is important in a PKI solution, as it allows you to quickly respond to growth within your organization exactly when required. It is very difficult to scale a PKI after the fact.

While an exact cost cannot be determined for PKI scalability, it may require a large upfront investment to ensure the solution can adapt to organization growth. This may involve:

- Hardware capable of increasing its load
- Additional software licenses
- HA and DR strategy
- Facilities outfitted to handle growth
- Additional support and PKI expertise

With Entrust Managed PKI, you can grow your PKI solution on demand, as your organization grows. You only purchase as many certificates as required by your organization at the present moment. As your organization increases in size, you can purchase additional certificates to meet demand.

6 Cost

Now that we have looked at all the possible features of a PKI, lets look at how to do it cost effectively.

An important element that comprises a successful PKI is its total cost. If an organization is over-paying for its PKI at the expense of its core business, the PKI is unlikely to be considered a successful one.

6.1 Determining PKI requirements

If your organization cannot tolerate downtime or take any chances with internal attacks or security breaches, you need a PKI that includes:

- High availability (HA), disaster recovery (DR), and backups to avoid downtime
- Hardware Security Module (HSM), root key generation (RKG) ceremony, audits, and security facilities to protect from internal and external attacks

Deploying a high quality PKI—one that includes HA, DR, backups, HSM, RKG, audits, and secure facilities—is expensive, both in terms of money and time. However, cutting corners will not allow you to provide the level of security required.

In order to save money without forfeiting quality, consider outsourcing your PKI to Entrust Managed Services PKI.

6.2 True cost of PKI ownership

To illustrate the cost-saving benefits of outsourcing your PKI to Entrust Managed Services PKI, Entrust conducted a total cost of ownership analysis.

Entrust examined two organizations with differing needs in order to provide a fair total cost of ownership assessment. The total cost does not include the cost of a test system (the non-production system), which is used to test various upgrades and patches. A test system may involve a total

replication of your CA (full set of features), or just the CA itself. Whatever the extent of the test system, you should be aware that it adds to the total cost of PKI ownership. With Entrust Managed Services PKI, all upgrades and patches are first tested on a non-production machine.

The business requirements for each company in the total cost of ownership analysis are outlined below.

Note: For an in-depth review, see *Why outsourcing your PKI provides the best value: A total cost of ownership analysis* available from the Managed Services page on the Entrust Web site: www.entrust.com/managed_services.

Table 3: System features for Company A and Company B

System features	*Organization A*	*Organization B*
High availability (HA)	√	
Hardware Security Module (HSM)	√	√
Secure facilities	√	
Disaster recovery (DR)	√	
Backups	√	
Audit	√	
Root key generation (RKG)	√	
Backups	√	

6.3 Cost of deploying an internal PKI

The following sections reveal the costs associated with deploying an internal PKI for Organization A and Organization B.

Note: Costs exclude software license and support fees for the CA, directory, and databases.

One-time cost

One-time cost refers to the initial setup fee required to deploy an internal PKI for a three-year standard term.

Table 4: One-time cost

Item	*One-time cost*	
	Organization A	Organization B
Planning and assessment	$124,600	$25,600
Facilities	$40,800	$2,500
Hardware and software	$85,900	$39,000
Installation and configuration	$67,600	$42,100
Disaster recovery	$96,800	$23,400
Backups	$10,000	$0
Root key generation	$95,100	$0
Audits	$0	$0
Maintenance and operations	$4,000	$0

TOTAL	$524,800	$132,600

Annual cost

Annual cost refers to the expense of maintaining an internal PKI each year.

Table 5: Annual cost

Item	*Annual cost*	
	Organization A	Organization B
Planning and assessment	$0	$0
Facilities	$0	$7,000
Hardware and software	$16,020	$6,820
Installation and configuration	$0	$0
Disaster recovery	$8,420	$3,800
Backups	$10,000	$0
Root key generation	$0	$0
Audits	$50,000	$0
Maintenance and operations	$147,804	$45,500
TOTAL	$232,244	$63,120

Per year cost

Per year cost refers to the one-time cost + the annual cost multiplied by the three year deployment, divided over a three year deployment period.

The formula is as follows:

```
<one-time cost> + (3 x <annual cost>) / 3
```

Table 6: Per year cost

Formula	*Organization A*	*Organization B*
<one-time cost> + (3 x <annual cost>) / 3	524,800 + (3 x 232,244) / 3	132,600 + (3 x 63,120) / 3
Per year cost	$407,177	$107,320

6.4 How you can save with Entrust Managed Services PKI

If you currently do not have a full-featured CA—one that includes high availability, disaster recovery, backups, audits, hardware security module (for private CA key storage), and a separate facility to house your CA—we provide these features in our base offering for a lower price than what you are paying for your less-secure CA today. You improve the security of your CA and can save up to 20%. This added protection also reduces the large costs associated with system downtime, data loss, and data tampering. Entrust Managed Services PKI offers cost savings and cost avoidance.

If you already have a full-featured, secure CA, and need to upgrade your hardware or software, we can offer major savings while maintaining or improving the security of your CA. We do this by sharing processes, tools, and facilities as well as by assuming the maintenance and operations duties—the largest expense in PKI ownership. For a 5,000 user service, Entrust Managed Services PKI can save you up to 80% of the cost of building your own PKI and up to 60% of the cost of competing services.

7 Why Entrust Managed Services PKI provides the best value

Entrust Managed Services PKI provides the best value for the following reasons:

- Cost savings

  Entrust Managed Services PKI is less expensive (*up to 80%) than deploying your own internal Certification Authority (CA).
  *based on 5,000 users

- Cost avoidance

  Entrust Managed Services PKI provides a highly scalable solution. You only pay for what you need at the present time. Furthermore, with better than 99% uptime and a top notch disaster recovery strategy, you can avoid the high cost associated with downtime.

- Efficiency

  Entrust Managed Services PKI dramatically improves time-to-market. Also, with Entrust's high performance architecture, which is tested to enroll more than 1,000 users per hour, you can increase the speed at which you enable users to conduct business securely.

- Effectiveness

  By outsourcing your non-core business operations to Entrust, you can focus your efforts on maximizing efficiency and offering more products and services.

- Increased security

  Entrust Managed Services PKI operates according to established best practices including the use of HSMs to protect the CA private key and the use of staff background checks and security clearances. Entrust has partnered with Savvis, a leading hosting provider worldwide, for secure infrastructure facilities. These best practices around operations and facilities are audited by a professional auditing firm.

- Flexibility

  Entrust supports migration from a service model to an in-house model – and vice versa – and leverages the same enhanced security solutions to help protect your investment in security and offers alternatives as requirements evolve and business expands.

- Brand value

Entrust is an acknowledged leader in PKI, embracing a lead role in securing digital identities and information. With Entrust, you can be certain you are teaming with the best in the industry.

8 Conclusion

Entrust Managed Services PKI does not believe organizations should compromise their security in order to save on cost, or pay too much to deploy a PKI system when there are less-costly ways to achieve your security goals. When you outsource your PKI to Entrust, not only are you getting a high quality PKI for a significantly reduced cost, but you are employing a company that is:

- Recognized by government, national defense, finance, and industry leaders for unequalled PKI deployment experience
- Deployed in e-governments worldwide
- Evaluated annually against the FIPS 140 and Common Criteria standards
- Audited by and external third part auditor
- Authorized to offer certification cross-certified with the U.S Federal Bridge

All the elements that comprise a high quality PKI—rich system features, maximum usability, and low cost—are offered by Entrust Managed Services PKI. Plus, we beat our competitors pricing by up to 60%!

By outsourcing your non-core business operations to Entrust, you can focus your efforts on maximizing efficiency and offering more products and services.

9 About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,692 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.