Entrust® Securing Digital Identities & Information

Why outsourcing your PKI provides the best value

A Total Cost of Ownership analysis

July 2009

The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Table of Contents

1 Introduction

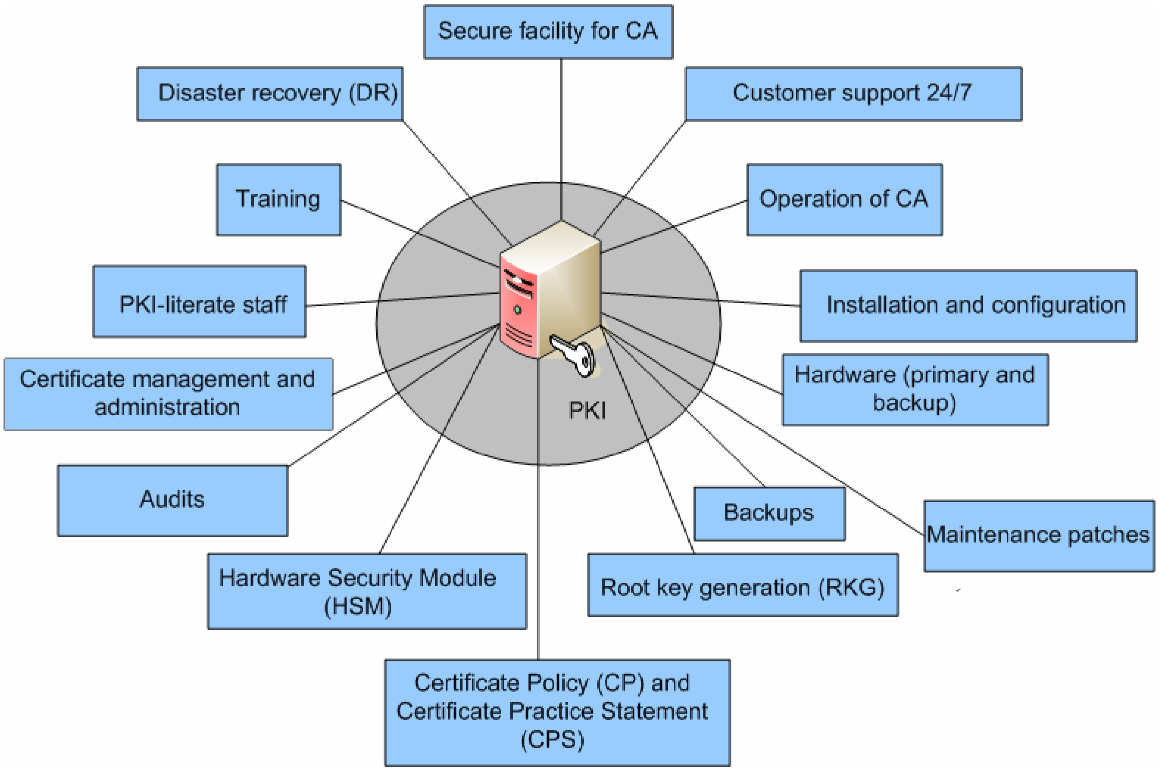
Once you conclude that you need a certificate to exchange information online securely, turn on the security inherent in your existing applications, or authenticate to users, computers, VPN, the Web, or buildings, the next point of determination is: how can I do this cost-effectively without forfeiting quality?

The answer is simple: outsource your Public Key Infrastructure (PKI).

Why should you consider outsourcing rather than deploying an in-house Certification Authority (CA)?

An internal CA can be expensive to deploy, operate, and maintain. Organizations require knowledgeable staff, a formal and binding set of policies and procedures, secure facilities, hardware that meets future extensibility requirements, and PKI software to create and manage certificates, to name a few. A complete solution also requires high availability to prevent costly downtime, disaster recovery if the main building housing the CA experiences a catastrophic event such as a fire, backups to ensure data can be retrieved in the event of a total failure, a hardware security module (HSM) for private key storage, and comprehensive external audits to validate security procedures.

Figure 1: Cost considerations when deploying an internal PKI


Secure facility for CA
Disaster recovery (DR)
Customer support 24/7
Training
Operation of CA
PKI-literate staff
Installation and configuration
Certificate management and administration
Hardware (primary and backup)
PKI
Audits
Backups
Maintenance patches
Hardware Security Module (HSM)
Root key generation (RKG)
Certificate Policy (CP) and Certificate Practice Statement (CPS)

This total cost of ownership white paper examines the cost of deploying an internal CA and the value of outsourcing your CA to Entrust Managed Services PKI. Entrust Managed Services PKI provides a more complete and value-added solution than other vendors offering a subscription certificate service.

2 Exposing the total cost of ownership

Often organizations fail to examine the hidden costs associated with Public Key Infrastructure (PKI) ownership, focusing much attention on the price of the PKI software that creates and manages certificates. While Microsoft, for example, bundles PKI software for free with Windows Server 2003, the overall cost savings is minimal at best—software is an incidental cost of owning and operating a successful PKI. Failing to consider all the costs upfront may lead organizations to deploy in house, which, in actuality, is much more costly than outsourcing your CA.

To assist you in determining the total cost of operating and managing an internal CA, Entrust reviewed all elements involved in PKI ownership and assessed the cost of each.

3 Assumptions

To fairly evaluate the cost of deploying an internal CA, Entrust makes some assumptions. These are listed and explained below.

3.1 Deployment type and system inclusions

To provide an accurate assessment, Entrust evaluated the cost of a PKI system based on two companies with different requirements for a PKI system. For the purposes of this study, they are labeled Organization A and Organization B.

Table 1: System features for Organization A and Organization 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)	√	

The business requirements for each organization are outlined below.

Organization A

Organization profile	*Business requirements*	*System features needed*
Conducts a large number of continuous transactions	“We want a system that is continuously operational. Because we conduct such a large number of transactions on a constant basis, we cannot tolerate any downtime.”	**High availability (HA)** HA ensures a certain absolute degree of continual operation of the CA, thereby preventing any business interruptions. HA is necessary for servers, database storage, networks, Internet, and Hardware Security Modules (HSM). **Disaster recovery (DR)** HA and DR are closely tied, as in

		order to remain continuously operational during a disaster, the system needs to transfer operations to a backup or disaster recovery system.
Conducts high value transactions	“We want a system that securely backs up all data. Because we conduct high value transactions, we cannot afford to lose any data.”	**Backups** Backups ensure that data can be retrieved in the event of a failure. **Audits** Among other benefits, audits verify that operators back up data and test the backups according to policy.
	“We want a system that prevents the creation of fraudulent certificates. Because we conduct high value transactions, we could lose a lot of money if anyone issued and used a fraudulent certificate to perform real transactions.”	**Hardware Security Module (HSM)** An HSM provides a secure location to generate and store the private key in an encrypted state in order to prevent the creation of fraudulent certificates—even by your own employees.
	“We want a system that issues trustworthy and accountable certificates. Because we conduct high value transactions, we could lose a lot of money if the integrity of our certificates is compromised.”	**Root key generation (RKG)** RKG ensures the root key, which is the heart of your trusted system and used to sign digital certificates, is securely created (without the insertion of malware into the software install). Secure creation of the root key ensures the integrity of the root key.
	“We want a system that physically secures the CA from internal attacks. Our employees have insider knowledge of the organization and are aware of the value of our transactions. We need to ensure the CA is well protected.”	**Secure, separate facilities** Secure facilities provide physical security of the CA, which issues certificates and securely binds the names of the users to their public keys. Physical security minimizes the risk of tampering with day-to-day operations so as to ensure trustworthy certificates.
Conducts business with external partners	“We want to extend trust relationships with people outside our internal domain through cross-certification.”	**Audits** Audits verify that an organization is in compliance with its Certificate Policy (CP) and Certificate Practices Statement (CPS). Once cross-certified, audits

		are necessary to verify compliance with the policies imposed by the cross-certified CA. Audits are necessary for cross-certification initiatives.

Organization B

Conducts a small number of transcations that are not time critical	"We are not concerned with the system being up and running continuously. Because we conduct a small amount of transactions, we can tolerate the system being down for days."	A system without high availability or disaster recovery provides the right level of operation based on organization requirements.
Conducts low value transactions	"Although we conduct low value transactions, we do not want to lose any of our data."	**Backups** Backups ensure that data is retrievable in the event of a failure.
	"We trust the CA was securely installed, but because several employees will maintain the CA over a long period of time, we want to increase system security to prevent the creation of fraudulent certificates. Because we conduct low value transactions, it's not so much about losing money as much as it is about damaging our brand should anyone issue and use a fraudulent certificate to perform real transactions."	**Hardware Security Module (HSM)** HSM provides a secure location to generate and store the private key in an encrypted state and mitigates the risk of anyone creating a fraudulent certificate.
	"Because of the low value of our transactions and the low frequency at which those transactions occur, we are not concerned with getting our certificates certified as trustworthy. We are not changing the nature of our business or	Since this organization only performs a minimal number of low value transactions within their own domain, it is not essential to perform a root key generation (RKG) ceremony. RKG ensures the integrity of the root key and is necessary for cross-certification purposes.

	expanding our business outside our own domain."	
	"We are not concerned with physically protecting the CA from internal attacks. The value of transactions and risk of attack is too low. We trust our employees."	A secured room or locked cabinet inside the organization's existing building provides the right level of security based on requirements.
Does not conduct business with external partners	"We do not need to extend trust relationships with people outside our internal domain."	Since this organization does not need to extend trust relationships outside their internal domain, audits, which verify that an organization is in compliance with their Certificate Policy (CP) and Certificate Practices Statement (CPS), are not essential. **Note**: If outsourcing a PKI, audits are recommended, as a way to verify the outsourcer is complying with the policy to which you agreed.

This white paper provides a total cost of ownership for Organization A and Organization B, which have different system features. This allows you to compare your organization based on the system features you would include if running your own PKI.

3.2 Numerical assumptions

All US dollar amounts cited in this white paper came from a variety of credible sources, so as to be as accurate as possible. Sources include:

- Vendors
- Entrust Professional Services
- Facilities managers
- Trade professionals
- Auditors

The least expensive options and vendor discounts are used where applicable.

Internal staff costs are based on a typical loaded labor rate and external consultant costs are at the low end of the price range.

3.3 Value metrics

This total cost of ownership white paper provides cost figures based on the average dollars per year. A year-by-year cash expenditure involves too many unknown variables, such as organization growth. The average dollars per year is based on a three-year time horizon, which is a common depreciation time frame.

3.4 Excluded costs

This total cost of ownership white paper only provides cost items inclusive to providing a certificate, and does not include application usage of the certificate.

In addition, to account for the low license cost of open source PKI software and Microsoft CAs, Entrust assumes the PKI license and support costs are $0.

4 Total cost of running an internal PKI

The following sections reveal the costs associated with deploying an internal PKI for the different deployment types outlined in section 3.1: Deployment types and system inclusions.

Detailed estimates are provided so you can compare the cost of running an internal PKI and outsourcing your PKI to Entrust. You can also compare the Entrust Managed Services PKI package and cost to other vendors.

This section examines:

- One-time costs
- Annual costs
- Per year costs

Note: As mentioned previously, costs exclude software license and support fees for the CA, directory, and databases.

4.1 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 3: 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	$81,800	$37,900
Installation and configuration	$67,600	$42,100
Disaster recovery	$92,700	$0
Backups	$27,600	$7, 700
Root key generation	$95,100	$0
Audits	$0	$0
Maintenance and operations	$4,000	$0
TOTAL	$534,200	$115,800

4.2 Annual cost

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

Table 4: Annual cost

Item	*Annual cost*	
	Organization A	Organization B
Planning and assessment	$0	$0
Facilities	$0	$7,000
Hardware and software	$14,200	$6,100
Installation and configuration	$0	$0
Disaster recovery	$7,600	$3,800
Backups	$21,900	$6,520
Root key generation	$0	$0
Audits	$50,000	$0
Maintenance and operations	$147,804	$45,500
TOTAL	$241,504	$65,120

4.3 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 5: Per year cost

Formula	*Organization A*	*Organization B*
`(<one-time cost> + 3 x <annual cost>) / 3`	(534,200 + 3 x 241,504) / 3	(115,800 + 3 x 65,120) / 3
Per year cost	$419,571	$103,720

4.4 Detailed account of internal PKI expenses

This section provides a detailed breakdown of the costs associated with running an internal CA.

Planning and assessment

An organization must plan for implementation based on organizational needs and requirements. This includes:

- **Training staff members**: Staff training is required for PKI and PKI-related components, such as the database, HA, HSM, certificate policy settings, and certificate lifetime. External training with the PKI vendor, and travel to the vendor's training facility, is also required to understand proprietary software.

- **Determining deployment architecture**: This includes: determining a network topology that maps to server needs; determining needs for high availability, DMZ, and redundancy; and determining the platform (UNIX or Windows). The deployment architecture is critical to get right and likely requires an expensive consultant to travel to your location.

- **Creating Certificate Policy and Certificate Practices Statement documentation**: A Certificate Policy (CP) is a high-level document that describes how a PKI operates. It describes the operation of the CA, as well as the responsibilities for requesting, using, and handling the certificates and keys. A Certificate Practices Statement (CPS) is a high-level document that describes how a CA implements a specific CP by specifying the mechanisms and procedures used to achieve the security policy. Both documents are required to maintain the integrity of the CA and attain accountability. Travel is often required to obtain several CP/CPS reviews and this documentation is audited.

  You can create a CP/CPS based on a template available from the Internet or purchased from a third party.

- **Hiring a PKI consultant**: A PKI expert is needed for knowledge transfer and reviews of architecture documents and CP/CPS documentation.

Table 3: Planning an assessment costs for an internal CA

Description	*Per year cost (over 3 years)*	
	Organization A	Organization B
Read PKI architecture documents and white papers	$3,500	$2,333
Gain knowledge of database and backup routines	$1,167	$1,167
Learn and work with high availability	$2,333	N/A
Learn and work with HSM	$2,333	N/A
Training courses, including Microsoft high availability	$3,333 (includes Microsoft HA @ $2,500/week)	$1,667
Travel (for training)	$2,667	N/A
Determine deployment architecture	$13,200	$1,167
Travel (for deployment knowledge)	$1,000	$0
Create CP/CPS documentation	$7,333	N/A
Travel (for CP/CPS knowledge)	$1,000	$0
PKI consultant	$3,667	$2,200
TOTAL	**$41,533**	**$8,534**

Facilities

For security and disaster recovery purposes, the primary and secondary CA should be housed in separate and secure facilities. A secure data center provides maximum protection for your PKI system so it cannot be compromised. In addition, should a catastrophic disaster strike the primary building housing your CA, such as a fire, natural disaster, or terrorist attack, your PKI system and sensitive data remain secure at the secondary facility.

While small organizations generally do not have the budget for a separate facility, a lab with independent security is still required.

If lab space already exists, the cost used is a percentage of the average facility's cost based on usage.

To securely house your CA, you must account for the following:

- **Suitability assessment and preparation**: This includes: working with facilities to locate a lab, office, and location; determining the feasibility of the facility and obtaining quotes; completing renovations such as building new walls, laying a non-static floor, building floor-to-ceiling protection, installing racks, wiring, servers, and a phone; and installing networking equipment and rack mounted machines.

  Medium and small companies may use existing lab space, and therefore a percentage cost based on usage is applied. The machines will occupy a full rack (10U of space), which cannot be shared as it needs to be locked for security. A typical third-party rack costs $33,000, which includes the physical cost of the rack, network, and wiring, as well as power, air conditioning, and space. The size of the data center also affects the cost (cheaper per square foot for a larger facility).

- **Facility operation requirements**: This includes: electricity, which involves getting a quote and hiring a contractor to install the panel and run power; a redundant air conditioning system enough to cool one rack of machines; and a backup generator. Power must be shut down while the new system is brought online.

- **Uninterruptable Power Supply (UPS)**: UPS is needed so that your machines maintain a continuous supply of power from an independent source when electricity from your normal power supply is not available. This requires a separate UPS system. Medium and small deployments might tie into the existing corporate UPS system and diesel generator system.

- **Security**: This includes securing building access, room access, and equipment access with a security device such as a card reader. The room must also be outfitted with fire and alarm systems and a safe to store key information.

Table 4: Facilities costs

Description	*Per year cost (over 3 years)*	
	Organization A	Organization B
Locate a lab, office, location	$233	Existing
Existing lab	N/A	$7,000
Obtaining quotes for new lab	$467	N/A

Outfit room	$3,333	Existing
Install racks, wiring, servers, and a phone	$833	$833
Install electric panel and run power	$1,333	Existing
Building outage while new system brought online	$233	N/A
Air conditioning	$3,333	Existing
Backup generator	Tie into existing backup generator	Tie into existing backup generator
UPS system	$2,000	Existing
Card reading machine	$333	Existing
Install card reader and tie into corporate system	$1,000	Existing
Fire and alarm systems	$167	Existing
Safe	$333	Drawer
TOTAL	**$13,598**	**$7,833**

Hardware and software

To deploy a PKI system, you require PKI hardware and software. Purchasing decisions must take into account scalability, application integration, high availability, operating system, backups, and so on.

The following are hardware and software requirements:

- **Firewalls**: This includes isolating the network and setting up a firewall or switch. A second firewall or switch is needed for high availability.

- **Main CA machine and disk space**: This includes a main machine for the CA and another machine for the database holding the certificates.

- **Machines for high availability**: High availability is for the customer whose business cannot tolerate any loss in service. Services that are affected by downtime include certificate creation (needed for creating corporate IDs), certificate revocation (needed to revoke the certificates of users no longer entitled to access), and access to certificate revocation lists (needed to determine revoked users who must be denied access). HA includes: a second machine for the CA, RAID disks, redundant power supply, redundant switching network, and redundant database and directory.

- **Operating systems (Windows or Linux)**: This includes an OS for the main machine and another OS for the high-availability machine. One server can hold up to four instances.

- **Hardware Security Module (HSM)**: A HSM contains the private key of the CA used to sign the certificates it issues as authentic. Protecting private keys in specialized, tamper-resistant hardware provides increased protection against unauthorized issuance and use of fraudulent certificates to gain access to assets intended to be protected by certificates. An HSM is necessary if you are worried about anyone gaining unauthorized access to assets and any resulting damage caused by such accessing. For the purpose of this study, HSM costs include the appliance, smart cards to contain backups in the event of a device failure, PIN entry device, and backup.

- **HSM for high availability (HA)**: This includes a second appliance.
- **HSM for disaster recovery (DR)**: This includes a third appliance. This item is included in the disaster recovery section.
- **Lab racking**: This includes the purchase and installation of a single rack for the machines and table for a monitor and keyboard.
- **PKI software**: To eliminate the debate on PKI software pricing, this study set PKI software cost at $0.
- **Database**: This includes a database, such as IBM Informix, to store data.
- **Directory software**: Since options are available for free open source software or Microsoft directories, this study does not include a cost for a directory.
- **Virtualization software**: This includes virtualization software for the server as well as for the high availability server.

Table 5: Hardware and software costs for an internal CA

Description	*Per year cost (over 3 years)*	
	Organization A	Organization B
Firewall	$1,333	$1,333
Firewall for HA	$1,333	N/A
Main CA machine	$3,733	$3,733
Machine for database	$8,000	Local disks
Machine for HA	$3,733	N/A
Operating system	$800	$800
Operating system for HA	$800	N/A
HSM	$6,400	$6,400
smartcard, PIN, and backup for HSM	$1,000	$1,000
HSM for HA	$6,400	N/A
HSM for DR	Included in DR hardware costs	Included in DR hardware costs
Single rack	$667	$667
Table	$333	Shared
PKI software	Free	Free
Database	$2,667	$2,667
Directory software	Free	Free
Virtualization software	$2,133	$2,133
Virtualization software for HA	$2,133	N/A
TOTAL	**$41,465**	**$18,733**

Installation and configuration

This includes the installation and configuration of the Certification Authority (CA), the directory, HSM, firewall, high availability (HA) software, supporting software (which includes the time server, monitoring, and load balancing), and the client registration software.

Table 6: Installation and configuration costs for an internal CA

Description	*Per year cost*	
	Organization A	Organization B
Install the Certification Authority	$7,333	$7,333
Install the directory	$3,667	$3,667
Install the HSM	$7,333	$0
Install the firewall	$1,167	$1,167
Install the high availability software	$1,167	$0
Install time server, monitoring, load balancing	$1,167	$1,167
Install Entrust Authority Administration Services for registration capabilities (registration software)	$700	$700
TOTAL	**$22,534**	**$14,034**

Disaster recovery

Disaster recovery (DR) ensures that your system continues to operate in the event of a catastrophic failure to the building housing the CA at the primary site. Continued business operation is achieved through backup systems, located at a separate and secure facility, which automatically assume the duties of the original server when necessary. Disaster recovery requires: redundant machines; an outfitted room in the separate and secure facility, with power, racks, main CA machine, and database machine; and setup of the DR site, and travel time to the DR facility.

Table 7: Disaster recovery costs for an internal CA

Description	*Per year cost*	
	Organization A	Organization B
Facility expenses	$13,100	N/A
Hardware expenses	$22,067	N/A
Setup, travel time for disaster recovery	$3,333	N/A
TOTAL	**$38,500**	**N/A**

Backups

Database backups ensure that data is retrievable in the event of a total failure. A loss of database information would be catastrophic, as you would:

- Lose all archived decryption keys, which means you cannot decrypt past encrypted data (that information is lost forever).
- Lose your CA key use, which means 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.

- Lose your CA, which means the CA has to be recreated. Once you recreate your CA, you need to do another key generation ceremony and associated audit, which is extremely costly. 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.

As such, the cost of implementing backups must be included when building your PKI solution. Backup costs include:

- **Small robotic tape system and server software**: This includes a high performance, robotic tape backup library system, tape, and a server application that communicates with the client software to enable writing of critical information to the tape machine.
- **Backup client software**: This includes an application that takes scheduled (periodic) snapshots of the database and logs as well as incremental backups in the event of a failure between scheduled backups.
- **Backup equipment through central IT services**: This includes using the backup equipment already available through central IT services instead of investing in a specific purpose machine. This is generally only an option for smaller deployments.
- **Installation**: This includes the installation of the tape system, putting the new machines in the backup cycle, installing backup software, and configuring encryption parameters.
- **Testing**: This includes testing the backup tapes periodically to ensure the data is actually being written. A backup system is of no value if the backup tapes contain no information.
- **Managing and coordination**: This includes managing the tapes and coordinating offsite storage.
- **Monthly backups to DVD**: This includes backing up your system on a monthly basis to DVD for system restores.
- **Offsite storage:** This includes an offsite storage fee with a 3rd party vendor for sending and storing tapes at an off-site location to avoid loss of data in the event of damage at the primary site.

Table 8: Backup costs

Description	*Per year cost*	
	Organization A	Organization B
Tape system and server software	$10,667	N/A
Backup client software	$533	N/A
Backup equipment through Central IT	N/A	$587
Installation	$2,200	$2,200
Testing	$8,400	$2,100
Managing and coordination	$2,100	N/A
Monthly backups to DVD	$4,200	$4,200
Offsite storage	$3,000	N/A
TOTAL	**$31,100**	**$9,087**

Root key generation

A root key generation (RKG) ceremony affirms that an organization's RKG policies are followed and that no anomalies occurred that might later impugn the integrity of the root key. This involves writing RKG scripts, which are detailed procedural steps that are executed and audited, and other professional services work, an auditor, a test-run of the RKG, an RKG ceremony to run through the script, and a test of the RKG at the disaster recovery site.

Table 8: Root key generation costs for an internal CA

Description	*Per year cost*	
	Organization A	Organization B
RKG scripts and other professional services work	$27,500	N/A
Auditor cost for RKG	Included in auditing cost	N/A
Test of RKG (4 people)	$1,867	N/A
RKG ceremony to run through script (6 people)	$1,400	N/A
Test of RKG at DR site (4-5 people)	$933	N/A
TOTAL	**$31,700**	**$0**

Audit

Regular audits determine whether policies and procedures established by an organization are being implemented as outlined in the CP/CPS. Conformance to policy demonstrates trust, provides accountability, and protects the trust of the brand. Any recommendations received from audits allow organizations to adjust policies and practices to improve their security framework. Audits are necessary if you establish trust relationships with CAs outside of your domain through cross-certification.

The audit cost provided here is based on a volume discount. Actual audit costs are likely much higher.

Table 9: Audit costs for an internal CA

Description	*Per year cost*	
	Organization A	Organization B
Annual audit	$50,000	N/A
TOTAL	$50,000	N/A

Maintenance and operations

This includes hiring staff to work 24/7, training staff, and purchasing a system monitoring tool. Fees also include premium pager duty, on-call staff time, and charge-backs from the network monitoring group for managing the machines.

Table 10: Maintenance and operations costs for an internal CA

Description	*Per year cost*	
	Organization A	Organization B
Full-time staff available 24/7	$126,000	$42,000
Staff training	Included in LLR	Included in LLR
System monitoring tool	$1,333	$0

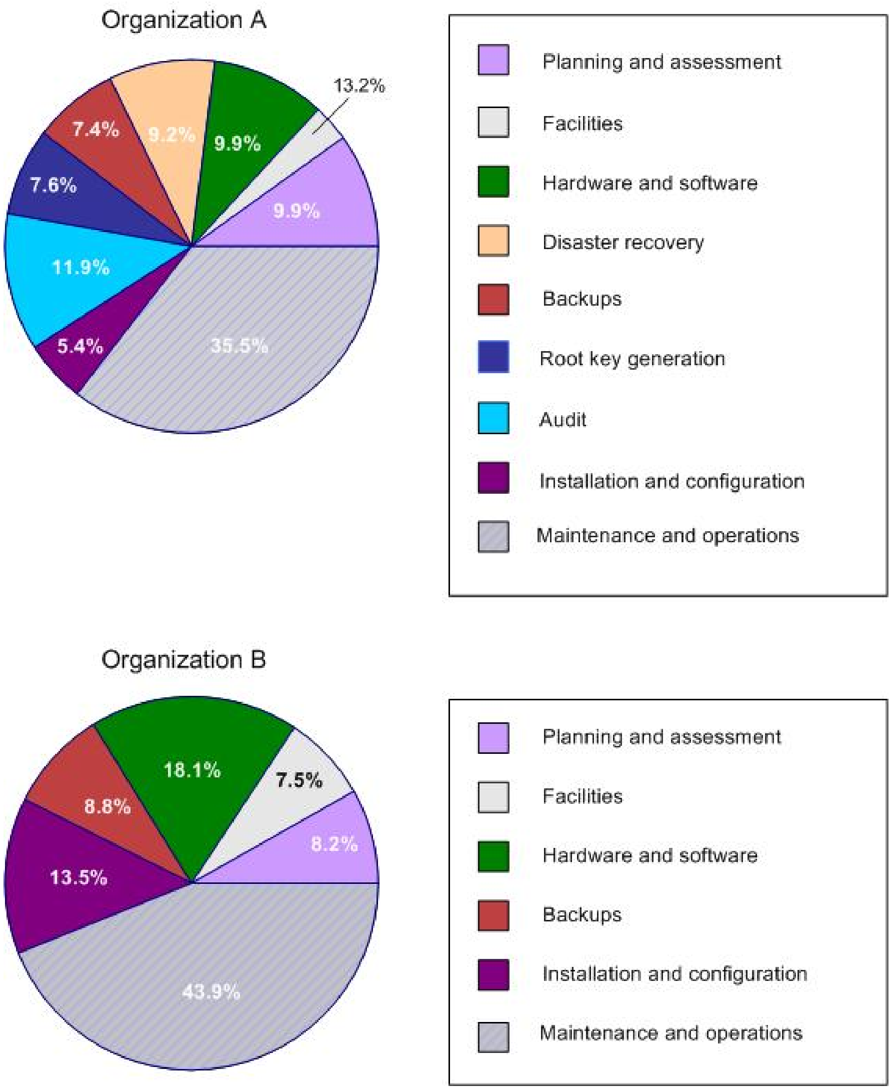
Pager duty and on-call staff time	$18,304	$0
Network monitoring group charge-backs	$3,500	$3,500
TOTAL	$149,137	$45,500

4.5 Cost distribution for an internal CA

The following figure illustrates the cost distribution for each element of PKI ownership. Note that the hardware and software costs are only a small percentage of the overall cost of PKI ownership. The people time to run the system is the largest expense.

The cost distribution remains the same regardless of the number of certificates issued, as the cost to run a PKI is based on your system inclusions.

Figure 2: Cost distribution for an internal CA



4.6 Cost per certificate

Given a static system, the cost of running a PKI does not change whether you need 1,000 certificates, 50,000 certificates, or anything in between. As mentioned previously, the cost of a PKI is based on all the items described in this paper, such as: planning and assessment, facilities, hardware and software, installation and configuration, disaster recovery, backups, root key generation, audits, and maintenance and operations.
However, the number of certificates you require does impact the cost your organization is spending per employee: the price per employee decreases as the number of certificates increases. This can affect the ability to reach business goals.

Table 11: In-house CA price per certificate

Number of certificates	***Cost per certificate***	
	Organization A	**Organization B**
1,000	$420	$115
15,000	$28	$8
50,000	$8	$2

5 Comparing an in-house CA to a hosted CA

A hosted certificate service provides many advantages over deploying your own in-house CA, such as:

- Enabling critical resources so you can focus on core competencies
- Reducing risk by relying on a service provider's security and operations expertise
- Shortening time-to-market to provide competitive advantage or meet regulatory requirements
- Providing certificates trusted by other CAs
- Reducing up-front investment and establishing predictable costs
- Reducing time commitment

The most measurable benefit is in terms of cost. This section compares the cost of deploying an internal CA with the cost of outsourcing your CA to Entrust Managed Services PKI.

5.1 Cost comparison methodology

To accurately examine the cost of an in-house CA, Entrust evaluated two companies, both with different PKI requirements. While all organizations want a PKI system that includes a full feature list, the cost often exceeds the budget. Most companies cut features to reduce costs, but now there is another way. By outsourcing your PKI to Entrust Managed Services PKI, you can reduce costs without reducing PKI quality. Entrust Managed Services PKI is trusted security for less.

With Entrust Managed Services PKI, all system features are included to ensure organizations have the most secure and successful PKI possible.

Entrust Managed Services PKI base offering includes the following system features:

- High availability and system monitoring with a service level agreement of greater than 99.5% to ensure business continuity
- Hardware Security Module storage of private key to prevent tampering or theft

- Separate, secure facility for Certification Authority to ensure security of data
- Disaster recovery with backups and equipment at a remote site to ensure business continuity in the event of a disaster
- Secure, automatic backups of the database and logs on both a scheduled (periodic) and incremental basis to ensure data is retrievable in the event of a total failure. Backups are also tested to ensure the backups are usable and not, for example, an empty file.
- Root key generation to verify the integrity of the root key
- Annual audits by a third-party to verify compliance to Entrust's Certificate Policy and Certificate Practices Statement and to provide accountability

Table 12: Comparison of Entrust Managed Services base offering

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

Due to the feature-rich Entrust Managed Services PKI offering, the most accurate price comparison is between Organization A and Entrust Managed Services PKI, as Organization A includes the system features available in the Entrust Managed Services PKI base offering.

6 How Entrust Managed Services PKI saves you money

Entrust saves you money by: sharing processes, tools and facilities across a number of customers; providing disaster recovery services; having highly trained experts on-staff and available 24/7; maintaining hardware and software upgrades; and providing security audits. Entrust is able to achieve volume discounts that are shared with our customer base.

Entrust removes the cost and hassle associated with building your own infrastructure. With Entrust Managed Services PKI, you can benefit from Entrust's expertise and capitalize on Entrust's existing infrastructure. This also leads to faster deployment and time-to-market.

Costs are upfront and predictable with Entrust Managed Services PKI, as your PKI solution adapts to your organization's requirements. You no longer have to invest upfront based on forecasted, or predicted, growth.

Organizations can request and manage certificates through Internet-based applications without any requirement to purchase and maintain client software.

Note: Should you desire fully automated certificate enrollment, Entrust does offer the Entrust Entelligence Security Provider client (for Windows and Mac). Security Provider also offers a plug-in for Microsoft Outlook, which delivers capabilities that simplify the delivery of secure messages from the sender to the recipient's desktop (over what Microsoft provides). For more information about the value of Security Provider, see *Why you should use certificates with Entrust Entelligence Security Provider*, available under the **Resources** tab of www.entrust.com/managed_services.

Many commercial off-the-shelf (COTS) applications—including email, desktop folders, remote access (VPN), and electronic forms—transparently integrate with certificates, so there is no need to invest in additional resources or alter current practices.

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.

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

7 Why Entrust Managed Services PKI is the best value

Entrust's hosted solution provides a number of benefits but the high level key benefits from a cost and security standpoint are the provision of high-end security for less than what it costs you to run a PKI today, system features that far exceed what many companies would spend if implementing their own CA in-house, and Entrust includes many features that competitors charge extra for.

- 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 99.5% 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, Entrust's high performance architecture allows for quick user enrollment, allowing you to increase the speed at which you conduct business.

- 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 has partnered with Savvis, a world leading hosting provider, for secure infrastructure facilities. In addition, all employees are subject to background checks and security clearance. **Note**: Root Key Generation, Hardware Security Module, and established proven policies and procedures applied by security experts and audited by external auditors are vital to minimizing risk of errors resulting in security breaches.

- Flexibility

  Entrust Managed Services PKI offers the flexibility to choose a managed PKI and migrate to a self-hosted option later. You can also switch from self-hosted to hosted.

- 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 Summary

As this paper illustrates, deploying an internal CA is expensive, not only in term of resources, but in terms of business opportunity: the resources and time required to operate and maintain an in-house CA changes an organization's composition. This means an organization no longer has 100% to give to their core business, which can lead to missed opportunities and, perhaps, a decline in business.

Entrust Managed Services PKI is less expensive than deploying an internal Certification Authority (CA), even with the cost of PKI software removed, and allows you to focus on your core business.

If you want to save money on a PKI, and do not want to cut quality or reduce the focus on your core business, outsource your PKI to Entrust Managed Services PKI. Entrust Managed Services PKI provides trusted security for less.

For more information, visit www.entrust.com/managed_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.