



WHITE PAPER

---

# Total Cost of Ownership for Public Key Infrastructure



Where it all comes together.™



**CONTENTS**

+ Introduction	3
How Assumptions Are Stated	3
Definition of Total Cost of Ownership	3
Comparison Cases: VeriSign vs. “Product B”	3
Comparison Metric: Average Dollars per User, per Year	4
Size of Installation Assumptions	4
+ Inputs: The Costs of VeriSign Managed PKI	4
Price: VeriSign Managed PKI	4
IT Staff Time	5
Registration Authentication Costs	6
+ Inputs: The Costs of Insourcing	7
Price: Software Modules	7
PKI Consulting	7
IT Staff Time	8
Registration Authentication Costs	8
Hardware: Servers	9
Facilities and Infrastructure Security	9
+ Results	14
VeriSign Is Lowest Cost	14
+ Additional VeriSign Advantages	15
+ Conclusion	17
Summary of Analysis	17



# Total Cost of Ownership for Public Key Infrastructure

## + Introduction

It has become widely accepted in the IT industry that the correct method for analyzing the cost of a vendor's products or services is to do a Total Cost of Ownership (TCO) analysis. Rather than focusing solely on price, buyers of IT products and services must consider the additional, often hidden, costs of operating and managing their purchases.

To help sales representatives better serve customers, VeriSign has conducted a complete TCO analysis comparing two alternatives:

1. Outsourcing Public Key Infrastructure (PKI) with the VeriSign® Managed PKI system.
2. Insourcing an in-house PKI system by buying from a PKI software vendor.

The conclusion is unequivocal: VeriSign Managed PKI system is significantly less costly in TCO terms than buying PKI software and running it in-house. This paper provides an in-depth look at the TCO of these two alternatives.

### How Assumptions Are Stated

Although PKI TCO has been studied previously, these prior studies have often failed to state their numerical assumptions. This paper explains every numerical assumption in detail. If desired, someone could check the validity of this analysis by conducting an independent review of the cost descriptions that are used.

### Definition of TCO

One of the most important characteristics of software, in contrast to a managed service such as VeriSign's Managed PKI, is the high level of additional costs associated with it. PKI systems are particularly expensive to maintain if they are based on software installed internally.

This paper uses the standard definition of TCO as all the costs, in addition to the price paid to a software vendor or managed service provider, required to operate and maintain a PKI system. Such costs include: IT staff time, hardware, security, registration authentication, facilities costs, and certificate policy and certificate practices statement. Detailed estimates of these costs are provided so that Managed PKI can be compared to the competition.

### Comparison Cases: VeriSign vs. "Product B"

For the purposes of this paper, no particular software vendors are selected or named, but instead "Product B" is used to represent generic vendors selling PKI software.

Comparison Metric: Average Dollars per User, per Year

There are multiple possible value metrics for a TCO analysis. This paper considers two of these metrics in depth:

- Year-by-year cash expenditures
- Average dollars per user per year

In the end, it proved more effective to present the information using the second metric, average dollars per user per year. One disadvantage of the first metric, year-by-year cash expenditures, is that computing it requires knowledge of the size of the enterprise (or the number of users in the PKI installation) and the time horizon over which the enterprise evaluates its technology investments. Because these variables cannot be known in advance, this paper provides a metric that can be multiplied by the variables once they are known. This metric is average dollars per user per year.<sup>1</sup>

Size of Installation Assumptions

This paper makes few assumptions about the expected installation size, although VeriSign pricing is provided only for installations of less than 10,000 users. To determine the average TCO per year for an installation, it is necessary to multiply the average dollars per user per year cited in this report by the company’s number of users. Further customization can be provided by VeriSign sales representatives.

**+ Inputs: The Costs of VeriSign Managed PKI**

Price: VeriSign Managed PKI

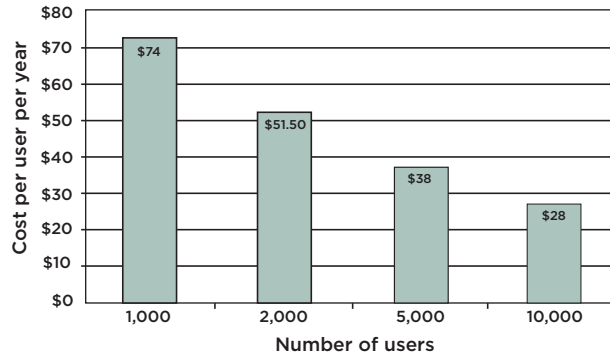
The following table and chart show detailed costs to customers, including set-up labor, for VeriSign Managed PKI as of March 15, 2005.

MANAGED PKI FULL PUBLIC	SMALL 250 - 1,000*	MEDIUM 1,001 - 5,000	LARGE 5,001 - 10,000
<i>Per User</i>	\$38	\$29	\$18
<i>Annual Managed Service Fee</i>	\$35,000	\$45,000	\$100,000
<i>Total Annual Service Fee</i>	\$44,500 - \$74,000	\$74,029 - \$190,000	\$190,018 - \$280,000
<i>Total on a Per-User Basis</i> <i>*Minimum of \$50,000</i>	\$74	\$74 \$38	\$38 \$28
<i>One-Time Set-Up Fee</i> <i>(Standard Implementation)</i>	\$10,000	\$10,000	\$10,000

Pricing is not shown for Very Large (> 10,000 users) installations as these enterprise-class deals require customization. However, the conclusions of this paper would hold as well if the inputs were customized for Very Large installations, because insourcing burdens increase significantly with an increase in installation size.

<sup>1</sup> Note that a three-year time horizon is used. Results vary only slightly when a five-year time horizon is used.

The chart below shows pricing based on a three-year average cost in dollars per user, per year. Managed PKI pricing is based on a set-up fee, an annual management fee, and a per user, per year fee. Because the annual fee recurs yearly, taking a three-year average does not affect the annual fee. The average only affects the set-up fee, which is divided by three.



As the above chart illustrates, the average price per user per year declines as the number of digital certificates issued becomes larger. For 1,000 users, public digital certificates average \$74 per user, per year all-in (including set-up costs), whereas for 10,000 users the price drops to \$28.00 all-in.

Interestingly, on a TCO basis, it will become clear that although the VeriSign Managed PKI prices are higher for lower volume levels, the cost of insourcing is dramatically higher. At lower volume levels VeriSign offers the greatest margin of benefit over insourcing.

#### IT Staff Time

Even the VeriSign Managed PKI system requires some internal IT staff time to operate and maintain it. To be conservative, this paper assumes that at least one-half Full Time Equivalent (FTE) of IT labor is required to operate and maintain a Managed PKI installation for up to 5,000 users.

Obviously, other variables, such as the number of office locations participating in the PKI system, will impact the number of IT FTE required to manage it.

IT staff time is one of the most important variables for a potential insourcer to consider. In general, it takes at least 3 to 4 times the IT staff time to manage an insourced installation as it does to manage a VeriSign Managed PKI installation. (See Inputs: The Costs of Insourcing on page 7.)

Note: IT staff resources typically are allocated on Certificate Authority Management (zero for outsourcing to VeriSign), Registration Authority Management, Operation and Maintenance (1/4 if outsourced to VeriSign), Application Interoperability Testing (zero if using VeriSign's out-of-the-box Go!Secure applications), and the initial PKI Project Deployment (at least 1/2 if outsourced to VeriSign).

### Registration Authentication Costs

Whether a company insources its PKI system using software or outsources it with VeriSign Managed PKI, it will expend time registering and authenticating new users to the system. Therefore, the costs assessed in this section apply to both insourcing and outsourcing a PKI system and do not differentiate between the two. There are two possible procedures: automatic authentication and manual authentication. Each procedure has different costs associated with it and VeriSign supports both methods.

#### *Manual Authentication*

Manual authentication can be used to authenticate, for example, businesses to a B2B extranet. The point of the process is to: (1) make sure that the company receiving the digital certificate is, in fact, who it says it is and (2) make sure that the individual who receives the digital certificate on behalf of the company is, in fact, authorized by the company to do so.

To accomplish #1, the entity's data is checked against a Dun and Bradstreet database or other business database to verify that the business exists. To accomplish #2, the authentication worker places a telephone call to the business and confirms that the individual who requested the certificate does in fact work at the company and is authorized to represent the company by receiving its digital certificate. In addition, the individual's own telephone number is retrieved, and the individual is called at his or her own number. Finally, a "negative response letter" is sent to the company after the cert has been issued, informing the company of the cert and requesting a response if the cert was issued incorrectly.

This manual authentication process can require many telephone calls and a significant amount of work. Based on internal testing, VeriSign has found that a trained authentication worker can authenticate about 55 companies per week. Some authentications can be accomplished quickly, but others can take multiple hours of work if there is a problem receiving verification.

VeriSign assesses the fully loaded cost of an authentication worker at \$45,000 per year, which represents salary, benefits, and overhead. At 48 productive weeks per year – excluding training, holidays, and vacation – the average cost of an authentication is \$17.05 in labor time.

#### *Automatic Authentication*

A lower level of authentication quality can be achieved using automatic authentication procedures. In automatic authentication, only a lookup on a database (e.g., an enterprise's existing LDAP or Active Directory) is performed. There are no phone calls or negative response letters. The applicant is asked to answer certain questions, and the authentication worker checks the answers against internal or external databases. This type of authentication often will be used at companies that are authenticating their employees into a digital certificate system.

The auto-administration features require a server. This paper assumes that a second server is created for hot backup and recovery. The cost of each server is estimated at \$10,000.

**+ Inputs: The Costs of Insourcing**

Price: Software Modules

The prices of PKI software modules have varied widely (even bundled for free – Microsoft Certificate Server in Windows Server 2003). Also, pricing can be very complex as vendors charge separately for specific individual features. To simplify the analysis here, the cost of software can be boiled down to just three variables:

- Cost of software per server (dollars per server)
- Cost of software per client machine
- Software maintenance and support contract (percentage of purchase price per year)

The total cost of the software then will be determined by the number of users and the number of servers required to serve that number of users.

Based on an internal analysis of one software vendor’s pricing, this paper estimates that, including discounts, the minimum price of software that can be achieved for a real (non-pilot) installation is as follows:

INSOURCE SOFTWARE	COST
<i>Server modules</i>	\$27,000
<i>Desktop modules</i>	\$30
<i>Software maintenance and support (as percentage of purchase price per year)</i>	18%

In other words, server software costs \$27,000 per server, and desktop or client software costs \$30 per client. Maintenance and support will cost an additional 18 percent per year. Of course, any individual deal might have assumptions that differ from these. As will be seen, it does not matter what those assumptions are once the TCO is considered. The TCO of a software-based, insourced PKI installation exceeds that of Managed PKI, even if the software is priced at \$0. (See Results on page 14.)

PKI Consulting

Insourcers require a certain amount of consulting by PKI experts to set up their systems. This paper estimates 30 days of consulting at a fully loaded cost, including expenses, of \$2,500 per day.

DESCRIPTOR	VALUE
<i>Days of outside PKI consulting time</i>	30
<i>Outside PKI consultant expenses (daily rate and expenses)</i>	\$2,500



IT Staff Time

*Set-up Labor*

In addition, the insourcer must expend IT staff time to set up the PKI system. This paper estimates 12 weeks of internal set-up and configuration time and estimates the fully loaded cost of IT staff at \$143,000 per year, which represents \$110,000 per year salary plus 30 percent overhead.

DESCRIPTOR	VALUE
<i>Number of person-weeks to configure</i>	4
<i>Loaded cost of IT staff</i>	\$143,000

*Ongoing Maintenance*

Here is a crucial variable in the insourcing analysis. Because of the labor time involved in ongoing maintenance of the PKI system, this paper estimates a minimum requirement of one and half IT FTE for a system of 5,000 users or less. This estimate is exactly three times the estimate above for the IT FTE required for a VeriSign Managed PKI installation. Again, IT staff costs, fully loaded, are assessed at \$143,000 per year.

DESCRIPTOR	VALUE
<i>Minimum ongoing IT staff commitment</i>	1.5
<i>Number of users supported by this commitment, in this case</i>	5,000

Registration Authentication Costs

*Manual Authentication*

As stated in the assumptions regarding VeriSign Managed PKI, authentication costs are the same whether insourcing or using the Managed PKI system. (See Manual Authentication on page 6 for details.)

*Automatic Authentication*

As stated in the assumptions regarding VeriSign Managed PKI, authentication costs are the same whether insourcing or using the Managed PKI system. (See Automatic Authentication on page 6 for details.)



Hardware: Servers

Servers are a significant, though by no means the largest, cost component of insourcing. A reasonable base case for server cost is \$50,000 per server, assuming performance required to operate a PKI system. This paper estimates that the maximum number of users supported per server is well over 10,000, so that in the present range of installation sizes considered, one server is sufficient. In addition, this paper assumes that one backup server is purchased for each primary production server. These assumptions are shown in the table below.

DESCRIPTOR	VALUE
<i>Server hardware</i>	\$4,500
<i>Number of users supported per server</i>	> 10,000
<i>Number of backup servers desired</i>	1
<i>Annual hardware maintenance costs (as percentage of expenditures)</i>	20%

Facilities and Infrastructure Security

*Introduction*

Many categories of expenditures related to insourcing PKI are important for maintaining the security, redundancy, and availability of the PKI system such as, physical security, redundant systems, backup and recovery, anti-hacker teams, security guards, monitoring cameras, special cabinets to protect key tokens, training in procedures for key protection, background checks on employees, etc. VeriSign spends over \$5 million per year just in maintenance contracts and staff to operate one data center in Mountain View, California. Companies insourcing PKI can potentially avoid some of these expenditures by accepting a lower level of security than that provided by VeriSign.

This paper is not asserting that an insourcer will need to spend the same as VeriSign does on security. Instead, it analyzes facilities and infrastructure items an insourcer might want to have and assesses the typical costs of those items for an insourcer with a 5,000-user PKI installation. VeriSign has every one of these items and spends, in some cases, more than ten times the amount assessed for these items here.

This paper makes two sets of assumptions for secure facilities and infrastructure costs:

- **Minimalist** – A client might say, “We already have many of the items listed below.” Therefore, presented here is a scenario in which the company spends a bare minimum amount on incremental security for its PKI system. In this analysis the company funds only one secure facilities and infrastructure item, a small Network Operations Center (NOC).

SECURITY COSTS INPUTS (based on 5,000-user installation)		
<i>Description</i>	<i>One-Time Cost</i>	<i>Annual Cost</i>
NOC staffing and equipment	\$300,000	\$300,000

At VeriSign, the NOC is a Tier 5 protected room with 60-inch plasma screens, which performs real-time system performance monitoring of both the network and the data center environment – including variations in voltage, heat, and temperature. The staff watches all system activity, including any attempts at hacking, and has an escalation list of procedures. Ultimately, the quality of a security system depends on the quality of the people, and VeriSign's large network operations security staff undergoes the highest-level background checks before assuming their dedicated roles.

The NOC version envisioned at the cost above is much smaller. It consists of just two dedicated staffers (who may not provide support 24 hours a day, seven days a week) plus a small amount of equipment.

- **Normal** – In the normal scenario, this paper assumes that the company goes beyond just a NOC and spends typical amounts to acquire all of the following secure facilities items:
  - Physical facilities
  - Security equipment
  - Information systems – disaster recovery backup
  - Telecommunications and information systems
  - Root key management
  - Audit

These typical amounts are much less than what VeriSign spends on its own versions of these items. The rest of this section will describe these secure facilities and infrastructure costs individually.

#### *Physical Facilities*

Physical facilities, in general, are items built into the walls, doors, and skeletal framework of the data center, protecting access to the PKI system. Each of these items is summarized below with a description of what VeriSign has in place. The typical insourcer will not build to VeriSign quality. Costs are assessed in the table on the following page, not at VeriSign levels but at the lower levels of quality a typical insourcer would have to spend for the item. The objective of all the items is to ensure the security, fail-over and backup redundancy, and continuous availability of the system.

- **Hardened building.** At VeriSign, walls are secured with layers of stainless steel mesh. There are hardened doors and hardened locks. It is almost impossible for someone to ever force entry into the VeriSign data center. This protects data from physical threats.
- **Redundant power.** At VeriSign, there are multiple Power Distribution Units (PDUs) in each room. A power source runs from each one of those PDUs to a Central Processing Unit (CPU) cabinet. In each CPU cabinet every piece of equipment is multi-homed, so there are two different power sources. The result is virtually every possible level of electrical redundancy that can be created to ensure maximum system availability.
- **Backup generators.** Right now VeriSign operates out of buildings that have not one but two emergency generators. Each emergency generator is capable of solely running the entire electrical load of the building itself. Not only that, they are fed through redundant Uninterruptible Power Supply (UPS) systems. If one fails the other takes over. This system costs \$1 million right up front, though a much lower typical cost is assessed on the following page for what an insourcer might pay.

- **Redundant HVAC.** HVAC means heating, ventilation, and air conditioning. VeriSign has redundant HVAC systems. What is very critical is maintaining the desired ambient temperature inside the data centers. VeriSign can lose 33 percent of its systems and still maintain 100 percent of the cooling effectiveness of its environment. A much lower cost and quality is assessed on the following page for the typical insourcer.
- **Pre-action fire system and FM200 system.** The data center needs to be protected against fire, but it also needs to be protected against water damage to machines in the event of fire. That is what these two systems do. The FM200 system involves an inert gas that removes oxygen from the air. An alarm will sound in the room with a fire, giving occupants 30 seconds to evacuate. At that point the system is triggered and oxygen is eliminated without affecting the equipment. With the pre-action fire system, two alarms sound and only then do the sprinkler heads fill with water. Therefore, if a contractor falls and accidentally strikes a sprinkler head, for example, he or she will not release all the water because the system will not fill with water yet. The costs of these systems include ongoing maintenance and testing.

The table below shows typical cost assumptions for the relatively small insourcer of these items.

PHYSICAL SECURITY COST INPUTS FOR TYPICAL INSOURCER (based on 5,000-user installation)		
Description	One-Time Cost	Annual Cost
Hardened building/room	\$5,000	-
Redundant power, PDU, UPS, generator	\$200,000	\$20,000
Redundant HVAC	\$50,000	\$20,000
Pre-action fire system and FM200 system	\$20,000	\$2,000

### Security Equipment

There are two types of security equipment related to the facilities: access equipment and monitoring equipment.

#### Access

At VeriSign, the data center rooms have Defense Department Tier 5 secure access. To access the data center a person must pass through multiple tier environments until he or she reaches the core, which is a Tier 5 environment. No one can access Tier 5 without (1) an ID card read, (2) a PIN, (3) a hand scan, and (4) an eye scan. This equipment costs \$500,000 for scanners alone. For the typical insourcer, a much lower cost is assessed for access equipment (see table on next page).

#### Monitoring

In each data center, VeriSign has a fully staffed Security Operations Center (SOC) with banks of internal and external video cameras running 24 hours a day, seven days a week. The company stores hundreds of thousands of hours on tape. Here again, costs are \$500,000 in equipment alone.



The table below shows the costs assessed for a typical insourcer for this equipment.

<b>SECURITY EQUIPMENT COST INPUTS FOR TYPICAL INSOURCER</b> (based on 5,000-user installation)		
<i>Description</i>	<i>One-Time Cost</i>	<i>Annual Cost</i>
Security equipment - access control	\$15,000	\$2,000
Security equipment - monitoring	\$20,000	\$2,000

*Information Systems - Disaster Recovery Backup*

Disaster recovery is a critical issue in PKI. If the system is unable to recover, all the certificates have to be reregistered and reissued, potentially slowing down business processes, eliminating the audit trail, and creating substantial labor time costs. At VeriSign there are multiple backup systems. The entire data center is mirrored, including every single piece of equipment, software, etc. In the event that any individual piece of equipment goes down or a problem occurs, the system instantly switches over to the mirror data center. There also is an additional backup data center that can come online in a matter of hours. The cost of this redundancy is tens of millions of dollars.

For the typical insourcer, however, it is estimated that the cost of a small, hot backup system is as follows:

<b>DISASTER RECOVERY BACKUP COST FOR TYPICAL INSOURCER</b> (based on 5,000-user installation)		
<i>Description</i>	<i>One-Time Cost</i>	<i>Annual Cost</i>
Disaster recovery backup - hot site	\$100,000	\$5,000

**Facilities Personnel**

Two types of security personnel are crucial to the protection of the data center: (1) the security guards in the SOC's. and (2) the anti-hacking and system-monitoring network defense team (in the NOC already described). Both rooms are staffed 24/7.

**Security Operations Center**

The 24/7 team of guards undergoes sophisticated background checks. Shown below are estimated costs for a typical insourcer, which are based on relatively inexpensive security guards.

<b>SECURITY COST INPUTS</b> (based on 5,000-user installation)		
<i>Description</i>	<i>One-Time Cost</i>	<i>Annual Cost</i>
Personnel SOC staffing	\$100,000	\$100,000

*Telecommunications and Information Systems*

A host of items are needed to properly outfit a secure data center for PKI. Companies that already have data centers already might have some of these items. Below is a list with estimated costs for a typical insourcer.

<b>OTHER TELECOMMUNICATIONS AND INFORMATION SYSTEM COSTS</b> (based on 5,000-user installation)		
<i>Description</i>	<i>One-Time Cost</i>	<i>Annual Cost</i>
<b>Telecommunications</b>		
Phone switch	\$150,000	\$25,000
PBS	\$50,000	\$50,000
Redundant voice and data feeds	\$50,000	\$50,000
<b>Information Systems</b>		
Router	\$10,000	-
Firewalls	\$5,000	-
Load balancers	\$6,000	-
Web servers	\$5,000	-
Database servers	\$10,000	-
Application servers	\$5,000	-
Crypto hardware	\$8,000	-
Monitoring hardware and software	\$3,000	-
Software licenses	\$150,000	\$25,000

*Root Key Management*

Nothing is more important in PKI than protecting the root key. Keys are protected in hardened token cabinets. At VeriSign those cabinets cannot be opened without the simultaneous participation of six people who are part of a core list, and then the process is videotaped the entire time the cabinet is open. So VeriSign has tremendous control over who can go in and what they can do. Thus, protecting the root key means using special equipment and procedures to make sure that no individual knows the root key in its entirety.

The typical insourcer will spend much less on root key protection than VeriSign and, consequently, will run a greater risk of breach. The following typical costs for key management are assessed below.

<b>ROOT KEY MANAGEMENT COSTS</b> (based on 5,000-user installation)		
<i>Description</i>	<i>One-Time Cost</i>	<i>Annual Cost</i>
Key	\$8000	-
High security token	\$5,000	-

*Audit*

The cost of external audits, which provide third-party validation of internal security procedures, is shown below for a typical insourcer. Note that these are just audit costs, not the actual costs of implementing the security procedures and the facilities being audited.

<b>AUDIT COSTS</b> (based on 5,000-user installation)		
<i>Description</i>	<i>One-Time Cost</i>	<i>Annual Cost</i>
External compliance (SAS 70, Webtrust for CA)	\$75,000	\$60,000

**+ Results**

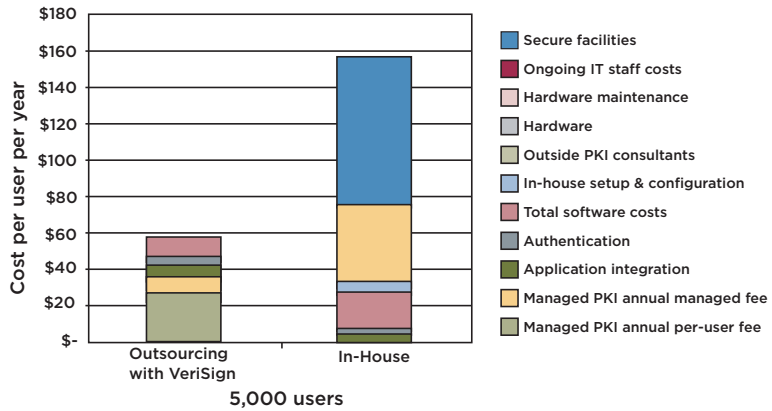
VeriSign Is Lowest Cost

**Insourcer’s Secure Facilities, Infrastructure, and IT Security Personnel Costs Are One Key Driver of the VeriSign Advantage**

First, examine the results of the analysis for 5,000 users. The chart below compares VeriSign Managed PKI to insourcing with Product B, a typical software installation. As can be seen, the total cost per user per year of insourcing is \$157 versus a TCO for Managed PKI of only \$58 per user per year for a 5,000-user installation.

This estimate uses the minimal secure facilities and infrastructure cost assumptions already described (i.e., it assumes only a small 24/7 NOC costing \$300,000 up front and \$300,000 per year, as shown on page 9). That cost is shown in the blue bar as part of the costs of insourcing.

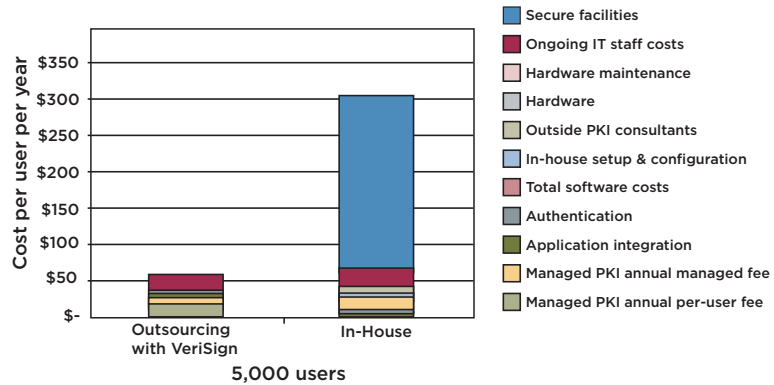
*PKI Total Cost of Ownership - Three Year Average*



Note first that the insourcer’s actual product cost – what is paid for software – is only a fraction of the TCO of PKI. In fact, the TCO of an in-house PKI system would still be greater than the TCO of outsourcing with VeriSign – even if the insourcer’s software costs were zero. This is obvious from the chart above. The total software costs are a relatively small component of the insourcer’s costs (based on the pricing estimates here, though some software vendors might charge more) after secure facilities and infrastructure costs and ongoing IT staff costs are included.

Moreover, the \$157 estimate of the TCO of insourcing PKI is conservative, because it excluded many possible insourcing costs. For example, it is assumed the insourcer allocates almost no money for many secure facilities, infrastructure, and security staff items such as: hardened facilities, redundant power and HVAC, security equipment, security personnel, disaster recovery backup system, telecommunications equipment, redundant Internet connections, key management, audit compliance, etc. Were these items to be included, the typical costs of which are itemized in the previous section, the TCO of insourcing PKI would be \$300 per user per year, as shown in the second chart below. A VeriSign sales representative can provide consultation to qualified enterprises regarding additional expected secure facilities and infrastructure expenditures and how they affect the cost of insourcing.

*PKI Total Cost of Ownership - Three Year Average  
(with increased Expenditure on Secure Facilities)*



**Insourcer’s Cost of IT Labor Time Is a Second Key Driver of the VeriSign Advantage**

Finally, note that the insourcer must spend three times as much on internal IT labor than a VeriSign Managed PKI outsourcer. For a 5,000-user installation, it is estimated that the insourcer’s internal IT labor cost will be \$42.90 per user per year over three years versus the outsourcer’s cost of \$14.30 per user per year. These costs are shown as the red rectangles in the chart above. In fact, even excluding secure facilities costs entirely (the blue bar, which represents secure facilities and infrastructure as well as security personnel), the labor costs of insourcing, along with other hardware, consulting, and software costs, would cause insourcing to be significantly more expensive than outsourcing with VeriSign. Once again, VeriSign sales representatives can customize this analysis for qualified enterprises interested in Managed PKI.

**+ Additional VeriSign Advantages**

Though a TCO analysis strongly favors Managed PKI over insourcing the PKI system, VeriSign Managed PKI has additional advantages:

- Time to implementation
- Probability of successful implementation
- In-house IT talent is not distracted by allocating them to an internal PKI system
- Quality of security
- Brand value
- VeriSign Certificate Policy and Certificate Practices Statements
- Out-of-box application integration
- Wide Directory/Database Support
- Ease of Deployment and Use

To the degree that these items are important to an enterprise, they might become the deciding factor above and beyond cost issues.

#### Time to Implementation

As an already implemented backend service with policies and procedures and limited customization requirements, VeriSign Managed PKI can be implemented in less than one third the time required to implement a software-based PKI system in-house. Rapid scalability – to multiple locations, to tens of thousands of users, etc. – is already accomplished rather than being a wished-for possibility. For an enterprise with an urgent need to get PKI done quickly, VeriSign is the only choice.

#### Probability of Successful Implementation

Because the majority of the VeriSign Managed PKI system is based on an existing backend infrastructure, the probability of successful implementation of the system is very high. By contrast, software-based PKI systems might face a questionable chance of actual implementation over time.

#### In-House IT Talent Is Not Distracted

Not every enterprise wants to take a significant number of its IT staff and dedicate them to maintaining an in-house PKI system.

#### Quality of Security

As detailed already, VeriSign takes such great care with each and every PKI security item, from secure facilities to key protection measures, that the probability of a security breach will be lower using VeriSign than it will be using a software-based system.

#### Brand Value

As VeriSign enterprise clients use VeriSign PKI to interact with suppliers and customers, they gain the benefits of VeriSign's brand, which helps give suppliers and customers confidence in the enterprise's security.

#### VeriSign Certificate Policy & Certification Practices Statements

Developing certificate policy (CP) and certification practices statement (CPS) can take considerable amount of time and legal resources. When VeriSign customers choose the VeriSign co-branded Managed PKI services, customers automatically leverage the VeriSign Trust Network CP& CPS and can assure their certificate relying parties of their compliances to the well-documented VeriSign CP and CPS. The VeriSign co-branded MPKI services free customers from having to develop their own CP/CPS.

If customers do decide to develop their own separate CP/CPS for their private Managed PKI deployments, VeriSign Consulting can provide CP/CPS services as well.

#### Out-of-box Application Integration

Integrating a PKI infrastructure/platform with your existing and planned PKI applications such as S/MIME email, Web portal authentication, and document signing often require additional custom development and testing as each vendor application has its specific PKI requirements. VeriSign Managed PKI services seamlessly support many PKI-enabled applications including Microsoft® Outlook®, IBM® Lotus Notes®, VPN software (Check Point®, Cisco®, and Nortel®), Smart Card integration (e.g., ActivCard® and Aladdin®) and Adobe® document signing. Having VeriSign services pre-integrated and qualified with these best-of-breed applications free customers having to conduct their own integration development and testing efforts.

## + Conclusion

### Summary of Analysis

This white paper has provided a fairly exhaustive comparison of the TCO of VeriSign Managed PKI versus the main alternative: insourcing a software-based PKI system. Unlike many other discussions of TCO, all numerical assumptions are included in the paper. As a result, customers can check the assumptions against their internal beliefs in order to verify the study's conclusions.

The VeriSign Managed PKI service is an outsourced offering that alleviates the burdens and risks of building, deploying, and maintaining an in-house PKI while allowing enterprises to maintain internal control over vital aspects of security such as certificate issuance, suspension, and revocation. By leveraging VeriSign's industry-leading technology, expertise, and certificate practices statement, enterprises not only reduce costs, speed time to deployment, and strengthen security, but also win the confidence of partners, customers, and suppliers who recognize and trust the VeriSign name.

The result is quite clear: VeriSign Managed PKI is dramatically less expensive on a TCO basis than insourcing with a software-based PKI system. In fact, even if software vendors were to give their products away for free, VeriSign Managed PKI would still be less expensive on a TCO basis.

This conclusion holds regardless of what the insourcer spends on secure facilities, infrastructure, and additional IT security personnel costs. However, when these latter costs are properly allocated to the insourcer's budget for PKI, the difference in cost becomes even more dramatic.

IT staff time is a significant cost to the insourcer that is much reduced by using VeriSign Managed PKI. There also are many other components of costs that the insourcer must bear.

Finally, even aside from TCO considerations, additional factors impact the decision to use VeriSign Managed PKI include the following:

- Time to implementation
- Probability of successful implementation
- Doesn't require focusing a lot of in-house IT talent on PKI maintenance
- Quality of security
- Brand value
- VeriSign Certificate Policy and Certificate Practices Statements
- Out-of-box application integration
- Wide Directory/Database Support
- Ease of Deployment and Use

## + For More Information

For more information about VeriSign Managed PKI, please call 650-426-5310, or visit [www.verisign.com/products/pki](http://www.verisign.com/products/pki).

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.