Giga Information Group

A Total Economic Impact Analysis of Two PKI Vendors: Entrust and VeriSign

From Giga Information Group

September 1998

Project Director: Ira Machefsky

Published by:
Giga Information Group
One Longwater Circle
Norwell, MA 02061-1620

Tel: (781) 982-9500
Fax: (781) 982-1724

Note: Although great care has been taken to ensure the accuracy and completeness of this report, Giga Information Group is unable to accept any legal responsibility for any actions taken on the basis of the information contained herein.

Circulation or disclosure in whole or in part of this report outside the authorized recipient organization is expressly forbidden without the prior written permission of Giga Information Group.

Table of Contents

Table of Figures

Executive Summary

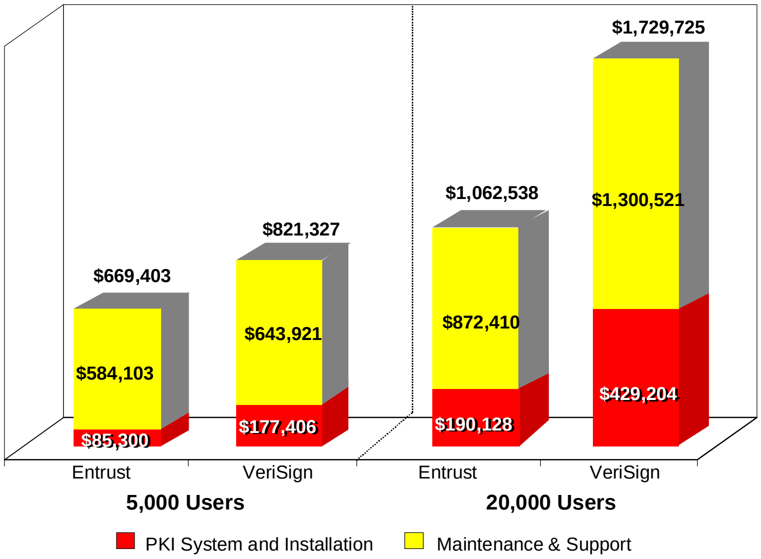
Given the growing importance of public key cryptography to many applications from encryption and secure e-mail to electronic commerce, *a public key infrastructure (PKI) is probably the most critical enterprise security investment a company will make in the next three years*. One of the most hotly contested security product battles is currently being waged between Entrust and VeriSign for deployment of PKIs. This report is an attempt to sort out the conflicting claims between these two companies and the PKI alternatives they offer.

In order to do this we applied a Giga Total Economic Impact (TEI) analysis to each company's current offerings and combined this with in-depth interviews of eight customers (four from each vendor). We selected three PKI application scenarios to compare, deployed across bases of 5,000 users and 20,000 users. We combined the resulting five year total cost of ownership (TCO) model of these scenarios, which included all direct, indirect, user and support costs, with the other elements of Giga's TEI analysis, benefit of ownership, flexibility and risk, to round out the report.

Five Year TCO

Scenario 1, an attempt to create the lowest cost scenario for each vendor, employed digital certificates for user authentication in a pure browser environment. Here we found that Entrust's five year TCO was 18 percent less than VeriSign's in the 5,000-user case, and 39 percent less than VeriSign's in the 20,000-user case. This was due to lower certificate licensing, distribution and help desk costs from Entrust's bi-annual deployment of certificates, in contrast to VeriSign's annual deployment of certificates (see Figure A).

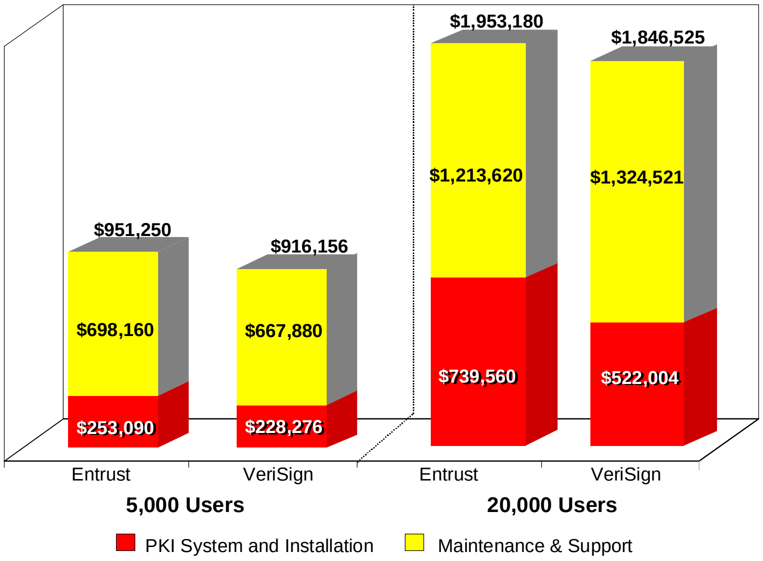
Figure A: Five Year TCO of Basic Certificates for Web Authentication — Scenario 1



Source: Giga Information Group

Scenario 2 employed digital certificates for user authentication with certificate life-cycle management. Here we found the five year TCO for the two vendors to be very close, favoring VeriSign by 4 percent in the 5,000-user scenario and by 5 percent in the 20,000-user scenario, but with costs allocated to very different categories. VeriSign was less costly than Entrust in combined product and installation costs and much less costly than Entrust for product maintenance costs, but Entrust users enjoyed significant savings in certificate distribution costs and associated help desk costs using Entrust's life-cycle managed certificates (see Figure B).

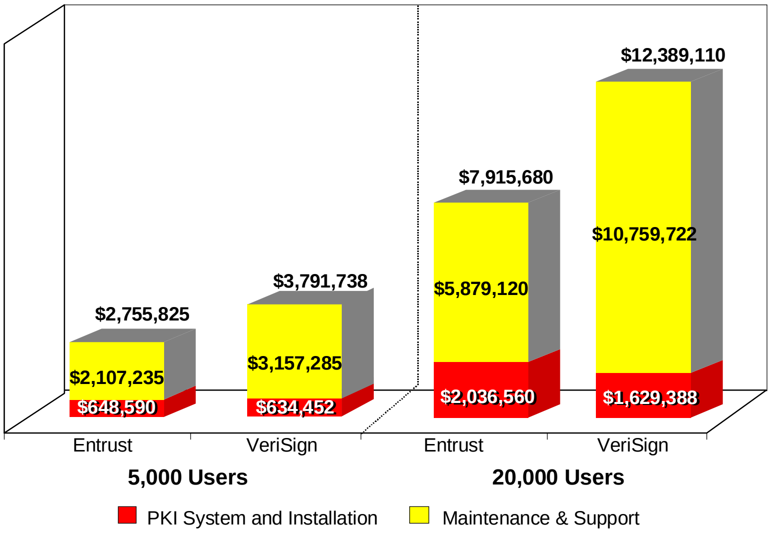
Figure B: Five Year TCO of Managed Certificates for Web Authentication — Scenario 2



Source: Giga Information Group

Scenario 3 employed digital certificates with two enterprise security applications, secure e-mail and desktop file encryption, together with certificate life-cycle management. Here we found that Entrust's five year TCO was 27 percent less than VeriSign's in the 5,000-user case and 36 percent less than VeriSign's in the 20,000-user case. VeriSign product and installation costs were 2 percent to 20 percent less than Entrust's, but Entrust users enjoyed significant operational cost savings from both certificate life-cycle management and automatic key backup and recovery management provided by the Entrust PKI (see Figure C).

Figure C: Five Year TCO of Managed Identities for Two Enterprise Applications — Scenario 3



Source: Giga Information Group

(Note: VeriSign has announced capabilities to support a more managed PKI, to be available in stages during the next four to eight months. As such capabilities appear and their functionality becomes better known, we will have to revisit these scenarios.)

End-User Benefit

In terms of user benefit, Entrust end users enjoy operating cost savings that range from 13 percent to 57 percent less than VeriSign users, based on lower ongoing end-user certificate distribution costs and lower associated help desk costs. In our interviews we found that Entrust users prefer the benefits of a best-of-breed security solution that they completely control while VeriSign users prefer the benefits of a public trust utility that allows them to outsource some of their security management. Customer interviews support the importance of a complete life-cycle managed PKI with automatic certificate revocation list (CRL) checking for both servers and clients.

Flexibility

In terms of flexibility, VeriSign shines here in the perception of its customers, since certificate rental allows them financial flexibility, among other kinds of flexibility, in avoiding capital and depreciation costs; although, as our study shows, such flexibility may cost more in the long run. Entrust users enjoy the flexibility of being able to assemble and manage their PKI as best they see fit.

Risk

Implementation

In terms of implementation risk, we were surprised to find that VeriSign customers took approximately 1.5 times to two times as long Entrust customers in the implementation phases of their PKI. (Planning and design times were approximately the same.) In our in-depth interviews we found that this was partly due to the greater uncertainty of VeriSign’s customers in how to proceed with their PKI — how they would use it, what it was good for, etc., perhaps influencing a desire to rent in the first instance. Other factors affecting delays for VeriSign customers included technical problems in accessing VeriSign servers through a firewall and the organizational issues of dealing with an external group. In general, though, Entrust’s customers moved forward confidently and with alacrity to implement their PKI within four to 12 weeks while VeriSign users took 1.5 to two times as long.

Scalability

In terms of scalability risk, almost all of the users we interviewed were just in the pilot stage of their PKI. Numbers of active users ranged from hundreds to 7,000. Most said they expected their PKIs to support “tens of thousands of users” by next year, although one large VeriSign user expressed extreme skepticism over numbers this large. While one Entrust customer has 50,000 active users, in general, data from either vendor is insufficient to predict scalability and large-scale performance issues.

Vendors

In terms of vendor risk, their customers hold both vendors in high regard. VeriSign’s customers view them as a visionary for building a public trust utility on the Internet. Entrust’s customers tend to hold the company in adulation, using terms like “excellent” and “fantastic” to describe the company, especially its customer service group.

Note: All products referred to within this report are registered trademarks, including: VeriSign OnSite, Entrust/ Web Connector, Entrust/Direct, Entrust/PKI, Entrust/ICE, Entrust/Express, Entrust-Ready, etc.

The Brave New World of Internet Security

A revolution is sweeping through the security world. Information security, long an arcane, highly specialized backwater of IT, has moved to the top of the agenda, not just of IT but of the business itself. Although the vast majority of security-related losses traditionally come from unauthorized insider access and attacks by disgruntled employees, IT security, as a prevention from harm, has never played well in the enterprise. While important, security has been viewed as an impediment to ease of use, harmful to system or network performance and costly. Most companies minimized it, choosing instead to manage security risk by underwriting it themselves. If nothing bad happened, they got away with it.

What is changing all this is the view of security as an enabling technology for electronic commerce. And this, of course, is yet another all-encompassing change brought about by the Internet. Everyone remembers the *New Yorker* cartoon with the two dogs sitting in front of a PC, one saying to the other, “On the Internet, nobody knows you’re a dog.” Who is out there trying to do business with you? This cartoon represented a prescient turning point in the way we looked at the online world. It personified (or perhaps canineified) the ambiguities of the online world, the threats and the opportunities of doing our business online. In one image it combines our concerns about security, privacy, the danger and thrill of the unknown, the kidnap of innocents with the possibilities of a “brave new world” that is about to unfold.

Everyone is concerned about security and also worried that too much security may get in the way. Traditionally, security deals with risks, threats, vulnerabilities and attacks. This is security seen as a way to keep bad things from happening to good information. But in the brave new world of the Internet, security is an enabler of functions and activities that would otherwise be impossible. These activities allow the enterprise to reach out and work with customers, suppliers, distributors and partners in ways that were impossible just a few years ago. And remarkably, the enterprise’s internal security is now being driven by the external mechanisms put in place to enable electronic commerce. We believe that IT will want and need to establish internal security mechanisms that are homogeneous with those that are deployed for the external world.

Why a PKI? — Entrust and VeriSign

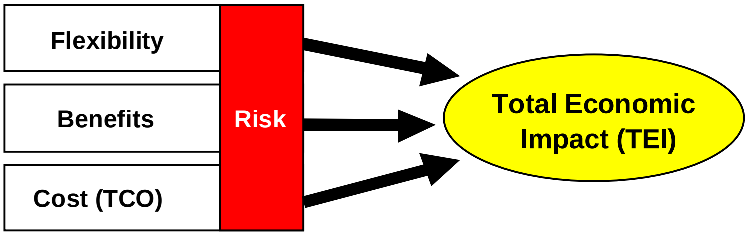
The chief of these mechanisms is the technology to establish a public key infrastructure (PKI). Given the growing importance of public key cryptography to many applications from secure e-mail to electronic commerce, *a PKI is probably the most critical enterprise security investment a company will make in the next three years*. PKI technology solves the problem of who is out there trying to do business with you by providing strong authentication with digital certificates, and allows reliable business communications by providing privacy and data integrity through the use of encryption and nonrepudiation through the use of digital signatures.

One of the most hotly contested security product battles is currently being waged between Entrust and VeriSign for deployment of PKIs. Entrust offers a traditional software product that is purchased, installed and operated by the enterprise while VeriSign offers a PKI service that VeriSign operates on behalf of the enterprise, essentially a leased or outsourced PKI. This report is an attempt to sort out the conflicting claims between these two companies and the PKI alternatives they offer.

What Is a Total Economic Impact Study?

Most previous reports on this subject have focused exclusively on cost of ownership, sometimes called total cost of ownership (TCO). However, determining which project will provide the best return for the organization or which product to purchase to make that project a reality requires a model that goes beyond the currently popular model of total cost of ownership. TCO only measures the cost side of an existing IT investment. Using TCO to make decisions on cost alone can, and often will, lead to improper decisions with questionable impact on organizational goals. Clearly, a new model is necessary. To this end, Giga has developed a Total Economic Impact (TEI) model for making IT decisions. TEI embraces the cost components of TCO and a best-practice approach to minimizing costs, and extends it by explicitly incorporating both benefits and flexibility while tempering them with concepts of risk (see Figure 1). Where TCO measures efficiency, TEI measures effectiveness. Using TEI an organization can evaluate project and product decisions in light of individual organization goals and move from the "cost center" positioning of TCO into a strategic "value center" position in the organization. This study, then, is a TEI analysis of Entrust's and VeriSign's PKI offerings, adding the categories of product benefit, flexibility and risk to the traditional one of cost of ownership.

Figure 1: Total Economic Impact



Note: Risk is an inherent part of the TEI model and overlays all parameters.
Risk equates to uncertainty and broadens estimate ranges for all other variables.

Source: Giga Information Group

Study Methodology

In doing this study we have relied upon vendor-supplied pricing data together with in-depth interviews of customers. We interviewed four customers of each vendor (a total of eight customers), the interviews ranging from 45 minutes to two hours. The customers included companies in financial services, publishing, manufacturing, high tech R&D and manufacturing, and a federal government research agency. Rather than sample data from a large number of users, we sought to do extensive interviews with the leading users of each product to gather insights into their choices and the issues they were grappling with. We formulated our judgements on the basis of the interviews together with an analysis of the pricing data. The conclusions we have come to are ours exclusively, and we bear the responsibility for any errors or misrepresentations. We are aware of the fact that so small a population of users may have resulted in sampling errors. However, consistency of reports across the population gives us confidence that we did uncover some true trends. Customers spoke to us candidly on the basis of confidentiality and we have, accordingly, taken pains to keep their identity secret. Where possible we have used direct quotes or paraphrases from our interviews to let the customers speak for themselves and emphasize the sometimes sharp differences in their positions. We call this "*the voice of the customer*."

PKI Scenarios

We selected three PKI scenarios of increasing sophistication, comparing deployments of 5,000 and 20,000 users for each scenario. While some PKI studies look at deployments in the 100,000s or millions of users, we feel that deployments of 5,000 to 20,000 are more practical to study since they will represent the vast majority of enterprise applications for the next 18 to 24 months. Some users we spoke to were just entering or exiting the pilot stage of their PKI projects while others had deployments of 1,000 to 7,000 users currently. Some of the users with deployments of around 1,000 users were anticipating their numbers to grow into the tens of thousands within 12 to 18 months, although one large bank, a VeriSign customer, expressed total skepticism about the near-term practicality of such large deployments saying, "60,000 users is bull % &*#." The largest user we spoke to, a financial services company employing Entrust, had already issued 100,000 digital certificates to 50,000 active customers and was in a position to boast that they had revoked more certificates than most companies had ever issued. Another large financial services company, while embracing digital certificates for strong authentication, was still struggling with the issue of whether all users or just merchants really need digital certificates for strong authentication and encryption.

Scenario 1

Entrust/Web Connector and VeriSign OnSite

We selected three PKI scenarios to reflect the different uses of digital certificates and to try to fairly match the differing capabilities of Entrust's and VeriSign's products. Scenario 1, an attempt to create the lowest cost scenario for each vendor, employs digital certificates for strong authentication in a pure Web-browser environment. In this scenario we compare Entrust's Web Connector with VeriSign's OnSite service offering. Web Connector is Entrust's PKI product for supporting pure Web-browser authentication. It has none of the features of Entrust's other managed PKI products, such as management capabilities for automatically rolling over certificates when they expire, autochecking certificate revocation lists (CRLs), or providing for key recovery and nonrepudiation. This is the Entrust product that is most nearly comparable to VeriSign's OnSite offering, which also lacks these managed certificate capabilities in a pure browser environment.

OnSite is VeriSign's PKI service offering for the enterprise. It is a service that VeriSign offers in which they operate the certificate authority on behalf of the enterprise. VeriSign has added a number of custom services and software modules to OnSite, which we have included in scenarios 2 and 3. We have omitted these VeriSign custom service and software modules in Scenario 1, *making scenario 1 the simplest, lowest cost PKI for each vendor.* VeriSign tells us that 40 percent to 60 percent of their enterprise customers use all of these custom services and software modules. Included in these are: (1) the custom PKI hierarchy ($30,000), which is a ceremony to create a custom hierarchy and root key for the enterprise, and (2) the Auto Admin software module and Local Hosting service ($20,000), which allow enterprises to locally host the Registration Authority approval process and locally host directory information and the interface to the Certificate Authority (CA). Basically, the only component of the PKI that VeriSign keeps for itself is the certificate issuance capability of the certificate server.

Scenario 2

Entrust/Direct and VeriSign OnSite

Entrust/Direct is the next step up from using digital certificates in a pure browser environment for strong authentication. It offers the managed certificate capabilities of Entrust's enterprise PKI product, but limited to authentication and encryption in a Web-based application. Thus, it provides for automatic certificate roll over upon expiration, auto-CRL checking, nonrepudiation and key backup. Direct also provides encryption between the Web browser and Web server, thereby essentially duplicating and eliminating the functionality of SSL while adding explicit trust as specified by corporate security policy. Direct was developed by Entrust, together with ScotiaBank, as a response to some of the concerns about the user controlled security model of SSL for financial service applications. It replaces the browser's user-centered control of security with centralized enterprise control of security, while at the same time providing for certificate life-cycle management services. It presently offers more functionality than VeriSign's OnSite, but at the cost of moving beyond a pure browser environment. VeriSign has announced plans to provide better certificate management capabilities in the future, but for this analysis we only dealt with currently available capabilities.

Scenario 3

Entrust/PKI With Entrust/ICE (desktop encryption) and Entrust/Express (secure e-mail) and VeriSign OnSite With Secure E-Mail and Desktop File Encryption Applications

Scenario 3 attempts to capture the use of a PKI in two of the most common enterprise applications: desktop file encryption and secure e-mail (using S/Mime). This scenario deploys the full, managed Entrust/PKI together with two Entrust-Ready applications, one for desktop file encryption and another an S/Mime plug-in for secure e-mail. We selected two Entrust applications that work with the Entrust/PKI for this scenario, Entrust's Entrust/ICE and Entrust/Express. For VeriSign, we again use the VeriSign OnSite service together with two VeriSign ready applications, Entevo (formerly QueriSoft) SecureFile for desktop file encryption and OpenSoft ExpressMail, a secure (S/Mime) e-mail plug-in. Both companies are VeriSign partners, listed on their Web page. Costs for this scenario include the licensing cost of these two applications for each PKI. While we could have chosen to use browser-based e-mail and avoided the e-mail plug-in charges for each PKI vendor, we decided against this since so few enterprises use browser-based e-mail for messaging and so few users have email clients that already support S/Mime. In this scenario key backup and recovery become a major issue since loss of access to a user's key results in lost access to encrypted data and encrypted mail messages.

Total Economic Impact Analysis: Cost

Cost is the most common differentiator in competitive choice. Given this, *it is interesting to note that not a single customer we interviewed for this study cited cost as the most important element in their choice of a PKI.* More important issues had to do with the perceived benefits, flexibility and risk of the solution. Perhaps this is also because the cost of a PKI can be so hard to calculate. We attempt to remedy this problem in this section. We have calculated cost comprehensively, including costs for hardware, software, certificate licensing, consulting and installation services, maintenance, administration and operation of the PKI, cost to users to update expired certificates, cost to do key backup and recovery (Scenario 3) and help desk costs in supporting the PKI. Executive summary figures A-C have the graphs of PKI costs for all three scenarios while Appendix A has a more detailed breakdown of cost than the summaries here.

Scenario 1

Entrust/Web Connector and VeriSign OnSite

Previous studies that have shown VeriSign's OnSite to be dramatically cheaper than Entrust's PKI have compared the more full-functioned (and more costly) managed Entrust/PKI to the unmanaged browser-based PKI supported by OnSite. Entrust recently introduced a new product, Web Connector, that provides services in an unmanaged Web browser environment comparable to VeriSign's OnSite. The Web Connector certificate authority issues certificates that are stored directly in the browser, just as VeriSign's service does. Roll over of certs upon expiration is an entirely manual process for the end users with both products. Since this is not a managed PKI environment, there is no special client software provided by either vendor to do automatic certificate life-cycle management. Figures 2 and 3 show the costs for this scenario.

Figure 2: Five Year TCO of Basic Certificates for Web Authentication – Scenario 1

Entrust: Entrust/Web Connector
VeriSign: OnSite

Issuing 5,000 Certificates/Yr

	Entrust	VeriSign
PKI System	$52,024	$146,126
Installation & Set-up	$33,276	$31,279
Vendor Maint. & Support	$26,551	$0
Enterprise Support	$557,552	$643,921
Total	$669,403	$821,327

Issuing 20,000 Certificates/Yr

	Entrust	VeriSign
PKI System	$108,024	$344,100
Installation & Set-up	$82,104	$85,104
Vendor Maint. & Support	$29,701	$0
Enterprise Support	$842,708	$1,300,521
Total	$1,062,538	$1,729,725

Source: Giga Information Group

Figure 3: TCO/User/Year — Scenario 1

	5,000 Users	20,000 Users
Entrust	$27	$11
VeriSign	$33	$17

Source: Giga Information Group

An examination of the details in Figure 1 Appendix A shows that the main difference in cost between the two solutions is in certificate/licensing costs and ongoing cert distribution costs. Since Entrust Web Connector is a product, licensing costs for certificates are not incurred yearly. In fact, the default for the product is to issue and license new certs every two years. Of course, they can be reissued even less frequently if one so desires, creating even lower licensing costs for the certificates; however, this is probably not a good security practice. Since this is an unmanaged PKI environment, there is no special life-cycle management of certs provided and no special software available on the client to perform this service. Hence, the Entrust certificate licensing costs are much lower than for their other managed PKI environment.

Thus, in this scenario we have attempted to spec the lowest cost PKI available from each vendor. We have assumed the use of no VeriSign OnSite local hosting software and no custom PKI hierarchy.

Scenario 1 Cost Finding:

The five year TCO for Entrust's Web Connector yielded 18 percent to 39 percent cost savings when compared with VeriSign's, based on the following:

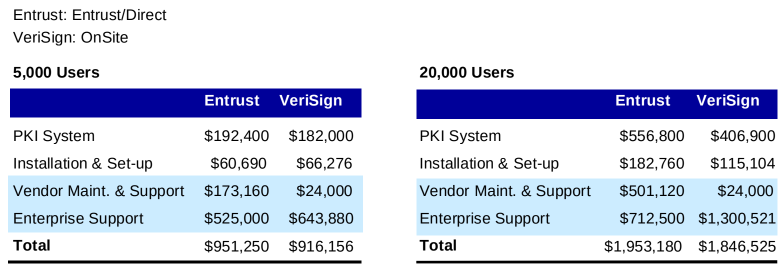
- **Entrust users incur lower annual certificate licensing costs**
- **Entrust users incur lower ongoing costs for bi-annual certificate distribution**
- **Entrust users incur lower help desk costs**

Scenario 2

Entrust/Direct and VeriSign OnSite

This second scenario takes us into the realm of managed certificates, which chiefly take advantage of Entrust's special client software that provides automatic certificate rollover capability. VeriSign currently has no similar capability, being tied to the constraints of whatever support is provided by the browser for certificate life-cycle management. While the total five year TCO for the two competitors is within 4-5 percent, the allocation of costs is in very different categories. Figures 4 and 5 tell the story.

Figure 4: Five Year TCO of Managed Certificates for Web Authentication – Scenario 2



Entrust: Entrust/Direct
VeriSign: OnSite

5,000 Users

	Entrust	VeriSign
PKI System	$192,400	$182,000
Installation & Set-up	$60,690	$66,276
Vendor Maint. & Support	$173,160	$24,000
Enterprise Support	$525,000	$643,880
Total	$951,250	$916,156

20,000 Users

	Entrust	VeriSign
PKI System	$556,800	$406,900
Installation & Set-up	$182,760	$115,104
Vendor Maint. & Support	$501,120	$24,000
Enterprise Support	$712,500	$1,300,521
Total	$1,953,180	$1,846,525

Source: Giga Information Group

Figure 5: TCO/User/Year — Scenario 2

	5000 Users	20000 Users
Entrust	$38	$20
VeriSign	$37	$18

Source: Giga Information Group

Although the total costs of the two vendors in Scenario 2 are within 4-5 percent of one another, we see that they are allocated in very different categories. Appendix A Figure 2 shows that the costs for the PKI system together with installation favor VeriSign by 2-29 percent. And since the Entrust/Direct solution requires $192,400 worth of software in the 5,000-user scenario and $556,800 worth of software in the 20,000-user scenario, software maintenance costs for Entrust are far greater than for VeriSign, whose annual maintenance charge is against local hosting software costing only $20,000. However, Entrust gains significant savings in certificate distribution and help desk support costs from its managed PKI of 18-45 percent.

Scenario 2 Cost Finding

The five year TCO for Entrust/Direct and VeriSign OnSite are within 4-5 percent, however the allocation of costs differ as follows:

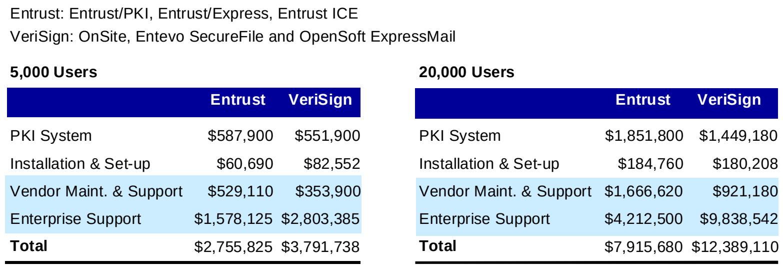
- **VeriSign users sustain 2-29 percent lower PKI system and installation costs than Entrust**
- **VeriSign users sustain 86-95 percent lower maintenance costs than Entrust**
- **Entrust users sustain much lower costs for ongoing end user certificate management**
- **Entrust users sustain 18 percent to 45 percent lower help desk and other related PKI support costs**

Scenario 3

Entrust/PKI With Entrust/ICE and Entrust/Express and VeriSign OnSite With Entevo (QueriSoft) SecureFile and OpenSoft ExpressMail

Scenario 3 takes us beyond the realm of Web-based applications to examine the two most common enterprise applications that use public key cryptography: desktop file encryption and secure e-mail, using S/Mime. In this scenario we have included the cost of the two enterprise applications, one being actually an email plug-in, in the cost of the PKI system for both vendors. The PKI system and applications, together with installation, favor VeriSign by 2 percent in the 5,000-user scenario and by 20 percent in the 20,000-user scenario. The major difference between the two vendors doesn't emerge, however, until costs for certificate life-cycle management, and especially key backup and recovery, are taken into account. Figures 6 and 7 provide the details.

Figure 6: Five Year TCO of Managed Identities for Two Enterprise Applications – Scenario 3



Entrust: Entrust/PKI, Entrust/Express, Entrust ICE
VeriSign: OnSite, Entevo SecureFile and OpenSoft ExpressMail

5,000 Users

	Entrust	VeriSign
PKI System	$587,900	$551,900
Installation & Set-up	$60,690	$82,552
Vendor Maint. & Support	$529,110	$353,900
Enterprise Support	$1,578,125	$2,803,385
Total	$2,755,825	$3,791,738

20,000 Users

	Entrust	VeriSign
PKI System	$1,851,800	$1,449,180
Installation & Set-up	$184,760	$180,208
Vendor Maint. & Support	$1,666,620	$921,180
Enterprise Support	$4,212,500	$9,838,542
Total	$7,915,680	$12,389,110

Source: Giga Information Group

Figure 7: TCO/User/Year — Scenario 3

	5,000 Users	**20,000 Users**
Entrust	$110	$79
VeriSign	$151	$124

Source: Giga Information Group

Scenario 3 is the most complicated of the lot since it involves costs not only for end-user management of certificates and attendant help desk costs, as did the preceding two scenarios, but also significant costs for key backup and key recovery. In this scenario, if keys are lost for encrypted data or encrypted e-mail, the data and messages are lost forever. How significant is key loss in this environment? Our interviews with customers show that it is very significant. Customers using applications that require password access to encryption keys report that 25 percent to 40 percent of their users forget the password to unlock their keys over the course of a year. Entrust's PKI and Entrust-Ready applications like Entrust/ICE and Entrust/Express include automatic key backup and recovery capabilities as part of the other key life-cycle services provided by the Entrust/PKI. In the case of VeriSign, however, these capabilities are provided only by manual means.

Scenario 3 Cost Finding

The five year TCO for Entrust products yielded 27 percent to 36 percent cost savings when compared with VeriSign products, based on the following:

- **While sustaining 2-20 percent lower product and installation costs, VeriSign users sustain significantly higher operating costs for manual key update and manual key backup and recovery.**

Total Economic Impact Analysis: Benefit

Our preceding cost analysis has already made explicit mention of the operating benefits that Entrust's managed PKI has over VeriSign's unmanaged PKI. Entrust's sometimes higher product costs and higher maintenance costs were greatly offset by the cost savings to end users and help desk workers in the managed PKI environment. It is worth remembering, too, that in an extranet or Internet application a large part of the operating costs of a PKI are borne by the external organization. The greater the operating burden on them the greater their reluctance to use such technology. Figures 8-10 below are a summary of the differences in enterprise support costs from Figures 2, 4 and 6 above.

Quantitative Benefit in User Operating and Support Costs

Figure 8: Enterprise Support Costs for Basic Certificates for Web Authentication — Scenario 1

	5,000 Users	20,000 Users	5K Cost/usr/yr	20K Cost/usr/yr
Entrust	$557,552 (13%)	$842,708 (35%)	$22	$8.43
VeriSign	$643,921	$1,300,521	$26	$13

Source: Giga Information Group

Figure 9: Enterprise Support Costs for Managed Certificates for Web Authentication — Scenario 2

	5,000 Users	20,000 Users	5K Cost/usr/yr	20K Cost/usr/yr
Entrust	$525,000 (18%)	$712,500 (45%)	$21	$7
VeriSign	$643,880	$1,300,521	$26	$13

Source: Giga Information Group

Figure 10: Enterprise Support Costs for Managed Identities for Two Enterprise Applications — Scenario 3

	5,000 Users	20,000 Users	5K Cost/usr/yr	20K Cost/usr/yr
Entrust	$1,578,125 (44%)	$4,212,500 (57%)	$63	$42
VeriSign	$2,803,385	$9,838,542	$112	$98

Source: Giga Information Group

Benefit Finding for Operating Costs of a Managed PKI

Entrust users receive operating cost savings that range from 13 percent to 57 percent, based on the following:

- **Entrust users sustain lower ongoing end-user certificate distribution costs**
- **Entrust users sustain lower help desk costs**

Benefit of Best-of-Breed Security and Trust Model

When we interviewed users, other benefits of both Entrust and VeriSign appeared, sometimes in stark relief. Remember, no user cited cost as a primary driver of their decision to go with either vendor. Rather, that decision seemed to be based on a cultural alignment toward controlling their own security and trust model or a desire to take advantage of the Web's public utility of security and trust being built in the browser and by VeriSign.

The Voice of the Customer

Entrust customer — a Global 500 financial service company	**VeriSign customer — a Global 500 financial service company**
"We want best-of-breed security where we control the trust model. We want a platform for future e-commerce. A very high standard of security went into our design. Entrust has all the bases covered for our trust model. Having VeriSign control our security and trust model doesn't meet our standards."	"They [companies who insist on only doing their own security] are idiots. They wear tin-foil hats and think someone is looking at them all the time. Command and control as a mentality is over. You need to leverage everything around you to get your job done … Command and control doesn't cut it."

The stark contrast between these two visions of managing security appeared again and again in our interviews. Entrust customers share a concern for best-of -breed security solutions that are under their control and managed by them. VeriSign's customers were content with the Web's *de facto* security model, as being built by the browser vendors and VeriSign. In fact, they believe that only a general trust utility can achieve the global scale required for trust on the Web. As one of them put it: "VeriSign is a visionary. They have a public utility that works. They are a single, focused company. It takes a public utility to make a global impact." It is this faith in the public utility of trust that is being built on the Web, in contrast to a totally controlled best-of-breed security solution, that gives them the confidence to outsource their security management and trust model to VeriSign.

It seems that this position is as much a starting point as a conclusion with the customers we interviewed. It is a premise on the basis of which they make their decisions, a part of the enterprise's cultural DNA, rather than a conclusion they come to. It is tempered, we believe, by some of the flexibility they find, especially in the VeriSign solution (more on this topic in the "Flexibility" section). VeriSign's users seem to be taking more of an experimental and wait and see approach to the PKI. This makes them more willing to rent one and try it out rather than building a solution of their own. Entrust's customers seem to know exactly what they want, what they will do with it, and move aggressively to implement it.

We will have to see whether time and experience will modify these starkly opposed positions and allow movement from one side to the other of this security divide. However, even Entrust's most ardent supporters see the occasional use for VeriSign's trust model as a bootstrapping process to their own PKI. In order to use Entrust's managed PKI, special desktop software must be downloaded to the client. How can this be done in a trusted manner? One of Entrust's customers uses an SSL-enabled Web server using VeriSign server certificates for this purpose. Once the Entrust client software is installed, the Entrust PKI is established and supercedes the VeriSign PKI.

Benefit Finding

Entrust's customers are looking for a best-of-breed security solution that is under their complete control. The centrally managed Entrust PKI with full certificate life cycle services meets those needs. VeriSign's customers are more experimental in their outlook, looking for mix-and-match components with the *de facto* security standard the Web provides. They believe that ultimately such a public utility will prevail over any best-of-breed model that doesn't have the worldwide scope of the Web. A hybrid trust model, in which VeriSign public server certificates are used to run an SSL server to download Entrust software, which then supercedes the VeriSign PKI, is one solution to overcoming the start-up problems of a private PKI.

Benefit of a Managed PKI

The users we interviewed confirmed the findings in our cost analysis of the benefits of a managed PKI.

Voice of the customer:

- *"It [Entrust's automatic certificate rollover] is excellent … Will really save us in the future ... No interruption of service — works really well."*
- *A customer on the support costs of Entrust's managed PKI: "Cost of technical support is way below what was budgeted."*
- *A VeriSign customer on the importance of dual keys for nonrepudiation* [Note: VeriSign does not support dual keys yet]*: "Function of two separate keys is really valuable when you go to key recovery."*

How important is a good key backup and key recovery system? We were surprised to find from speaking to customers that 25 percent to 40 percent of users forget their key password over the course of a year. This makes key backup and recovery essential to the operation of enterprise applications in Scenario 3. Without such a system, the risk of loss of access to encrypted data becomes very high. But with key backup and recovery comes the issue of nonrepudiation and the necessity of having two keys to support that function. Entrust's key backup and key recovery system, with dual key support, solves these problems and makes enterprise applications with a PKI practical.

VeriSign and Netscape have recognized the importance of a managed PKI and have made announcements about supporting automatic certificate rollover, key backup and key recovery, and dual keys in future releases of their software. These features will probably appear over the course of the next 4-8 months. Obviously, such features would change the competitive profile of Entrust and VeriSign. As these features become available and users gain experience with them, we will have to revisit our cost model.

Another important feature of Entrust's PKI is automatic CRL checking. This feature has been absent from VeriSign's PKI offering, but recently a plug-in has been provided to do server-side CRL checking. However, client-side CRL checking is still missing. Three out of four VeriSign customers had problems with the manual-based CRL checking mechanism, apparently prior to the availability of VeriSign's CRL checking plug-in. One had an issue in synchronizing their directory with VeriSign's CRL directory. Two others went to the trouble of writing their own application to automatically check CRLs at the server. They described this as a "significant" effort, about two person-months. But such an application, or the recently available VeriSign server plug-in, does not help applications that require CRL checking at the client, e.g., secure email.

Benefit Finding

Interviews with customers confirm the importance of a managed PKI revealed by the cost model numbers. Customers report that Entrust's managed PKI works well and saves them money on support costs. Although VeriSign recently provided a server plug-in to do automatic server-side CRL checking, there is still no automatic CRL checking on the client. VeriSign and Netscape have recognized the importance of a managed PKI and will probably begin the phased support for this over the next four to eight months.

Total Economic Impact Analysis: Flexibility

Perception of flexibility is one of the areas where VeriSign shines. In our interviews we found VeriSign's customers liked the idea of leasing a PKI for the perceived flexibility it provided them, one of the traditional reasons for leasing rather than buying goods. Although one usually thinks of a PKI as a long-term infrastructure investment, one VeriSign customer we spoke with said they went with the company because they weren't really sure how to proceed with their PKI plans and wanted to try one out first. Following a "try before you buy" scenario, this company planned to issue a request for proposal (RFP) for a more permanent PKI after a year of testing VeriSign's.

Another VeriSign customer said their business people didn't know at what rate they would issue certificates. With no revenue stream to easily identify, they didn't want capital and depreciation costs to hit their books, so they found it more financially advantageous to rent a PKI than buy one.

Yet another VeriSign customer was going to issue certificates to clients of their own main customer. They did not want to become an intermediary between their customer and their customers' clients. VeriSign served as a neutral party for issuing certificates.

Entrust's customers found flexibility less in the external arrangements of the PKI and more in the ability to follow their own dictates and assemble the PKI as they saw best. The flexibility to be master of their own destiny and in control of their own security and trust policies was their prime motivator.

Flexibility Finding

VeriSign's customers like the idea of leasing a PKI for the flexibility it provides them in its external arrangements. They can "try before they buy," optimize capital and depreciation costs through rental rather than purchase, or use VeriSign as a neutral third-party issuer of certificates. Entrust's customers enjoy the flexibility of being in control of their own security and optimizing the PKI as they best see fit.

Total Economic Impact Analysis: Risk

Implementation Risk

According to VeriSign's own marketing, minimizing the perceived risk of implementing a PKI is one of the company's main value propositions. This, together with a quick time to market of PKI-dependent applications, is the reason VeriSign says you should lease their PKI rather than buy and install one of your own. What we found in talking to VeriSign's customers was something quite different. Although it could have been a result of selection error from the small population of user we spoke with, all of the VeriSign customers we talked to generally took 1.5 times to two times longer to implement their PKI and applications than did Entrust's customers. Both VeriSign's and Entrust's customers took the same amount of time in planning and designing their PKI, generally three to six months, sometimes more. Implementation time, after planning, was four to six weeks for Entrust and six to 12 weeks or more for VeriSign.

We found several reasons for this surprising result. The main reason seems to be that VeriSign's customers are less sure of how to proceed with their PKI, what they want it for, how extensive it should be, etc. In general they are less aggressive about rolling it out. Therefore, time sensitivity is not an issue for them. Entrust's customers, on the other hand, are much more confident of their purposes and move aggressively to implement their PKI. This goes back to the flexibility issue above. Being somewhat less certain of themselves, VeriSign's customers move more slowly and enjoy the benefits of a rental program rather than having to pay for and implement a product.

Some of the VeriSign customers we spoke with were implementing a directory for the first time. A directory is a key component of a PKI. Most of the PKI system integrators we speak with say implementing a successful directory system is the real key to a successful PKI. Whether you rent a PKI or buy one, you are likely to implement your own directory for it. Since this piece of infrastructure is on the critical path to a PKI implementation, it is likely to slow down all PKI deployments, whether you rent or buy.

There were other reasons that were peculiar to each VeriSign user we talked to for relative slowness of implementation. One user had a problem getting through their firewall to the VeriSign servers. Another user found the back and forth of dealing with an external organization to take more time than expected. Although it seems intuitive that implementing an already running service should be more timely than getting a product running from zero, that was not the experience of the users we talked to. Working with an outside organization sometimes takes its toll. In general, the VeriSign users we spoke with said they were surprised that it took them longer to implement their PKI than they expected.

The Entrust customers we spoke with found their Entrust implementations relatively straightforward and painless. While PKIs have a reputation of being hard to implement, one Entrust user commented that it was "not hard at all."

One issue to bear in mind when establishing a managed PKI that supports an extranet application is the possible resistance of outside organizations to having software loaded on their PCs. This resistance would make it difficult to have a managed PKI.

Users of both VeriSign and Entrust began with a pilot project before moving on to wider implementations. Many projects were still in the pilot stage with around 1,000 users or fewer. Thus, it is premature to predict the scalability of either solution, although it should be noted that one Entrust user we spoke with does have an implementation of 50,000 active users.

Implementation Risk Finding

VeriSign users we spoke with tend to have longer implementation cycles by a factor of 1.5 times to two times Entrust users. This was due to greater uncertainty about how to proceed with their PKI, perhaps reflecting their interest in a PKI service rather than a product. VeriSign users also experienced delays in interactions between their company and VeriSign. Cross-organization communication delay seemed to be the culprit here. Scalability of both solutions remains uncertain until more users have gone beyond the pilot stage in their PKIs. In an extranet setting, the reluctance of outside organizations to load special software on their desktops could make it difficult to have a managed PKI.

Total Economic Impact Analysis: Vendor Risk

We found Entrust's customers unusually vocal in their approval of the company, some even holding the company in adulation. The terms that came up the most often in their description of Entrust were "fantastic" and "excellent." Specifically cited for praise was Entrust's support organization.

The voice of the customer:

- *"Entrust is very responsive."*
- *"Entrust support organization was fantastic". "[They] bent over backwards to help, even when we were just in evaluation mode. Entrust rewrote Entrust client for Unix during the evaluation trial for us."*
- *"Fantastic company in terms of listening to customer requirements."*
- *On automatic certificate rollover: "It is excellent. [It] will really save us in the future."*

VeriSign's customers, while generally giving the company very high marks, did not share quite the same level of enthusiasm as Entrust's customers. One VeriSign customer said the rapid growth of the company meant there were always new faces in meetings, which slowed down the deployment of their PKI. This seems to have settled down as of June 1998.

Voice of the customer:

- *"VeriSign is a visionary. They have a public utility that works … It takes a public utility to make a global impact."*
- *"When we had a problem they put on the gas to fix it … [They] showed up in force to fix it."*
- *"VeriSign really knows their stuff. But every time we talked to them there were two or three new people in the room … [It] finally settled down in June."*

Vendor Risk Finding

Entrust's customers hold the company in unusually high regard, verging on adulation. Entrust is especially good at listening to customer requirements and their support organization is described as "fantastic." VeriSign's customers call the company "visionary," and it is responsive to their support needs. Rapid growth at VeriSign sometimes meant too many new people at meetings, slowing down PKI deployment. This problem has diminished since June 1998.

Appendix A

Figure 1

Basic Certificates for Web Authentication – Scenario 1

Entrust: Entrust/Web Connector

VeriSign: OnSite

Issuing 5,000 Certificates/Yr

	Entrust	VeriSign	% Saved Using Low Cost Vendor
Hardware Components	$8,000	$0	NA
Certificates/Licenses	$22,523	$146,126	85%
Directory	$1,502	$0	NA
CA Software	$15,000	$0	NA
Other CA components	$5,000	$0	NA
PKI System (Subtotal)	$52,024	$146,126	64%
Installation & Set-up	$33,276	$31,279	6%
Vendor Maint. & Support	$26,551	$0	NA
Ongoing Cert. Distb'n	$32,552	$81,396	60%
Ongoing Support	$525,000	$562,525	7%
Enterprise Support (Subtotal)	$557,552	$643,921	13%
Total	$669,403	$821,327	18%

Issuing 20,000 Certificates/Yr

	Entrust	VeriSign	% Saved Using Low Cost Vendor
Hardware Components	$8,000	$0	NA
Certificates/Licenses	$75,023	$344,100	78%
Directory	$5,002	$0	NA
CA Software	$15,000	$0	NA
Other CA components	$5,000	$0	NA
PKI System (Subtotal)	$108,024	$344,100	69%
Installation & Set-up	$82,104	$85,104	4%
Vendor Maint. & Support	$29,701	$0	NA
Ongoing Cert. Distb'n	$130,208	$325,521	60%
Ongoing Support	$712,500	$975,000	27%
Enterprise Support (Subtotal)	$842,708	$1,300,521	35%
Total	$1,062,538	$1,729,725	39%

Figure 2

Managing Certificates for Web Authentication – Scenario 2
Entrust: Entrust/Direct
VeriSign: OnSite

Issuing 5,000 Certificates/Yr

	Entrust	VeriSign	% Saved Using Low Cost Vendor
Hardware Components	$8,000	$4,000	50%
Certificates/Licenses	$157,500	$146,100	7%
Directory	$11,900	$11,900	No Difference
CA Software	$15,000	$0	NA
Other CA components	$0	$20,000	NA
PKI System (Subtotal)	$192,400	$182,000	5%
Installation & Set-up	$60,690	$66,276	8%
Vendor Maint. & Support	$173,160	$24,000	86%
Ongoing Cert. Distb'n	$0	$81,380	NA
Ongoing Support	$525,000	$562,500	7%
Enterprise Support (Subtotal)	$525,000	$643,880	18%
Total	$951,250	$916,156	4%

Issuing 20,000 Certificates/Yr

	Entrust	VeriSign	% Saved Using Low Cost Vendor
Hardware Components	$8,000	$4,000	50%
Certificates/Licenses	$495,000	$344,100	30%
Directory	$38,800	$38,800	No Difference
CA Software	$15,000	$0	NA
Other CA components	$0	$20,000	NA
PKI System (Subtotal)	$556,800	$406,900	27%
Installation & Set-up	$182,760	$115,104	37%
Vendor Maint. & Support	$501,120	$24,000	95%
Ongoing Cert. Distb'n	$0	$325,521	NA
Ongoing Support	$712,500	$975,000	27%
Enterprise Support (Subtotal)	$712,500	$1,300,521	45%
Total	$1,953,180	$1,846,525	5%

Figure 3

Managing PKI IDs for Enterprise Applications –
Scenario 3
Entrust: Entrust/PKI, Entrust/Express, Entrust/ICE
VeriSign: OnSite, QueriSoft SecureFile and OpenSoft Express Mail

Issuing 5,000 Certificates/Yr

	Entrust	VeriSign	% Saved Using Low Cost Vendor
Hardware Components	$8,000	$8,000	No Difference
Certificates/Licenses	$553,000	$492,000	11%
Directory	$11,900	$11,900	No Difference
CA Software	$15,000	$0	NA
Other CA components	$0	$40,000	NA
PKI System (Subtotal)	$587,900	$551,900	6%
Installation & Set-up	$60,690	$82,552	26%
Vendor Maint. & Support	$529,110	$353,900	33%
Ongoing Cert. Distb'n	$0	$162,760	NA
Ongoing Support	$1,578,125	$2,640,625	40%
Enterprise Support (Subtotal)	$1,578,125	$2,803,385	44%
Total	$2,755,825	$3,791,738	27%

Issuing 20,000 Certificates/Yr

	Entrust	VeriSign	% Saved Using Low Cost Vendor
Hardware Components	$60,000	$18,380	69%
Certificates/Licenses	$1,738,000	$1,312,000	25%
Directory	$38,800	$38,800	No Difference
CA Software	$15,000	$0	NA
Other CA components	$0	$80,000	NA
PKI System (Subtotal)	$1,851,800	$1,449,180	22%
Installation & Set-up	$184,760	$180,208	2%
Vendor Maint. & Support	$1,666,620	$921,180	45%
Ongoing Cert. Distb'n	$0	$651,042	NA
Ongoing Support	$4,212,500	$9,187,500	54%
Enterprise Support (Subtotal)	$4,212,500	$9,838,542	57%
Total	$7,915,680	$12,389,110	36%