The Total Cost of Ownership for Voltage Identity-Based Encryption Solutions

A White Paper by Ferris Research

May 2006. Report #586

Commissioned by Voltage Security

Ferris Research, Inc.
408 Columbus Ave., Suite 1
San Francisco, Calif. 94133, USA
Phone: +1 (415) 986-1414
Fax: +1 (415) 986-5994
www.ferris.com

Recent Reports From Ferris Research

Microsoft's Latest Push for Notes and Domino Migration

Snapshot: Lucid8 GOexchange Preventive Maintenance

Exchange Reliability and Its Impact on Organizations

Snapshot: Teneros--Application Continuity Appliance for Microsoft Exchange

Implementing Email Archiving

The Benefits of Integrating Enterprise Content Management Systems and Team Workspaces

Enterprise Mobile Messaging Survey

The Email Archiving Market, 2006-2010

Exchange 12 Assessment

Anti-Spam Technology in the Asia-Pacific Region

Why Exchange 12 Will Be 64-Bit Only

Top 10 Messaging & Collaboration Issues: 2006

The SyncML Standard and Its Impact on Mobile Messaging

Boundary Email Security: The First Line of Defense

Oracle Content Services: An Alternative to SharePoint Services for Enterprise Content Management

The Plan for AOL Instant Messaging

The Email Security Market, 2005-2010

Techniques for Zero-Hour Virus Protection

New Features and TCO Benefits of IBM Lotus Notes/Domino 7 Implementing the Sender ID Framework in DNS

Introduction to Presence Models and Standards

Proofpoint’s Content Security and Regulatory Compliance Offering

Using Content Security to Achieve Regulatory Compliance

Microsoft Operations Manager (MOM) 2005 and Exchange Server 2003 Management Pack for MOM

The Total Cost of Ownership of IBM Notes/Domino 6

Zero-Hour Anti-Virus Defense

New Features of IBM Lotus Notes/Domino 6

New Developments in Virus Control

Wikis

The Global Economic Impact of Spam, 2005

Calculating Spam Costs for Your Organization

Adomo Voice Messaging for Exchange: A Messaging-Centric Approach to Voicemail

Key Trends in Messaging and Collaboration, 2005-2010

Email Archiving: In-House, Outsourced, or Hybrid?

Table of Contents

Table of Figures

Executive Overview

This report examines the total cost of ownership (TCO) of Voltage Security's identity-based encryption (IBE) system, and compares it with the TCO of a typical public key infrastructure (PKI) system.

We surveyed and interviewed users and resellers of PKI and Voltage IBE systems to discover the real-world parameters driving the TCO of these systems. We then built a TCO spreadsheet, based on the standard Ferris Research TCO model.

In this report, we include an overview of IBE in general and Voltage's IBE system in particular. We then discuss our findings on Voltage's TCO and how it compares with traditional PKI-based encryption. Finally, the Appendix explains our financial analysis and the associated Excel calculator, which organizations can adjust to their own situations.

The findings from our research are summarized below:

- Overall, the TCO of a typical Voltage IBE system is one-third the TCO of a typical PKI system.
- The Voltage IBE system needs a far simpler infrastructure than does a typical PKI system, meaning fewer servers and easier installation.
- Operations costs for a typical Voltage IBE system are one-fifth those of a typical PKI system.
- User productivity losses for the Voltage IBE system are three times lower than those for a typical PKI system.

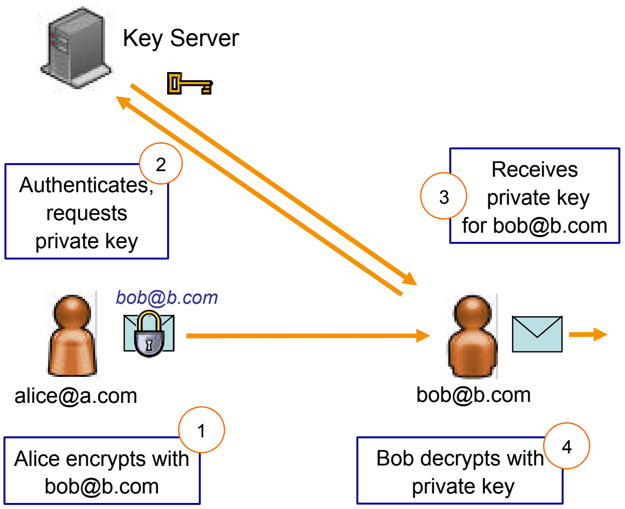
IBE: A Brief Introduction

Identity-based encryption is an alternative form of public key cryptography. It enables a simple *identity*—such as an email address—to be used to generate a public key. This eliminates the need for certificates in the system, which in turn greatly reduces the complexity for end users and administrators.

Example of IBE

The simplified example in Figure 1 shows Alice sending an encrypted message to Bob. Alice uses Bob's email address to generate his public key.

FIGURE 1 SENDING AN ENCRYPTION MESSAGE USING VOLTAGE


Key Server
2
Authenticates, requests private key
3
Receives private key for bob@b.com
bob@b.com
alice@a.com
bob@b.com
1
Alice encrypts with bob@b.com
4
Bob decrypts with private key

Alice sends Bob encrypted email using his identity to generate his public key.
Source: Voltage Security

Alice and Bob need not work for the same organization. The IBE system will work as long as the key server is accessible to Bob. Alice's organization owns the key server, but Bob can decrypt the message because he has access to Alice's IBE key server through the Internet. Alice only needs access to the server at the point of initial installation on her desktop (or if she needs to decrypt a message).

Of course, for Bob to receive his private key, he must be able to authenticate to Alice's IBE server, and this authentication must be sufficiently strong. This could be done simply by Alice telling the IBE server to send a confirmation message to Bob. The message would contain a URL for him to click and thus confirm his identity. Other stronger but more complex methods of authentication are also available, such Active Directory/LDAP, username/password, or RSA SecurID.

Potential Advantages of IBE

Simplicity Without Certificates

Unlike a conventional public key infrastructure, IBE does not require complex pre-enrollment or revocation checking. There is essentially no need for certificates. Instead, a recipient's public key is derived from his or her identity.

An IBE system also does not require a complex PKI to generate, certify, decertify, and store individual public keys. IBE is so simple because *the public key is based on the email address* (or some other identity).

The only information the IBE server permanently stores is a "master secret"—essentially a large random number that is exclusive to the security domain. The server uses the secret for two purposes:

- To create a common set of public key parameters, which are given to each user who installs the IBE software. The parameters contain a "seed," the current week number, and the address of the server.
- To create this week's private key for each recipient, which is given to each recipient (or agent) on demand when required.

A new public key is constructed for each recipient and week from three components:

- The public key "seed."
- The current week number.
- The recipient's identity (e.g., his or her email address).

No Pre-enrollment

In the example above, this may be the first time Bob has ever used encryption. The IBE server can issue him a suitable key to decrypt the message on an "on-demand" basis. In other words, Bob does not need to be "signed up" for encryption before Alice sends the message.

Key Expiration Instead of Revocation

One of the most difficult problems for a PKI system to address is *revoking* public keys if they get compromised or if an employee leaves. IBE addresses this problem by including a week number when generating public keys. Thus, the IBE system must issue a new private key to each recipient every week.

Note that the time period is typically one week—the default in the Voltage system. However, it is up to the operator of an IBE system to determine how rapidly keys should roll over.

Reduced Vulnerability to Spammers

Another important yet often-overlooked advantage of IBE is that an organization does not need to publish a list of valid email addresses (i.e., a directory of certificates). Such a list can be vulnerable to spam address harvesters.

Time Travel Using IBE

With IBE, a sender can encrypt a message that cannot be decrypted until a specified date in the future. Returning to our example, Alice could send a message with information that is embargoed until the following week by encrypting the message with a public key generated for that week.

IBE vs. PKI: Total Cost of Ownership

Ultimately, IBE's simplicity is likely to have TCO advantages over traditional PKI systems. This report quantifies those advantages so potential customers can estimate the TCO for their situation.

Summary of Voltage's IBE Offering

Voltage has implemented a set of software products that allows organizations to employ IBE to encrypt and decrypt email messages.

The Voltage Product Structure

Voltage's offering mainly consists of the following products.

Voltage SecureMail IBE Server

This is a set of Web (HTTP) accessible Voltage servers that can be hosted on a single shared computer system or on multiple distinct systems. It provides:

- *An enrollment service*, which authenticates a user using organizationally specified credentials, such as a name and password.
- *A key service*, which issues private keys and enables the master secret and records logs to be backed up and restored.
- *A management service*, which controls how users authenticate (e.g., using Active Directory or a single-sign-on service).
- *A Web-browser-based decryption service* for email recipients who cannot or have not installed a decryption plug-in.

Email Client Plug-ins

Plug-ins are currently available for IBM Lotus Notes, Microsoft Outlook, and Microsoft Outlook Express. These support both the encryption and decryption of email messages by individual users.

Gateway Software

This puts all the server components onto an appliance that can be integrated with other message protection services, such as anti-spam and anti-virus products. The gateway software supports both the encryption of email messages exiting an organization and, optionally, the decryption of messages entering an organization based on policy.

Policies can also be defined to control when an email is encrypted. These policies may also be defined in a content scanning solution.

How the Voltage IBE System Works

The Voltage IBE plug-in provides a relatively transparent and easy-to-use way to send and receive encrypted email.

Sending a Message Using a Plug-in

Alice composes an email to Bob and presses the “send secure” button. Behind the scenes, the message is encrypted using Bob’s email address combined with additional elements—the week number and the public key seed—that are common to all senders.

Receiving a Message Using a Plug-in

When Bob receives a secure email from Alice for the first time, he is asked to authenticate. By doing so, a private key for that week is cached on Bob’s PC. Bob can now read his secure message just by opening it. For subsequent messages sent to Bob from Alice’s company, Bob does not need to go online and authenticate until the cached key expires. Then he can fetch his private key for the new week.

If Bob’s company is also running the Voltage IBE system, the system automatically federates to enable Bob to authenticate against his own system.

Receiving a Message Without a Plug-in

If Bob does not have a plug-in, he receives text with instructions on how to read Alice’s message. It tells him to open the HTML attachment, which prompts him to authenticate by entering his username/password. Bob is then presented with the decrypted message in his browser. He can reply or forward securely, in a similar manner to traditional Web mail.

Behind the scenes, Alice’s entire message arrives in Bob’s inbox. By opening the attachment and authenticating, the encrypted message is posted back to Alice’s server and decrypted on-demand. The benefit of this approach is that Bob can easily decrypt the message any time in the future.

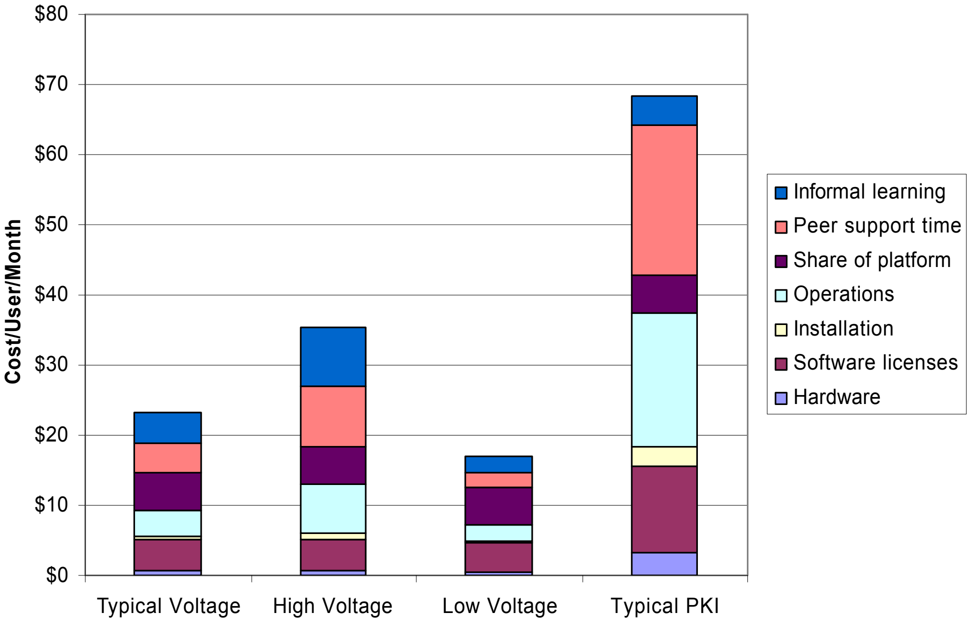
TCO Assessment

This section shows the results of running the Ferris Research TCO model spreadsheet with its default values, to compare the Voltage IBE and PKI systems. The model is described in the Appendix, along with instructions on downloading and customizing the spreadsheet to represent an organization's likely TCO.

TCO Elements

Figure 2 illustrates the range of TCO costs for Voltage and PKI systems, broken down by TCO element.

FIGURE 2 TCO ELEMENT COMPARISON SUMMARY



Even in the high-TCO scenario, Voltage has an almost 2:1 advantage over a typical PKI system.

Note that our model offers "bracketed" cost scenarios—high, typical, and low—based on varying cost assumptions. This demonstrates a cost *range* rather than a single "magic" number.

The typical examples from the model show the TCO per user per month for the Voltage system is around $25, compared with nearly $70 for a PKI system—approximately one-third the cost.

Hardware

The Voltage IBE system requires very few servers to operate. Whereas typical PKI systems often require one or more servers per email store, the typical Voltage installation requires just one pair of key servers and a failover clustered pair of zero-download Web servers.

The Voltage system requires fewer servers because its architecture is almost *stateless*—that is, the servers store hardly any information permanently. Keys are not stored on, managed using, or backed up from the servers. Instead, they are generated automatically from the identity.

Typical PKI systems require high-bandwidth/low-latency connectivity to the server. This increases the server hardware requirement because each site needs servers.

The typical examples from the model show the amortized hardware cost per user per month for the Voltage system is around $0.50, versus $3.50 for a PKI system—approximately one-fifth the cost.

The high-TCO scenario does not increase the hardware cost, but the low-TCO scenario saves money by including only one key server and not implementing failover for the Web server.

Software

Up-front costs for the Voltage software are about two-thirds the costs of a comparable PKI system. Support and maintenance are typically similar percentages of the up-front costs.

The standard example from the model shows the amortized software cost per user per month for the Voltage system is around $4.50, versus $19.00 for a PKI system—approximately one-third the cost.

There is no cost difference between the high-TCO and typical-TCO scenarios. Software in the low-TCO scenario is less expensive because fewer servers are needed.

Installation

Because of its minimum-state design, the installation and upgrade process for the Voltage server is far simpler than the typical PKI process. Fewer servers and less state mean easier installation.

The standard example from the model shows the amortized installation cost per user per month for the Voltage system is around $0.50, versus $3.00 for a PKI system—approximately one-fifth the cost.

The high-TCO scenario assumes that installation and major upgrades cost twice the typical amount. Low-TCO installation costs are half the typical value.

Although typical PKI systems take substantially more effort to install than a Voltage system, the costs are small compared with the total costs.

Operations

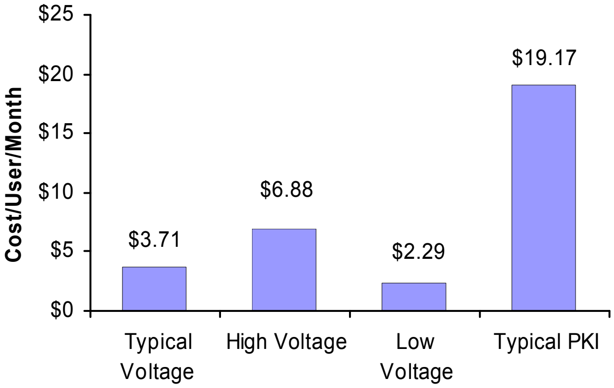
Of all the cost comparisons for two competing products, people costs typically show the greatest differences. This analysis is no exception.

Our research shows that:

- Voltage needs less “care and feeding” from administration staff.
- Help desk calls are simpler and less frequent.
- User training is less onerous.

Once again, the Voltage IBE minimum-state design seems to make for easier operations. As Figure 3 illustrates, typical PKI systems cost much more to run than even the most pessimistic Voltage scenario.

FIGURE 3 OPERATIONS COST SUMMARY



Large savings can be achieved with the Voltage IBE system through reduced operations costs.

The standard example from the model shows the operations cost per user per month for the Voltage system is around $3.50, versus $19.00 for a PKI system—approximately one-fifth the cost.

The high-TCO scenario assumes that the organization has more expensive administrators, who spend twice the typical percentage of time dedicated to Voltage. It also assumes that the help desk load and training time are double the typical amounts. The low-TCO scenario has cheaper administrators, who spend half the typical time, and help desk and training loads that are also half the typical amounts.

Platform

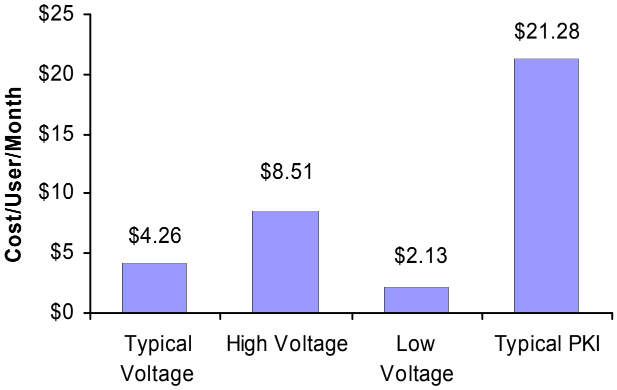
In each of the model’s scenarios, we arbitrarily assume that 1% of the total IT platform’s costs can be assigned to both the Voltage and PKI systems. From our research, $6,500 per user per year is a typical platform cost, so our 1% allocation is approximately $5.50 per user per month.

User Productivity Loss, Including Peer Support

Just as help desk costs are higher in a typical PKI environment, informal peer support also costs more. Once again, "hidden" people costs have a strong influence on the relative TCOs.

As Figure 4 shows, the complexity of typical PKI systems means that peer support can be a major issue. This inevitably leads to substantial productivity loss, with its associated costs.

FIGURE 4 PEER SUPPORT COSTS



The Voltage system yields even larger savings in the area of productivity loss because peer support costs are lower.

Peer support is by far the largest contributor to user productivity loss. The standard example from the model shows the productivity loss cost per user per month for the Voltage system is around $8.50, compared with $26.00 for a PKI system—approximately one-third the cost.

Summary of Key Cost Differences: PKI vs. Voltage

- Overall, the TCO of a typical Voltage IBE system is one-third the TCO of a typical PKI system.
- Operations costs for a typical Voltage IBE system are one-fifth those of a typical PKI system.
- User productivity losses for the Voltage IBE system are one-third those of a typical PKI system.

Author: Richi Jennings
Editors: Mona Cohen, Sue Hildreth
Peer review: David Ferris, Nick Shelness, David Via

Voltage's Sponsorship of This White Paper

Voltage Security commissioned this white paper with full distribution rights. You may copy or freely reproduce this document, provided you disclose authorship and sponsorship and include this notice. Ferris Research independently conducted all research for this document and retained full editorial control.

Appendix: The Ferris Research TCO Model

The Ferris Research TCO Model helps messaging system administrators gauge the relative effectiveness of their systems, cut costs, and make better decisions about where to invest time and money. We have been developing our model gradually and iteratively since 1991. In our first analysis that year, we looked at the costs of the PROFS email system for IBM mainframes.

The TCO model breaks down costs into the amount spent per user per month for expenses in three main categories:

- *Direct costs*. These are the items that messaging managers usually think of when they cost their systems. This category includes the costs for hardware, software, operations staff, and major upgrades.
- *Platform costs*. Organizations need a general IT infrastructure before they can add the specialized elements required to support email. This infrastructure includes items such as personal computers, networks, and support staff. A percentage of these costs is often allocated to encryption.
- *User productivity loss costs*. Any application can result in some loss of productivity. Time spent dealing with problems or answering colleagues' questions about how to use certain features, for example, results in productivity losses that should be considered in the cost analysis.

Notes About Our Model Design

In creating any financial model, designers inevitably make choices that can dramatically affect the results produced. For this model, a number of items are worth noting.

Downtime

When an email system becomes unavailable, business is disrupted. This is especially true if the outage lasts a long time. The resulting economic losses to an organization can vary enormously. We often include the cost of downtime in a TCO calculation.

Our downtime cost estimates are based solely on the projected hourly personnel cost per mail user (see Employee Costs below). The unavailability of email could have a much more dramatic impact, such as losing an important sale or delaying a critical project. However, such losses are difficult to quantify.

In this case, however, we suggest ignoring the cost of downtime. Availability statistics for different organizations are contentious and vary wildly. In addition, calculations of productivity loss due to downtime have a disproportionate impact on TCO. Your needs may differ, and the TCO model allows you to include your downtime figures.

Platform and User Productivity Loss Costs

Our model includes costs for the platform (e.g., server hardware, software) and for user productivity loss. Many other TCO studies are limited to those costs that messaging managers directly control. If desired, organizations can confine their analysis to the elements under the heading of Direct Costs.

High, Typical, and Low Costs

Our model offers "bracketed" cost scenarios—high, typical, and low—based on varying cost assumptions. This demonstrates a cost *range* rather than a single "magic" number.

Software Maintenance

Many software vendors include the first year of maintenance in the price of the initial software license. Our model represents software maintenance on an annual basis as a separate cost that is calculated as a percentage of the initial license cost. To ensure that software maintenance costs are not counted twice, we have proportionally reduced the estimated software license costs from the typical prices.

Employee Costs

We assume that the average email user costs an organization $80,000 annually. This figure is based on information provided by the U.S. Bureau of Labor Statistics for white-collar workers. It includes salary, benefits, office space, and relevant taxes. We further assume an average work year of 1,880 hours. Thus, the projected cost of user time for productivity and downtime purposes is a little more than $40 per hour.

In the United States, a 50% markup on salary is typical to account for overhead. In some European countries, a 100% markup is more appropriate, although average salaries may be lower. Salaries and overhead clearly vary from country to country, and readers may need to make adjustments for their particular environment. Nevertheless, the U.S. figure is appropriate for a wide range of developed economies.

Allocation of Platform Costs to Messaging

The allocation of platform costs to email and messaging is subjective. Encryption makes this especially challenging because organizations that use this platform for email may also use it for encrypting other information. In our TCO model, we have settled on a 1% allocation.

Period of Depreciation

We assume three-year, straight-line depreciation for up-front costs, such as hardware and software.

Accompanying Spreadsheet

We have created an Excel spreadsheet workbook to implement the TCO model. This file can be downloaded from www.voltage.com/tco.

This workbook contains three spreadsheets representing low, typical, and high direct TCO models. We recommend customizing the typical direct TCO spreadsheet to analyze a particular organization's TCO.

For a detailed description of the individual line items in the spreadsheets, refer to the cell comments. These can be viewed by positioning the cursor over the small red triangle in the top right corner of the commented cells.

Every organization's TCO is different. The results in the spreadsheet are estimates based on our survey research.

Customizing the Model

The model has various parameters that you can adjust to match your circumstances better. You can find these in the *Assumptions* sheet in the workbook. The parameters include:

- Number of users (internal and external).
- Lifetime of investment.
- Annual fully loaded cost of a full-time worker.

The default values we put into the model represent a typical 1,000-user organization that is headquartered in a major U.S. city and has smaller, satellite offices in two other U.S. cities, two European cities, and one Pacific Rim city. The organization's users all have access to encryption and are distributed 50% at headquarters and 10% in each satellite. In total, the users communicate with an additional 10,000 external users. The organization has a three-year investment horizon for an encryption infrastructure.

More About the TCO Elements

The essence of the TCO model is to combine all the cost elements described below, presenting a single annual TCO figure spread over three years. We chose three years as the expected life of this type of infrastructure investment. If you desire, you may adjust the lifetime in the accompanying spreadsheet (for example, to five years).

The spread in costs is a simple straight-line amortization. No account is made for the time value of money. In other words, the three-year TCO figure encompasses all the initial costs, plus all the annual costs multiplied by three. To reach the final annual cost, we simply divide the total by three.

Server Hardware Platform

With any cryptography mechanism, servers are required to enable some or all of the following functions:

- Issue keys (enroll users).
- Revoke keys (disallow future use of a key).
- Escrow keys (securely store copies of the keys).
- Decrypt messages at the gateway (e.g., for archiving or virus scanning).

Different mechanisms require different amounts of server horsepower. These differences are mainly due to the variation in the roles required, where the servers need to be positioned, and how computationally "expensive" the tasks are.

For example, a classic PKI system needs at least the first three server roles. In addition, it often is necessary to position servers close to their users to reduce network latency effects. In a large, distributed organization, several physical servers will need to perform each role for reasons of scalability.

There may also be network expenses. Any large implementation spanning multiple data centers may incur additional costs of backup, replication, or disaster recovery. In a Voltage IBE infrastructure, only the role of issuing keys is required. Revocation and escrow roles are not necessary because:

- Revocation is implicit, as keys expire (e.g., each week). They cannot be renewed for a user who has left the organization, assuming his or her account gets disabled in Active Directory, etc.
- Escrow is unnecessary, as private keys can be regenerated at will.

Key Integrity

An important problem for a PKI system to solve is key integrity. A PKI system establishes the integrity of each recipient's public key using a pair of methods:

- Digitally signing a recipient's public key using its own private key and embedding the result in a certificate. It also includes its own digitally signed certificate. This allows a sender to check the integrity of the resulting certificate with its hierarchy of embedded certificates before using a recipient's public key.
- Maintaining a list of revoked certificates in a Certificate Revocation List (CRL). Senders must verify that a recipient's public key has not been revoked, by checking whether the certificate ID appears in the CRL.

This is a complex set of tasks for a PKI system to perform. An IBE system does not have to establish the integrity of a public key. A sender simply generates it. An IBE system authenticates each recipient before issuing a private key to that recipient.

This allows the organization to choose an authentication method suited to the message's sensitivity—e.g., simple passwords for regular data, two-factor tokens for critical data.

Organizations can choose from a variety of authentication methods, including Active Directory, LDAP, or an existing single-sign-on infrastructure. Optionally, Voltage's own Enrollment Server can be used. It is designed for external business-to-business (B2B) and business-to-consumer (B2C) recipients, and offers a self-service username/password approach.

Client and Server Cryptography Software

Cryptography software is required to perform and manage the four server roles listed above. Software is also required to perform the actual encryption and decryption at the desktop.

Typically, the cost of the software has both an up-front and a recurring element: the initial purchase price and an annual subscription cost for support and updates. Software may be required at the end points, or other mechanisms may be available that eliminate the need for a software download. For example, Voltage's Zero Download Messenger decrypts the message using only a Web browser.

Installation and Professional Services

These are costs associated with the efforts needed to commission, install, and configure the servers. Also included are the costs for installing software on client devices, such as desktop PCs. Usually, such configuration involves the use of external consultants from professional services organizations.

Typical costs include:

- Integration with authentication mechanisms, both internal and external.
- Customization of the user experience when receiving messages.
- Implementation of a data center backup and failover strategy.

This represents an up-front cost and a cost associated with occasional software upgrades.

IT Staff

This expense category represents the fully loaded time required by the organization's IT staff to operate and manage the infrastructure. It includes tasks such as:

- Configuring users.
- Making and verifying backups.
- Repairing corrupt databases.
- Installing software patches.

Help Desk Staff

The cost of the IT help desk is separate from the previous group. It represents the fully loaded staff expenses associated with helping users who have problems with, and questions about, the cryptography infrastructure. Typical issues requiring help desk attention include:

- "I need a certificate."
- "I've lost my certificate."
- "How do I send encrypted email outside the organization?"
- "I've received an encrypted message that won't decrypt."

Training

Users require training on how to use cryptography software. IT staff require training on how to manage the infrastructure.

Ferris Research

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide with analysts located in North America, Europe, and the Asia-Pacific region.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 1, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

Free News Service

Ferris Research publishes a free daily news service. It provides comprehensive coverage of the messaging and collaboration field, and is a great way to keep current. Topics include spam, email, email retention/archiving, mobile messaging devices, consumer messaging services, Web conferencing, email encryption, email migrations and upgrades, regulations compliance, instant messaging, ISP messaging, and team workspaces.

The news is distributed daily. To register, go to www.ferris.com/forms/newsletter_signup.php. In addition, you will receive one or two emails every month announcing new Ferris reports or conferences. To opt out and suppress further email from Ferris Research, click on the opt-out button at the end of each news mailing.