Email Security - The IBE Architectural Advantage

Overcoming the challenges of Symmetric and PKI-based Messaging

CONTENTS

INTRODUCTION

Email is now the medium of communication for businesses around the world and has become the trusted communication channel for a wide variety of commercial transactions and private communications. As the use of email spreads, the use of security approaches such as digital certificates, encryption and email security become important in ensuring the privacy of communication. At the same time, companies are under increasing scrutiny to adhere to government regulations and other compliance requirements to protect the privacy of customers, employees and their personal data.

The traditional infrastructure used to protect data and communication based on certificates, commonly called Public Key Infrastructure (PKI), was not designed to deal with inter-enterprise communication at all, let alone the massive volume of communication from an ever-growing variety of connected devices that has become commonplace in the Internet-enabled era. Implementations in Fortune 1000 organizations have shown that not only do PKI systems have a high barrier to use, leading users to eschew them, but also they are difficult for administrators to manage. Plus, the high cost is often too difficult for a CIO to justify deployment of a PKI solution.

Other approaches to email security have had little impact, either due to the complexity of using them or because of their scalability characteristics – having to manage keys for millions of messages a day or maintain parallel messaging infrastructures. What is needed is a platform that provides high security, management of security policies and usability that is orders of magnitude better than what is available from secure messaging vendors today.

Voltage Security, Inc. was founded with the vision to secure all trusted business communication. Based on a breakthrough encryption technology called Identity-Based Encryption (IBE), Voltage Security enables today's enterprises to conduct secure, scalable communication and fully experience the benefits and ROI of moving business processes to the Internet.

This paper will:

- Describe the existing encryption solutions available on the market today and detail their inherent shortcomings;
- Define the critical requirements for a solution that enables ubiquitous secure business communication;
- Describe a groundbreaking new technology, called Identity-Based Encryption (or IBE), that addresses these critical requirements and enables universal transparent secure messaging; and
- Illustrate how IBE technology can be easily integrated into the most popular and fastest-growing applications — and describe the advantages it provides for each IBE-enabled application over existing solutions.

Shortcomings of Existing Network Security Solutions

Many attempts have been made to solve the problem of establishing trusted business communication—from the earliest use of symmetric cryptography in the 1970s, through the current PKI (public key infrastructure) standard.

Symmetric Cryptography

Beginning in the 1970s, military networks and academic systems—precursors of the modern Internet—were the early adopters of modern cryptography, using security systems built on top of the first publicly available cryptosystems based on "symmetric cryptography." These symmetric cryptosystems, the best known of which is the Data Encryption Standard, or DES, were widely used through the 1970s and is still used today as a component of modern cryptographic protocols.

In a symmetric cryptosystem, both the sender and the receiver use the same key. For example, if Alice wants to send a message to Bob, they meet in person and agree on a password. They can then use that password as a key to encrypt a message.

Implementations of symmetric cryptography, such as Kerberos, issue each user a password known both to the user as well as to a central server. So, if Alice wants to send a message to Bob, the following steps occur (see Figure 2 below):

Step 1	Alice sends a request—encrypted with her password—to the server, containing Bob's name.
Step 2	The server then generates a random key, and encrypts it with Bob's password. It also encrypts the key with Alice's password, and sends both password-protected keys to Alice.
Step 3	Alice then encrypts the document with the random key, and sends the message and the key encrypted to Bob by the server. Bob can then decrypt the document.

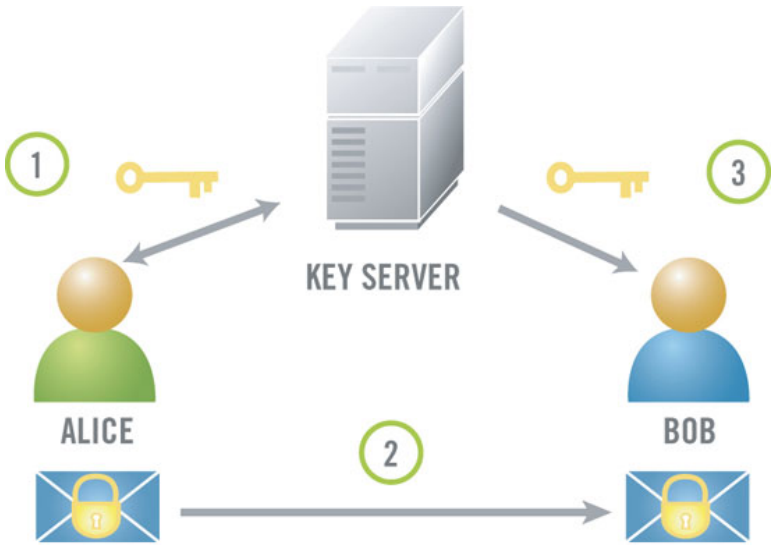

Figure 2: Symmetric cryptography

Symmetric cryptosystems exhibited three critical shortcomings or flaws as the Internet and the need to secure communication and transactions grew.

Scalability issues quickly arise

Symmetric cryptosystems are inflexible and difficult to manage outside of small groups of users because a central server must be involved in the transmission of every communication in the system. When any pair of users wishes to send messages, they must communicate with the central server. As the number of messages and users in the system increases, the server gets busier and busier, leading to serious scalability issues.

Strict online requirement removes offline capability

The need to communicate with the central server to establish a connection also requires that both the sender and the central server are available online and able to communicate at all times. If the server is down or the user is offline, secure communication is impossible.

Interconnection is difficult

Interconnecting partner systems using symmetric cryptography can be difficult, if not impossible. Key translation servers or active trust brokering servers are required to interconnect one enterprise's trusted servers with another. This can be prohibitively expensive and may also require establishing a trusted third-party intermediary.

Asymmetric CRYPTOGRAPHY

While symmetric cryptography was adequate for small, contained networks with a small number of users, it could not handle the volume of traffic brought on by the Internet boom in the 1990s. Handling this volume motivated the use of a newer form of cryptography that did not require online servers to broker keys for all users, called asymmetric, or public-key, systems. Commonly called PKI, asymmetric systems were introduced to the market in the 1980s. In the PKI model, different keys—a public key and a private key—are used to encrypt and decrypt messages.

The encryption policy—specifying which users can connect to which network resources, or which user can read which email from which sender—is created by defining policy elements such as user names, network addresses, and trust levels. These policy elements are then coupled with the user's identity to their public keys—the product of two randomly generated prime numbers—via a "certificate."

Certificates are electronic documents that contain the name of the owner of a key, some information about the validity of the certificate (for example, a time period over which the certificate is valid), and the owner's public key. The owner's certificate is then electronically signed by a trusted authority called a Certificate Authority (CA).

In such a system, if Alice wants to send an encrypted message to Bob, the following steps are necessary (see Figure 3 below):

Step 1: Alice contacts Bob—or a directory server—to obtain Bob's certificate, containing Bob's public key.

Step 2: After locating Bob's certificate, Alice then downloads his certificate, validates the certificate against published revocation lists, validates the certificate's signing chain, extracts the public key, and uses Bob's public key to encrypt the message to Bob.

Step 3: Bob then decrypts the message using his private key.

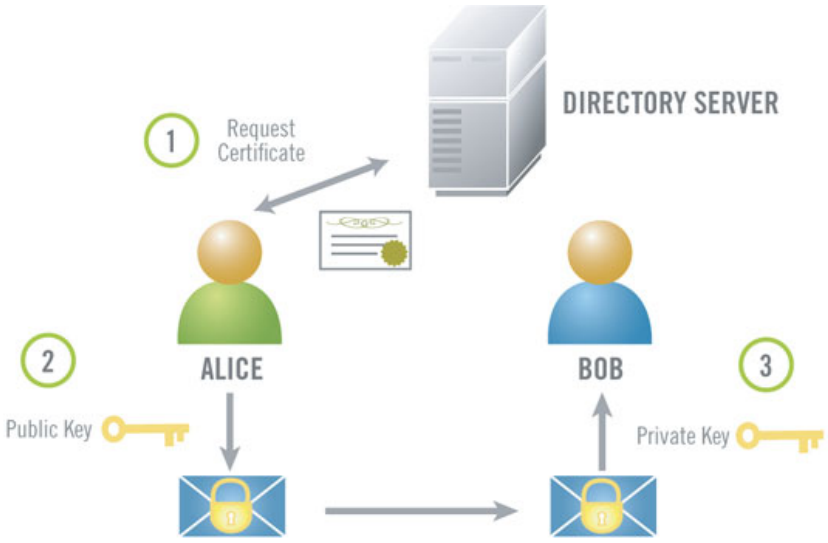

Figure 3: Asymmetric cryptography, or PKI

In theory, PKI should handle authentication of users and services flexibly and without limit with respect to the complexity of the policy. In reality, however, PKI has collapsed under the administrative weight of certificates, revocation lists, and cross-certification problems.

Five critical shortcomings and flaws exist in PKI that have prevented the technology from enabling ubiquitous secure messaging:

Certificates are not easily located

Before communication can take place, the client needs to locate a certificate for the message recipient. The lack of a standard directory that publishes certificates can make finding these certificates difficult—or impossible—even if both communicating parties are online simultaneously.

Strict online requirement removes offline capability

Closely related to the above point is the requirement that users be online to conduct secure business communication. In the case of email, or in situations where both the client and server are offline, the user can only access and use certificates that have been cached on his local machine, limiting communication to a small number of people for whom the user has certificates.

Validating policy is time-consuming and difficult to administer

Once a certificate is located, a client must validate the certificate, ensure that the certificate issuer is trusted, and match the certificate policy with the client's own policy requirements. This can be enormously time-consuming and difficult to administer.

For example, validating a certificate requires determining whether the certifying authority has revoked the certificate. Certificate authorities do this by either publishing a Certificate Revocation List (CRL), or by having the client contact an online revocation server. If the client is not online, this approach is rendered useless, because online revocation servers require that the client be online.

As the increased security requirements of web services translate to an increasing number of properties that can, and will be, put into certificates, this problem becomes even more difficult. With more properties added to certificates, the more complex policies become and the larger already gigantic Certificate Revocation Lists grow, leading to increased certificate volume and management overhead. For example, the CRL alone for a system with more than one million users would be larger than tens of megabytes per day!

Certificates leak data

Since they must be accessible to clients, certificates publish a vast amount of information about the certified entities to the world, making them inherently insecure. Each application or person that can access and read the certificate database of a large enterprise can construct a record of employee names, server names, and security status of those entities. Making this data accessible enables stronger security through better, more detailed policy decisions, but it also paradoxically devastates system security by publishing a detailed map of the enterprise's users, data, and services.

Users must pre-enroll

Before a user can send, conduct, or receive a secure message or transaction, pre-enrollment is required to make himself known to the PKI system. This means that a user cannot send a secure email or conduct a secure transaction with a web server that is not already known to the CA, limiting the community with which a user can conduct secure communication. This pre-enrollment requirement has been a primary factor limiting the ubiquity of PKI.

Overcoming the Flaws of Existing Technologies

The fundamental problem of both of the existing solutions described above is that they do not address the authentication of users and services based on user identity and the flexibility needed in conducting secure business communication. Applications should be able to identify the services to which they are connected and apply policies about those specific services, without user intervention or complex configuration requirements. For example, an email user should be able to dictate that only authorized recipients can view a message or an attached document. An Instant Messaging user should be able to indicate that only another authorized employee can view an IM. Services, too, must be able to reliably identify authorized users and the operations that those users are authorized to perform. For example, servers must be able to require that only supply chain collaboration partners can view inventory data.

It's clear that a new solution is required, one which overcomes the flaws of existing technologies and which addresses the critical requirements of secure communication beyond corporate boundaries. This new solution must:

- **Secure anytime, anywhere communication;**
- **Allow for self-provisioning to easily conduct secure communication;**
- **Enable secure messaging that is transparent to users;**
- **Be easily managed by administrators; and**
- **Be low cost.**

A New Approach to Secure Communication: Identity-Based Encryption

Based on a new form of public-key cryptography called Identity-Based Encryption, (IBE) that utilizes commonly used identities as the user's public key, Voltage Security delivers the breakthrough technology that radically changes the way people think about secure communication.

By eliminating the need for individual per-user certificates, Voltage Security's solutions provide a highly scalable, universally inter-connectible method for secure communication that overcomes the flaws of existing approaches. Specifically, Voltage Security solutions:

Secure anytime, anywhere communication

Voltage Security solutions allow users to conduct secure business communication anytime, anywhere – even on the road. For example, a secure email can be encrypted or decrypted on a laptop even when not online. With Voltage, users can conduct business securely—from anywhere in the world—because they can roam transparently, enabling complete flexibility in how, and when, users conduct their work.

Allow for self-provisioning to conduct secure communication

The elimination of per-user certificates and the related requirement to connect to third-party servers to verify these certificates before initiating secure connections allow for user self-provisioning. No pre-enrollment of users is needed to conduct secure ad hoc communication. Secure ad hoc communication enables users to securely exchange messages, via email, instant messaging or other means, without having knowledge of whether the other party is already enrolled or registered. This type of communication matches the way people normally interact over the telephone or with a fax machine. This makes Voltage Security solutions infinitely scalable for an enterprise.

Enable secure messaging that is transparent to users

By using a commonly used identifier as the encryption key, Voltage Security provides a simple, yet highly secure, method to encrypt business communication, thereby enhancing the overall enterprise security. No additional steps or clicks are required on the user's part to ensure secure communication because the user is recognized by his identity—email address or user login.

Are easily managed by administrators

With Voltage Security solutions, administrators can centrally manage the security of their business communication. Policies used to secure business communication are enforced at the central key server and can be changed simply and automatically. The sender merely transmits his security requirements and the key server enforces them. Administrators are also given the flexibility of working with any leading authentication methods with Voltage solutions. This flexibility allows Voltage solutions to secure virtually any system or network object centrally through one solution.

Are low cost

Voltage Security provides a lightweight solution that integrates easily and quickly with existing enterprise application infrastructure. Because heavy infrastructure and third-party CAs are not required, implementation of secure messaging within the enterprise's infrastructure is simplified. In addition, instead of deploying a point solution for each type of business communication to secure, administrators can deploy a single platform—the Voltage Security platform—to secure all types of business communication, ensuring a low total cost of ownership (TCO) for the enterprise.

The Voltage Security Architecture

There are four components of the Voltage Security architecture:

1. THE IBE ALGORITHM

Adi Shamir, one of the inventors of the well-known RSA public key system, originally proposed the idea behind Identity-Based Encryption in 1984. However, with no workable method to solve the problem known at the time, IBE remained one of the major unsolved problems in cryptography. It was until 2001, when Dr. Dan Boneh and Dr. Matt Franklin, professors of computer science at Stanford University and University of California, Davis, respectively, invented a practical scheme based on elliptic curves and a mathematical construct called the Weil Pairing.

IBE is the enabling technology within the Voltage Security architecture, similar to the RSA standard that is the enabling technology for PKI.

The mathematical construct that makes IBE work is a special type of function called a "bi-linear map." A bi-linear map is a pairing that has the property:

$$\mathbf{Pair(\ a \bullet X,\ \ b \bullet Y\ ) = Pair(\ b \bullet X,\ \ a \bullet Y\ )}$$

For IBE, the operator "•" is multiplication of integers with points on elliptic curves. While multiplication itself (e.g., calculating a•X) is easy, the inverse operation (finding a from X and a•X) is practically impossible. The bi-linear map that is used is a Weil Pairing or Tate Pairing.1

The idea of the bi-linear map is then applied to the IBE algorithm (Figure 4). A key server generates a secret s and a parameter P using random number generation. Next, the public parameters, P and s•P (the product of s and P), are distributed to all users. Then, a private key is issued to each user by the key server. This private key is the product of the user's identity and the secret s. For user Bob, this is s•IDBob.

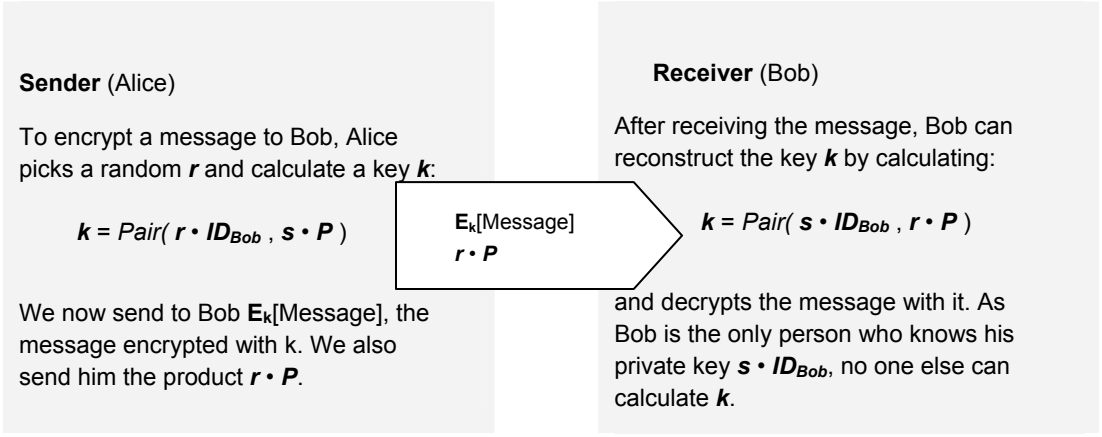

Figure 4: Sending and receiving a secure message with IBE

[1] For more technical details on how IBE works, see Identity based encryption from the Weil pairing by D. Boneh and M. Franklin. In proceedings of Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 213-229, 2001. This paper is available online at http://crypto.stanford.edu/~dabo/papers/ibe.pdf

2. THE KEY

Because IBE allows the user to choose his public key and receive his private key from a trusted, central source, Voltage users' public keys are their identities (e.g., email addresses or network logins). This seemingly simple but technically difficult breakthrough makes certificates superfluous and ties security policy directly to the encryption or authentication method.

The following examples illustrate the difference between keys in a public-key system and those in the Voltage Security solution. Figure 5 shows a public key for the RSA algorithm. Because the key is a number several thousand bits long, it does not have a concept of identity. As a result, a certificate is needed to tie the public key to an identity.

The sender must have all this information and connect it via a certificate to the recipient to send a secure message:

Public exponent:
0x10001

Modulus:

13506641086599522734960321627980596993892147560566702752448514385152651060485954383394028715057190945179820728216447153137368041970396419174304649658927425623934102086438320211037295872576235850964311056407350150918751062359462920556368552947521351595287941637732853390610975054433421981115005697723689092756 3

Figure 5: An Example of an RSA Public Key

In contrast, Figure 6 illustrates a public key using IBE:

Name = bob@b.com

Figure 6: An IBE Public Key

The ability to choose simple, understandable keys underlies the power of the Voltage Security architecture to encode policy directly into encryption and authentication methods.

3. KEY MANAGEMENT **(KEY GENERATION AND KEY UPDATING)**

Key management encompasses two primary functions: key generation and key updating. In the Voltage Security platform, these responsibilities are handled by the Voltage IBE Server™ – a centrally managed server that administers an enterprise's secure applications.

Key generation is the function of generating the public and private keys for use in secure communication. Key updating insures that keys are changed regularly, thereby protecting the system and the user if a key is lost or stolen.

Key Generation

For key generation, Voltage Security implements a Key Server as part of the IBE Server. The Key Server's primary function is to generate private keys in an IBE-based security system and to enable users, services, and applications to use IBE encryption.

Key Update

Key update is the component of key management that ensures the validity and authenticity of the key. To prevent against key compromise, Voltage uses a combination of an identity and the date, such as:

"name=Bob validity=11/1/02-12/01/02"

Since the public key is different for each time period, so is the corresponding private key. This automatically limits compromise to the duration of the original key. Furthermore, instead of revoking a key for a fired employee or compromised machine, the Voltage key server simply stops issuing private keys to that identity.

In contrast, key compromise in PKI-based systems is handled by placing the corresponding certificate on a Certificate Revocation List (CRL). In practice, most clients do not check CRLs and therefore compromised keys remain undetected.

4. POLICY ENFORCEMENT

Enterprises that use Voltage Security solutions in conjunction with the Voltage IBE Server can easily describe and enforce even the most complex security policies for any communication, including person-to-person, person-to-application, and application-to-application.

The Voltage IBE Server will be able to enforce policy in a method similar to the one used for key compromise. Rather than a simple identity or an identity-date pair as the public key, an identity-policy pair is used. So, instead of encoding a name, the policy is encoded instead, as shown in Figure 7:

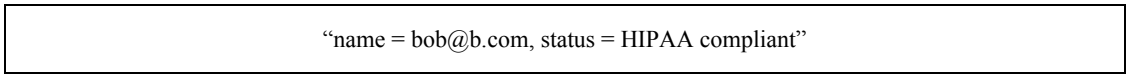

Figure 7: An IBE Public Key with Policy

For example, Alice wants to send a message to Bob, but only if Bob complies with HIPAA2 privacy requirements. Alice can then use the public key "Bob – HIPAA compliant." When Bob contacts the key server to get the corresponding private key, the key server will only grant him the private key if, in fact, Bob can properly authenticate who he is and is HIPAA compliant.

---

[2] The Health Insurance Portability and Accountability Act of 1996, which provides guidelines for safeguarding the use and disclosure of individually identifiable health information.

How the Voltage Security Solution Works

Voltage Security solutions allow enterprises to secure a wide range of mission critical business communication - one example of which is to secure email communication with the Voltage SecureMail™ solution..

Alice at Company A would like to send her customer Bob at Company B a sensitive email. For compliance reasons, the email must be secure. Alice uses the Voltage SecureMail solution to send the secure email to Bob.

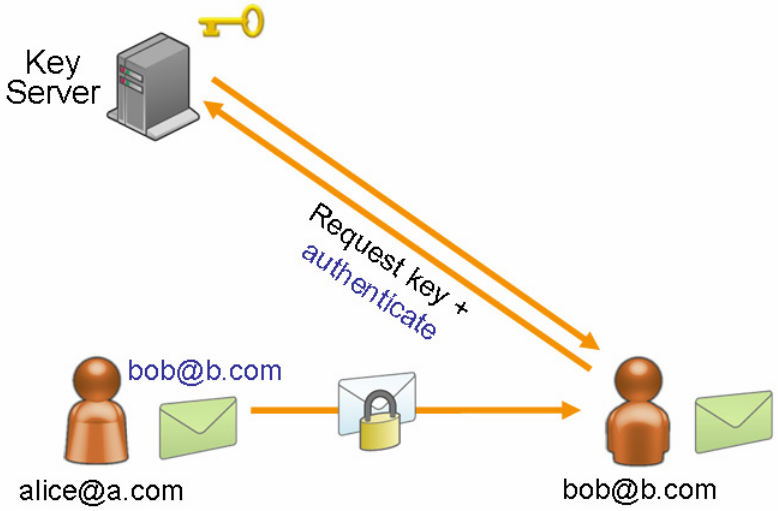

Figure 8: Sending a Secure Email using Voltage SecureMail is Simple

Alice Sends a Secure Message to Bob

After Alice composes the message, she simply hits the Send Secure button, which automatically secures the message, along with any attachments, using Bob's email address "bob@b.com".

Voltage SecureMail does not require pre-enrollment of users to receive secure email; even if Bob has never previously communicated with Alice or has never used Voltage SecureMail, he is still able to receive secure email from Alice.

Bob Receives the Secure Message

The first time Bob receives the secure message on his laptop, Bob clicks on a link in the message header and downloads the Voltage SecureMail client. He then proceeds to enroll and authenticate to Company A's IBE Server. The method used to authenticate Bob is completely flexible to the requirements of the enterprise.

Bob Decrypts and Views the Message

Upon completion of proper authentication, the IBE Server will present Bob with his private key to read the secure email. Alice and Bob can now communicate securely with Voltage SecureMail.

With his private key downloaded to his laptop, Bob can decrypt and view his received secure email even when he is offline on an airplane. Bob can even read his secure email at a business center using Voltage SecureMail's transparent roaming capabilities.

Using Voltage Security Solutions to Enable Secure Internet Messaging

Voltage Security solutions can be used to secure all types of Internet messages, including email and Instant Messaging (IM). Voltage's architecture allows users to encrypt Internet messages invisibly and makes compliance with privacy requirements easier, enabling enterprises to adhere to emerging requirements for strict audit controls over all incoming and outgoing messages.

Secure Email

Sending a secure email today, using a traditional email application combined with PKI, is complicated and presents many roadblocks, which is why the vast majority of email is not encrypted. Often, the sender only knows the recipient's email address, and must determine the recipient's certificate either by consulting a directory or by contacting the recipient directly. While directories do exist, they are not widespread, so consulting them is generally futile. If the sender must contact the recipient, this can create delays. Moreover, the request for the certificate is unprotected.

Another solution offered in the market today is web-based secure email. In this example, the message is stored on a web server and the recipient is notified of the message with a secure URL link. While its ease of use may be somewhat attractive, most email users are unwilling to switch over to non-standard email clients. The inability of easily integrating ones email into standard clients breaks workflow and creates usability issues for users. Because the email is now stored on a web server, the user is required to be online to view the email. Corporate email users have demonstrated the need for managing their emails locally on their machines. A solution that places strict online requirements will not suffice for enterprise email users.

In contrast, Voltage SecureMail enables users to send secure email directly to any recipient—instantly. If this is the first encrypted message received by the recipient, he simply contacts the enterprise key server to acquire the private key. Otherwise, he merely decrypts the message without any additional steps or effort.

Because Voltage Security solutions overcome the roadblocks to secure messaging and enables transparent encryption, enterprises gain better, finer-grained control over external communication. With fewer impediments to use, encryption becomes second nature, and the more users that implement secure email, the better enterprises can audit and comply with government regulations.

Using Voltage Security Solutions to Enable Secure Files

Whether it's a Microsoft Excel spreadsheet attachment sent via email, customer financial information stored on a hard disk, confidential patient information stored on a shared file server, or the latest product pricing strategy stored in the company intranet or pricing portal, all of an enterprise's files must be stored securely to ensure the protection of sensitive company secrets—and customers' privacy. The security must go beyond the creator of the file simply encrypting the document for his or her own use to encrypting and signing the file for designated users or groups of users.

The consequences of improper management of such sensitive material are serious, from both a corporate security as well as an economic standpoint. Recently passed federal regulations such as the Gramm-Leach-Bliley (GLB) Act or the Health Insurance Portability and Accountability Act (HIPAA) dictate the protection of customer data, and individual states have also enacted severe penalties for companies that fail to protect customer privacy.

The flexibility of Voltage Security's SecureFile™ allows users to encrypt and sign files for use by other authorized individuals. Files can be encrypted to multiple users based on their email addresses and/or policies set by the creator of the encrypted file. Secure files that are signed provide assurance of the authenticity of the originator of the encrypted file. Once secure, these files can be transported easily by any medium and be assured of its confidentiality.

CONCLUSION

Voltage delivers a revolutionary new way of securing communication that overcomes the hurdles of existing solutions. As a result, Voltage delivers communication security solutions that help enterprises to experience the full benefits and ROI of moving business processes to the Internet.

By using a commonly used identity—such as the user's email address or network ID—as the user's public key, Voltage is the only provider that addresses the critical requirements of ubiquitous secure communication beyond corporate boundaries.

Voltage Security solutions:

- Secure anytime, anywhere communication;
- Allow for self-provisioning to conduct secure communication;
- Enable secure messaging that is transparent to users;
- Are easily managed by administrators; and
- Are low cost.

Voltage's transparent encryption breaks down the barriers to secure messaging by making it second nature—thereby enhancing enterprise security. Voltage Security is the first to use identity to bring confidence to your business communication.

ABOUT VOLTAGE SECURITY

Voltage Security delivers the leading enterprise privacy management platform for protecting data privacy.

Based on an award-winning breakthrough in security and usability called Identity-Based Encryption (IBE), Voltage provides solutions for secure communication and data at rest to leading financial services, healthcare, government and pharmaceutical companies.

For companies concerned with complying with HIPAA, GLBA, PIPEDA, Basel II, SEC 17, SOX and SB1386, Voltage offers automated policy-based encryption that reduces the risks associated with privacy and compliance.

Voltage's Enterprise Privacy Management Platform provides a common framework for applying security and enforcing policies for data flowing inside and outside the enterprise, including email, files, documents, and instant messaging.

Voltage solutions secure data privacy by making anytime, anywhere security easy to use and painless to deploy.

For more information, please visit www.voltage.com, email info@voltage.com
or call +1 650 543 1280