
SecureMail: Encryption Made Easy

The Advantages of
Identity Based
Encryption

Safeserve.com Ltd.

safeserve

Contents

Contents	3
Introduction	5
What's Driving Interest in Secure Messaging?	5
What is Secure Messaging?	6
Symmetric Cryptography: The Origins of Secure Messaging	6
Drawbacks of Symmetric Cryptography	7
Bottom Line	7
Asymmetric Cryptosystems or PKI: An Improvement	7
Drawbacks of PKI	8
Bottom Line	9
Secure Webmail Systems	9
A Simple Solution, But.....	9
Bottom Line	9
IBE (Identity-Based Encryption).....	9
The Simplicity of IBE	10
IBE Keys	10
Key Management in IBE.....	11
Summary Comparison of Secure Messaging Solutions.....	11
Summary.....	12
About Safeserve.com Ltd.....	12
Safeserve.com Ltd	13

f

Introduction

The growing list of regulations for protecting data in virtually every size organisation and industry means enterprises are being pressed hard to find effective, affordable, easy-to-implement and use email encryption technologies. Effective secure messaging technologies keep sensitive information private, prevent anyone from tampering with the contents of messages and authenticate the identity of both the message's sender and recipient. And all organisations, regardless of their size, require encryption to be both user- and IT-friendly.

Safeserve Secure Messaging™, powered by Voltage IBE™ technology, provides policy-driven encryption that's easy to administer and easy to use. There are no keys or messages that have to be stored for extended periods. And it doesn't require end-users to jump through hoops to ensure that the right messages are encrypted at the right time. This whitepaper describes the history of secure messaging technology and the advantages of identity-based encryption over traditional approaches to public key cryptography.

What's Driving Interest in Secure Messaging?

For World War II's "greatest generation" loose talk, which could cost lives, was the greatest threat to security. Two generations later the threat to security is far more complex and multi-dimensional, but the stakes remain high. When valuable intellectual property is compromised, medical records revealed, or privacy rights threatened, there's hell (and often heavy fines) to pay.

Because of a perception that companies that haven't taken strong enough measures to protect against these dangers, governments at home and abroad, have stepped in. And in place of warning posters, there are statutes; many with sharp teeth.

A now familiar list of regulations either requires—or strongly suggests—that organisations adopt email encryption as an important component of their overall security architectures:

- ❖ In the UK the Data Protection Act: CEOs and CFOs of public companies personally accountable for documenting and controlling business processes and systems with intentional offenders facing up to twenty years behind bars.
- ❖ Corporations doing business globally are forced to adhere to other countries' laws as well. There are the US's Sarbanes-Oxley Act, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the European Union's Privacy Directive. Each specifies different guidelines or rules for the handling of private information. And, in some cases, penalties for non-compliance may apply.
- ❖ HIPAA (Health Insurance Portability and Accountability Act) regulations are aimed at protecting patient privacy. Penalties range for up to ten years in prison with fines to \$250,000 for knowingly misusing individually identifiable health information.
- ❖ Financial institutions of all types—from banks and security firms to tax-return preparers, credit counsellors, real estate settlement services and insurance companies—fall under the aegis of the GLBA (Gramm-Leach-Bliley Act), which includes a host of provisions for protecting consumers' personal financial information.
- ❖ It goes almost without saying that companies doing business with must comply with a whole raft of regulations including FISMA (Federal Information Security Management Act) when implementing email security.

But regulatory compliance concerns are only part of the picture—internal governance, privacy and intellectual property protection concerns are also driving organisations to take a closer look at technologies that can protect data both at rest and in transit. Because email is the most common conduit for all types of business information, email encryption (aka secure messaging) systems are becoming more popular with organisations of all sizes.

Only a company attempting a high dive into red ink needs a government edict to explain the absolute necessity for secure messaging that safeguards information. Trouble can suddenly appear anywhere there's a leak—being blind-sided by a competitor who acquired intellectual property, financial information getting out to the market prematurely, and social security numbers compromised. Unfortunately, the list of potential risks is long and uninviting.

What is Secure Messaging?

Secure messaging has three primary benefits: keeping sensitive information private, preventing anyone from tampering with the contents of messages and authenticating the identity of both the message's sender and recipient. By using encryption algorithms, the contents of sensitive messages are kept private from anyone except the designated message recipient(s).

Encryption works by means of digital "keys" which, similar to keys in the physical world, lock the contents of a message so that they cannot be viewed until "unlocked" with a corresponding decryption key. One of the primary differences between the various cryptographic systems is the way they handle the generation, distribution and management of these keys.

Beyond the technical details of each encryption system, effective enterprise secure messaging systems are primarily about enforcing messaging policy. The goal is to have a system that offers administrators the greatest control and ability to quickly set and change parameters for who will (and won't) be authorized to access specified information at specified times from specified individuals. At the same time, this has to be done without unduly inhibiting the free flow of other business communications, whether sent in encrypted form or "in the clear."

To understand the advantages of and differences between secure messaging systems in use today, it's helpful to review the history of encryption technology and the basics of how these systems work. In the following sections, four different approaches to email encryption are described.

Symmetric Cryptography: The Origins of Secure Messaging

In the 1970s, military and academic networks—the precursors of the Internet—were the early adopters of modern cryptography, using security systems based on first-generation "symmetric cryptography." Even today, symmetric cryptosystems (Data Encryption Standard or DES is the best known) are used as a component of modern cryptographic protocols.

In a symmetric cryptosystem, the sender and receiver of a secure message agree on a password and then use that password as a key to both encrypt and decrypt messages. Some symmetric cryptosystems issue the sender and recipient a password who also resides on a central server. When a sender wants to transmit a message to a recipient, the following steps are taken:

- ❖ Step 1: The message Sender sends a request encrypted with his or her password to the server that maintains the Recipient's name and passwords.
- ❖ Step 2: The server generates a random key and encrypts it using the Recipient's password. It also encrypts the key using the Sender's password and sends both password-protected keys to the Sender.
- ❖ Step 3: The Sender encrypts the message they want to send using the random key issued by the server.
- ❖ Step 4: The Sender transmits the encrypted message to the Receiver, along with the server-issued Receiver key.
- ❖ Step 5: The Receiver gets the encrypted message which can then be decrypted using the Receiver's password-protected key.

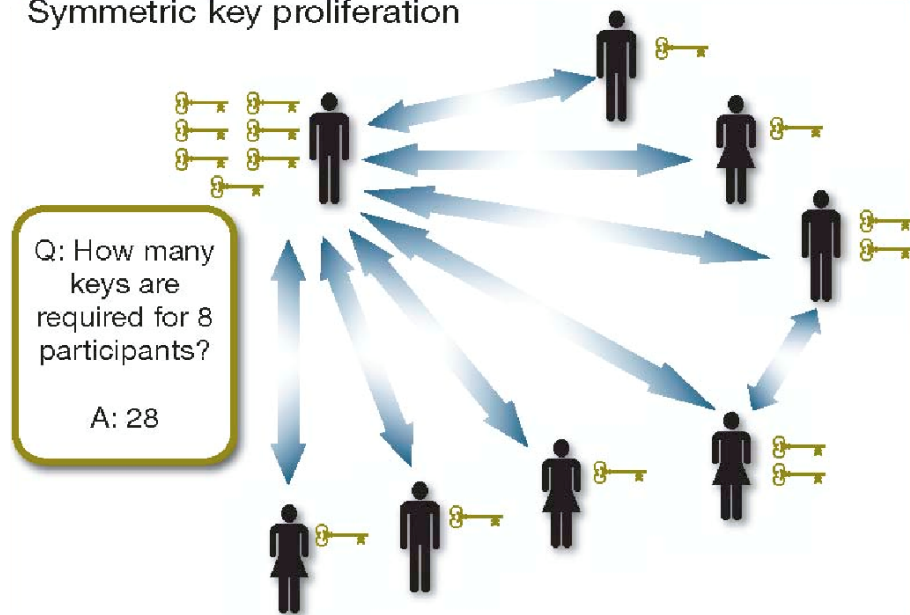
Drawbacks of Symmetric Cryptography

Because every secure message transmission involves the central server, server traffic can be a major headache. To enable secure communications, both the message sender and central server have to be online. Finally, because key-translation servers or active-trust-brokering servers are needed for interconnecting one enterprise's trusted servers with another, it's often close to—or downright impossible—to interconnect systems.

Another limitation of symmetric cryptography systems is the huge number of keys required. Think of it this way: Each pair of users requires a key to enable secure communications between those two individuals. We'll spare you the maths, but what this means is that for a network of "N" number of users, the number of keys required to enable communication between all individuals is equal to $N*(N-1)/2$. For a small workgroup of eight people, 28 unique keys would be required. For a medium-sized enterprise of just 1000 people, nearly half a million keys are needed.

Storing, archiving and backing up all of these keys—so that messages can be decrypted at a later date or to facilitate disaster recovery—becomes a massive burden as the number of users grows.

Symmetric key proliferation



Key management in symmetric cryptography: Just eight users require 28 keys to enable secure communication between all 8 parties ($8 \times (8-1)/2 = 28$). For a network of 1000 users, you would need almost half a million (499,500) keys!

Bottom Line

Symmetric cryptosystems are adequate for small, contained networks with limited numbers of users. So symmetric cryptography was a good solution for the military, for example, where "need to know" was tightly controlled. However, with the Internet's coming of age in the 90s, the volume of traffic begged for a better solution.

Asymmetric Cryptosystems or PKI: An Improvement

Asymmetric or public-key systems cryptography systems, better known as PKI (Public Key Infrastructure), were introduced in the 1980s and use two keys—a public key and a private key—to encrypt and decrypt messages.

Based on user names, network addresses and trust level, PKI encryption policies specify which users are permitted to connect to which network resources or who is allowed to read what email and from which sender. 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 (1) the name of the owner of a key, (2) some information about the validity of the certificate (for example, a time period over which the certificate is valid) and (3) the owner's public key. The owner's certificate is then electronically signed by a trusted authority called a “Certificate Authority” (CA).

In PKI systems, the two keys (public and private) are always used together to encrypt and decrypt messages. A user can share his or her public key with anyone so that they can encrypt a message destined for that user. When the user receives an encrypted message, they can then decrypt the message using their private key.

Clearly this is an improvement over symmetric cryptography systems. But what if someone that you don't already know wants to send you an encrypted message? Somehow that sender needs to get a copy of your public key. This is where certificates, certificate servers and revocation lists come in. The sender can contact a certificate server—essentially a trusted source of public keys—to retrieve your public key.

When a sender wants to transmit an encrypted message to a receiver using a PKI system, the following steps are taken:

- ❖ Step 1: The Sender contacts the Recipient or a directory server to get the Recipient's certificate—which contains the Recipient's public key.
- ❖ Step 2: The Sender downloads the Recipient's certificate, validates the Recipient's certificate against published revocation lists and validates the certificate's signing chain.
- ❖ Step 3: Once the Recipient's certificate is validated, the Sender extracts the Recipient's public key and uses it to encrypt the message.
- ❖ Step 4: Sender transmits the encrypted message to the Recipient.
- ❖ Step 5: Recipient receives the encrypted message which can then be decrypted using his or her own private key. .

Drawbacks of PKI

The drawbacks of PKI systems relate to the complexity involved in managing certificates, revocation lists and various cross-certification problems. This complexity leads to a lot of administrative overhead and expensive infrastructure, which have prevented PKI technology from enabling truly ubiquitous secure messaging. Consider the following problems

- ❖ Before sending a message, a sender must have a recipient's certificate: If a company doesn't maintain a standard directory of published certificates, it is difficult for the sender (client) to find a recipient's certificate on the server. Also, where does a company find the resources to dedicate to administering and always updating this constantly changing directory?
- ❖ Senders and recipients have to be online to conduct secure communication: If the client or server is offline, the user can only access certificates cached in his personal computer and only communicate securely with those people.
- ❖ Validation can be difficult: The client validates the certificate by checking the CA's (Certificate Authority) CRL (Certificate Revocation List) or contacting an online revocation server. Obviously, if the client is not online, the client can't check an online server.

Managing Certificates: An End in Itself?

Certificate management poses many issues for administrators, including:

- How do I renew certificates?
- How do I know when a certificate has been revoked?
- How do I find a recipient's certificate?
- How do I manage certificate distribution?
- What do I do if private keys are lost?
- Where are the aspirin?

Certificate Revocation Lists (CRLs) are an especially vexing problem. Using a state-of-the-art PKI system, The CRL list itself for a million-user system can grow by tens of megabytes per day.

- ❖ The Web has multiplied the amount of information put into certificates: More information means more complex policies. More policies mean larger Certificate Revocation Lists. Larger CRLs mean more management and more overhead. .
- ❖ Users have to be pre-enrolled or they can't send secure email to a Web server: Put another way, the Certifying Authority has to recognize the Web server before a user can conduct secure transactions with it. Obviously, this restricts who can use a PKI system.
- ❖ In a worst-case scenario, using PKI, disaster recovery can be a...DISASTER: Public keys, private keys, certificates—the list of bad things that can happen is daunting.

Bottom Line

Referring to its drawbacks (complicated, constantly in flux, difficult and expensive to administer), one wag succinctly summed up PKI as a “four-letter word”. However, PKI is not the last word in solving the secure messaging issue.

Secure Webmail Systems

To “simplify” their lives, some IT departments have turned to secure webmail, which, compared to PKI, is simple to use. An encrypted message is stored on a web server and the recipient is notified via email. Using HTTPS in place of HTTP in the URL, the user is directed to a secure port number. The session is then managed by a security protocol such as SSL.

A Simple Solution, But...

Many, if not most, email users aren't overjoyed at the prospect of switching to non-standard email programs to get messages. Plus, using Webmail for secure communications means there is an additional, separate email system to administer with messages to be stored and archived for weeks... months... years.

Bottom Line

Webmail is easier to use than PKI. However, the challenges of administering a second, parallel email system and parallel infrastructure, plus archiving secure messages can get expensive.

IBE (Identity-Based Encryption)

IBE puts a new spin on an old adage. IBE is like “throwing out the bathwater and keeping the baby.” It's having the best of PKI without the bad. IBE uses the same algorithms as PKI and provides the highest possible level of secure communication. What's missing is the cumbersome, complex and costly certification and certificate management process.

With IBE, there are no individual, per-user certificates. An email address or log-in is used as the encryption key identifying the user. Administrators manage and enforce policies from a central-key server and can change policies on the fly. IBE integrates easily with existing enterprise application infrastructures—one of the key reasons that Safeserve chose to incorporate IBE technology into Safeserve Secure Messaging.

Using IBE, email can be encrypted or decrypted online—or off—anytime, anywhere. IBE enables secure, ad hoc communication that mirrors how people communicate in the real world. It lets users exchange messages without worrying about whether or not the other user is enrolled or registered.

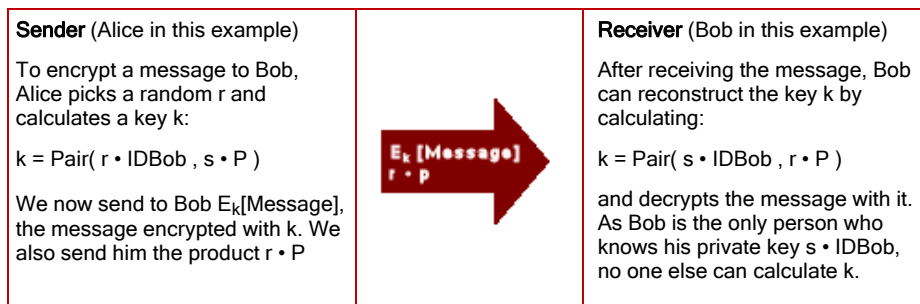
IBE enables secure messaging that's transparent to end users. Using IBE technology, Safeserve Secure Messaging can automatically encrypt messages that contain private or confidential information, without requiring any manual intervention by message senders.

The Simplicity of IBE

Safeserve's use of IBE ensures the security of encrypted email communications while minimising the burden on end users. Consider the case of a doctor who needs to send a message containing confidential medical information to a patient. The transaction works as follows:

- ❖ Step 1: Doctor A writes and sends an email to Patient B. He may use the SecureMail plugin with Outlook or trigger Safeserve's mail server (which analyzes the message and detects keywords) to encrypt the message.
- ❖ Step 2: Patient B receives the encrypted email and clicks the attachment to authenticate himself to the Safeserve Secure Messaging module via SSL.
- ❖ Step 3: Safeserve Secure Messaging decrypts the message and hosts it in server memory for Patient B to review. After Patient B accesses the message, it is removed from memory.
- ❖ Step 4: Using the Safeserve Secure Messaging module's webmail functionality, Patient B can securely reply to Doctor A.

Sending and receiving a secure message with IBE



IBE Keys

Because IBE allows a user to choose his or her own public key and to receive his or her private key from a trusted, central source, public keys (e.g., email addresses or network logins) become identities. While this seems simple, it is anything but. It took a major breakthrough to render certificates superfluous by tying security policy directly to encryption or authentication.

Here's an example of a public key for the RSA algorithm:

Public exponent:

0x10001

Modulus:

13506641086599522734960321627980596993892147560566702752448514
 38515265106048595438339402871505719094517982072821644715313736
 80419703964191743046496589274256239341020864383202110372958725
 76235850964311056407350150918751062359462920556368552947521351
 5952879416377328533906109750544334219811150056977236890927563

Because this key is a number several thousand bits long, it does not have a concept of identity. A certificate would be needed to tie the public key to an identity. Furthermore, to send a secure message, the sender must also have all this information and connect it via a certificate to the recipient.

But here is an example of a public key for IBE:

Name = bob@b.com

Choosing simple, understandable keys is "key" to the IBE architecture's ability to encode policy directly into encryption and authentication.

Key Management in IBE

Key management includes key generation and key updating. These functions are performed by a centrally-managed server (in this case, a component of the Safeserve Secure Messaging product).

Key Generation

As the name implies, Key Generation generates public and private keys for secure communication. The Key Server's primary function is generating private keys to enable users, services and applications to utilize IBE encryption.

Key Update

Key Updating ensures keys are changed regularly to protect the system and user if a key is lost or stolen. It is the component of key management that validates the key's authenticity and uses a combination of identity and date, such as:

"name=Bob validity=1/1/06-2/16/06"

The public key is changed for each time period. Therefore, the private key, which corresponds to the public key, also changes. This limits how long security could possibly be compromised.

Also, instead of revoking a key for a fired employee or compromised machine, the server simply stops issuing private keys to that identity.

In PKI-based systems, a compromised key ends up on a CRL, which is often not checked.

Summary Comparison of Secure Messaging Solutions

Key Features	Safeserve SecureMail	PKI based solutions	Webmail based solutions	Symmetric solutions
Usability	●●●●	●○○○	●●●●	●●●○
Scalability	●●●●	●○○○	●○○○	●○○○
Authentication options	●●●●	●●●●	●○○○	●○○○
Ad-hoc messaging	●●●●	●○○○	●●○○	●●●●
Disaster recovery	●●●●	●●○○	●○○○	●○○○
Integration with inbound anti-virus, anti-spam and content filtering	●●●●	●○○○	○○○○	●○○○

The table above summarizes the key differences between Safeserve Secure Messaging and other email encryption solutions. These solutions can be differentiated along six important criteria.

Usability

Safeserve's solution eliminates the need to use certificates, certificate revocation lists and the entire costly and complex infrastructure associated with PKI systems. As a result, it is substantially easier to use and offers a much lower total cost-of-ownership.

Scalability

Each type of solution scales differently because each approach requires different sorts of information to be stored. The relatively high storage requirements associated

with most solutions create a variety of disaster recovery, retention and backup problems (which are not shared by Safeserve Secure Messaging):

- ❖ With PKI solutions, you need to create keys as well as store and distribute certificates and revocation lists, which become onerous to manage over time.
- ❖ In webmail-based systems, all messages are sent to a separate inbox that resides in a parallel messaging architecture. This parallel mail infrastructure needs to store all messages and archive them.
- ❖ With symmetric solutions, keys are issued for every user and every message. This means that an online server must be available to encrypt and decrypt messages.

Authentication

Authentication is central to any encryption system. Safeserve can provide the widest array of options for authentication, including RSA SecureID, PIN/password, Active Directory, LDAP and custom adaptors. Most other solutions provide very limited integration capabilities for authentication.

Ad-hoc Messaging

Being able to send secure messages to recipients with whom you have never corresponded is a key requirement. Most solutions require pre-registration or the creation of additional, redundant credentials—which cannot be backed up—before encrypted messaging can be enabled.

Safeserve Secure Messaging was designed from the ground up to simplify this situation and requires neither user pre-registration nor software download to receive messages.

Disaster Recovery

Most solutions require the storage of information pertaining to certificates, credentials, users and messages in order to encrypt. With Safeserve Secure Messaging, none of this information ever has to be centrally stored, which makes it very easy to restore after a disaster.

Summary

Safeserve Secure Messaging, powered by Voltage IBE, is policy-driven (or “content aware”) secure messaging that’s easy to administer, easy to use, easy to change and easy to afford.

There are no keys or messages that have to be stored for extended periods. The end-user isn’t called on to handle compliance or enforcement or deal with complicated digital certificates or keys.

IBE offers significant advantages over Symmetric, PKI and Webmail-based encryption solutions in terms of usability, manageability and total cost of ownership.

About Safeserve.com Ltd.

Safeserve provides messaging security solutions for large and small enterprises to stop spam, protect against email viruses, ensure compliance with corporate policies and regulations and defend against leaks of confidential and proprietary information via email and other message streams.

Safeserve Modules

Safeserve Spam Detection

Safeserve Virus Protection

Safeserve EmailArchive

Safeserve SecureMail

Safeserve Intelligent Mailer

Safeserve.com Ltd

86 Beaufort Street
London, SW3 6BU
UK

P +44 (0)20 7349 1570
F +44 (0)20 7349 1574

E info@safeserve.com
www.safeserve.com