



***Sigaba Technology***

**Technical White Paper  
December 10, 2003**



# Sigaba Technology

<b>Introduction</b>	<b>3</b>	<b>Sigaba Email Solutions</b>	<b>10</b>
<b>Alternative Solutions</b>	<b>3</b>	Secure Enterprise Email	10
Web-Based Secure Email	3	Gateway	10
Auditing Access	3	Plug-ins	10
Separate Email Account	3	Case Study: Hospitals and Doctors	11
Additional Costs	3	Secure Statements	11
Desktop Clients and Plug-ins	4	Secure Reply	12
Difficult to Set up	4	Key Server	12
Difficult to Enforce Policies	4	Owning a Key Server	12
Password-based Solutions	4	Global Authentication	13
Ease of Use	4	Professional Services	13
No ability to change password	4		
Least Secure	4	<b>Conclusion</b>	<b>13</b>
Limited Control	4		
Gateway Solutions	4	<b>References</b>	<b>13</b>
Scalability Issues	5		
<b>Sigaba Technology</b>	<b>5</b>		
Unique Approach	5		
Global Authentication	5		
Standard Encryption	6		
Benefits of the Unique Approach	6		
Policy-Based Control	7		
Leveraging Existing Investments	7		
Auditing and Reporting	8		
Sender Control	8		
Attacks and Defenses	8		
Guessing the Encryption Key	8		
Changing the Content of an Email	8		
Untrusted Key Holder	9		
Man-in-the-Middle	9		
Stealing Email Messages	9		
Modifying Email Messages	9		
Generating Forged Email Messages	9		
Random Number Generator	9		
Intercepting the Key	9		
Forward and Backward Secrecy	10		
Security of the Database	10		

## INTRODUCTION

Everyone's defenses are up. On the Internet, they have to be. Vigilance is critical to make sure that data is safe, that privacy is guaranteed, that intellectual property is amply protected. To safeguard information is good business. It also is a government mandate – with penalties in abundance for non-compliance. And, in the battle to comply with legislation – Gramm–Leach–Bliley and the Health Insurance Portability and Accountability Act (HIPAA) – email is on the front lines.

It is overtaking postal mail for business correspondence – correspondence that contains private, confidential information: Information about health, finances, R & D, and national security. And all of it requires protection: protection in the form of encryption, of policy rules and their implementation, and of ongoing maintenance to guarantee that senders and recipients are constantly accounted for. It has always been a time-consuming, labor-hungry process.

Starting now, it will be different. Email security has evolved. Sigaba has developed a system that combines the encryption technology chosen for U.S. Government agencies with the simplicity of point-and-click procedures. On its own or interoperating with your current Private Key Infrastructure (PKI) or S/MIME applications (as well as with virus scanning and content filtering programs), Sigaba software can be up and running quickly. It works with every major email client and server and eliminates the need for recipients to have Sigaba software installed on their own systems. Scalability is, essentially, infinite.

This white paper presents the secure messaging solutions from the Sigaba and the technology behind them. It explains how Sigaba's breakthrough research and development has now made possible what before what was impractical. After reading this paper, it will be clear why Sigaba's technology is the superior technology for secure messaging.

## ALTERNATIVE SOLUTIONS

### Web-Based Secure Email

Web-based secure email products provide a web service in which messages are sent to recipients with links back to a web site. When the recipient receives the email, they click on a link and return to the web site to read the email. They log into their account using their credentials (e.g., user ID and password), view the email and download attachments over secure connections.

### Auditing Access

Secure web-based email solutions have the ability to accurately log when recipients retrieve their email. This feature allows the sender to audit message receipt and generate reports of all disclosures of sensitive email.

### Separate Email Account

Web-based solutions require the end-user to access a separate system to read secure email. This additional step is acceptable in some applications, such as secure statement delivery alternatives in which the recipient expects to retrieve their statement from a web site, but is not a workable solution for regular corporate email communications.

- The email is stored on a separate server and adds the additional burden of connecting to a separate web server to read secure email.
- It is more difficult to search through old emails because the secure emails are stored on a separate server.
- It is contrary to the model of email. Email is a push application in which the sender need not manage how or when the recipients get their email. Web-based secure email is a pull application in which the sending organization must manage the email lifecycle until all recipients read and delete the email.

### Additional Costs

Web-based solutions can be more expensive to deploy. They require companies to roll out web servers to host

the secure email content. They are costly to set up and they are costly to maintain. Processing and storage capacity must be maintained to service peak demand. Companies assume the time-consuming burden of managing the backup and aging of gigabytes or terabytes of old messages. Such costs can make securing email prohibitively expensive.

### **Desktop Clients and Plug-ins**

Outlook, Outlook Express and Lotus Notes include S/MIME security settings that allow users to encrypt and digitally sign email messages. There are also plug-ins available for these and other email clients that add different kinds of encryption and signing. These solutions are not often used because the underlying technology is too cumbersome for the user.

### **Difficult to Set up**

Many of the existing desktop clients or plug-ins require the end-user to acquire the digital certificates of all the people to whom they intend to send secure email before sending them email. The additional step of requesting someone's certificate is usually more of a burden than it is worth. Users opt instead to send the email without encryption. While some groupware solutions have certificate exchange built-in, the exchange is limited to the range of the directory service and does not solve the problem of sending secure email outside the group.

### **Difficult to Enforce Policies**

When using desktop software to encrypt email, IT managers rely on the end-user to make the decision whether or not to encrypt the message. While good corporate training programs help employees learn the security policies, employees sometimes forget. When employees forget, companies are at risk.

### **Password-based Solutions**

Sending secure email that is protected with a password is easy: the sender encrypts the email message with a password and the recipient decrypts the email message with the same password. While conceptually simple,

there is a significant burden on the message sender: how do all recipients get the password? Web-based registration systems are normally employed for such applications. However, these can be cumbersome to set up.

### **Ease of Use**

Password-based solutions can be easy to use. However, since the sender must communicate the password to all recipients, an extra step is involved when the message is initially sent. The password may need to be communicated via phone or perhaps through another, unsecured, email. Password-based solutions do not address the issue of password distribution.

### **No ability to change password**

Recipients who forget their password or want to change their password cannot do so with password based systems. It is possible to change a password but all documents encrypted with the old password will remain encrypted with the old password...this does not bode well for people who forget their password.

### **Least Secure**

Password-based solutions are the least secure of the three solutions discussed. Passwords are often short and chosen poorly. Furthermore, the encryption key is either derived from the password or is wrapped by the password (i.e., the encrypted message and the key are protected" by the weak password.) An attacker who knows the password can read all emails. An attacker who doesn't know the password can easily crack the message in a short amount of time, using easily-available password cracking programs.

### **Limited Control**

Password-based solutions do not permit any control after the email is sent. The reason is that the decryption key is either based on the password or wrapped by the password, which is known to the recipient.

## Gateway Solutions

Gateway solutions are hardware or software solutions installed at the edge of the department or company network, for the purpose of encrypting outgoing email and decrypting incoming email based on policies. The gateway approach has the advantage of enabling IT managers to establish policies by which encryption and decryption decisions are made. Using policies, it is easy to implement corporate security rules.

## Scalability Issues

Some of the gateway solutions have scalability issues that make it difficult to establish secure communications with a large group of people. The solutions that are limited in this manner are based on the S/MIME or PGP standard. Inherent in the standard is the requirement to have *a priori* possession of all the recipients' digital certificates. While it is reasonable to obtain the certificates of a small set of partners, solutions based on this technology fail when they are applied to larger deployments. The burden of exchanging certificates with thousands of partners or hundreds of thousands of individuals is unreasonable.

## SIGABA TECHNOLOGY

### Unique Approach

#### Key Exchange Technology

Sigaba developed a unique approach to managing key exchanges based on our patented distributed key server architecture.

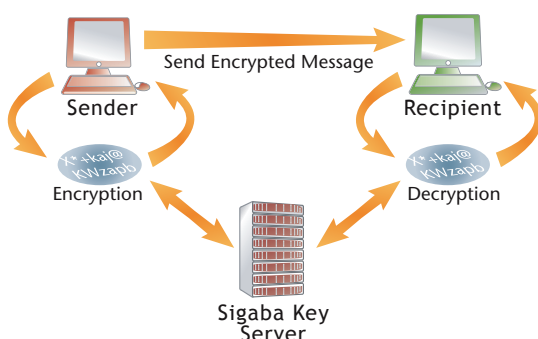


Figure 1. Key Exchange Technology

In this approach, the sending email client requests a unique key for each message the software encrypts.

The key server generates a new random key, stores it and returns a copy to the sending software to use for encryption. When the recipient receives an encrypted message, his or her software contacts the key server to request the key. If the recipient is authorized to read the message, his or her software is returned the key to use to decrypt the message.

Each corporation can purchase their own key server to generate and host the keys for messages they send. The URL to the key server that is storing a key for a particular encrypted message is contained in the message itself. When the receiving software opens the encrypted message, it discovers the location of the key server from which it must request the key.

Since the key of the message is not sent with the message, users derive both a security benefit and an auditing benefit. From a security standpoint, the sender avoids the Adaptive Chosen Ciphertext Attack when the key is not with the message. From an auditing standpoint, because the recipient software does not request the key until the recipient opens the message, the sender can determine when the recipient opened the message based on the key request timestamp.

Furthermore, senders have the ability to expire, or shred, a message key after they have sent a message. If the recipient has not yet opened the message, shredding the key will prevent them from reading the message. In this way, the sender maintains control of the message once it is sent.

## Global (Federated) Authentication

Sigaba has developed a patent-pending technology called Global (or Federated) Authentication that enables security products to integrate with any of a number of existing authentication mechanisms. The Global Authentication consists of connectors that integrate with existing authentication mechanisms and produce

digitally-signed, standard XML-based Name Assertions that vouch for the user's identity [1].

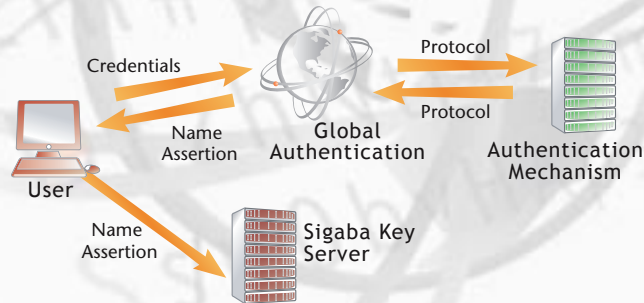


Figure 2. Authentication

Applications such as Sigaba's Key Server can accept the Name Assertion as a valid credential and not be burdened with having to authenticate users themselves. The separation of the authentication process enables new security applications to easily integrate with existing authentication technologies.

Sigaba can use this technology to integrate with smart cards, Secure ID, personal digital certificates, user ID and password authentication mechanisms.

Sigaba's email encryption products prompt the user for their credentials and authenticate the user via Global Authentication. The products receive the Name Assertion and pass it to the key server when requesting a key, both during the encryption and decryption processes.

When two companies are communicating securely with each other and both have their own authentication mechanisms, the Global Authentication enables them to send and receive encrypted email seamlessly. When the recipient's software receives a Name Assertion from their own authentication server, the software passes that Name Assertion to the sender's key server. If the sender's key server is configured to allow users from the recipient's domain to retrieve keys, the recipient's Name Assertion will be accepted as a valid credential. Since the Name Assertion is digitally signed by the recipient's Global Authentication, the sender's key server can confirm the authenticity of the Name Assertion.

### Standard Encryption

Sigaba uses the standard Advanced Encryption Standard (AES) encryption algorithm in all of its encryption software. AES is the Rijndael algorithm adopted by the National Institute of Standards and Technology (NIST) and is the Federal Information Processing Standard (FIPS) Publication that will specify a cryptographic algorithm for use by U.S. Government organizations to protect sensitive information [2]. AES is the new NIST standard to replace DES and 3DES, and it is one of the recommended encryption standards to use in complying with HIPAA.

### Public Key Infrastructure

A PKI can be used in several different ways. PKI enables three primary functions:

1. Key exchange,
2. Authentication of identity, and
3. Non-repudiation (authentication of origin).

Under PKI, the key exchange function (number 1 from the list above) is only useful if everyone has a digital certificate. For this reason, Sigaba uses a key server solution. The last two functions (2 and 3) do not require everyone to have a digital certificate. Sigaba can use PKI for authentication of identity and authentication of origin. In fact, through the Global Authentication, users can employ an authentication mechanism of their choice.

### Benefits of the Unique Approach

#### Send Securely to Everyone

The biggest benefit of Sigaba's key exchange technology's is the ability to send secure email to anyone and everyone who has an email account without having to first obtain their digital certificates, or any *a priori* knowledge of their credentials. The sender encrypts the message with a unique key obtained from the key server and sends the encrypted message along normal email channels to the recipients. Sending encrypted is as easy as sending in the clear.

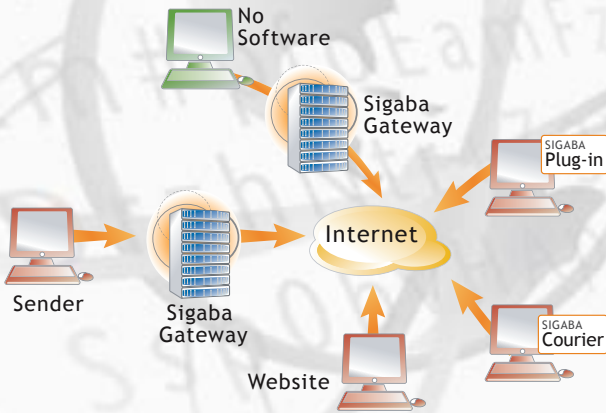


Figure 3. Send Securely to Everyone

Upon receiving the encrypted email, the recipient has a number of ways to read the email.

- **Secure Gateway:** The recipient can read the message as they would normal email if the recipient's company has a Sigaba Affiliate Gateway installed that is configured to decrypt the message as it enters the company's intranet.
- **Plug-In:** The recipient can download a plug-in for their email client which, once installed, will be able to decrypt the message. Sigaba provides plug-ins for all popular email systems.
- **Send Anywhere:** If recipients have neither an Affiliate Gateway nor a Plug-In, they can receive secure emails wrapped in an HTML attachment that opens in their web browser. The recipient does not need to pre-install any software to read the email.

In all of these cases, the recipient will have to properly authenticate prior to decrypting the message. For customers of companies using Global Authentication, this is merely a matter of entering their established credentials, such as the Social Security Number or Personal Identification Number. For individuals not associated with the sender or for companies not using Global Authentication, this is as simple as registering on-the-fly at a web-based registration page.

### Policy-Based Control

Sigaba's key exchange technology makes it easy to manage corporate security policies that dictate which email content needs to be encrypted over open networks. Some organizations prefer rigorous controls and encrypt all messages, encrypt all messages from specified departments or to specified locations, or encrypt messages containing specified content such as patient identification numbers. Other organizations may allow end-users to decide which messages should be encrypted. Sigaba makes it easy to redefine policies at any time, and policy-based encryption simplifies compliance with HIPAA rules and other regulations that govern private information sent over open networks.

Other solutions that don't use Sigaba's key exchange technology have difficulties dealing with recipients whose certificates are unknown or unobtainable. Such difficulties lead to problems implementing policies because email either gets delayed, temporary certificates are created or alternate methods of delivery are employed. In these cases, the administration becomes more burdensome and policies more complex. With Sigaba's key exchange technology, because email can be secured to everyone without the need for prior exchange of digital certificates, policies can be adhered to and email can be encrypted and delivered on time and without burden.

The Sigaba system lets administrators establish and enforce a wide variety of policy rules, giving them enormous flexibility and control over which messages get encrypted

### Leveraging Existing Investments

Sigaba's technology relies on existing email infrastructure to deliver email messages. Sigaba does not introduce new web-based email interfaces that require additional investment by corporations. Instead, Sigaba leverages existing groupware products, email clients and gateways to perform the function for which

they were purchased and seamlessly adds security on top. This has the two-fold benefit of leveraging existing personnel training in using the email applications as well as leveraging IT's technical expertise on administering the existing infrastructure.

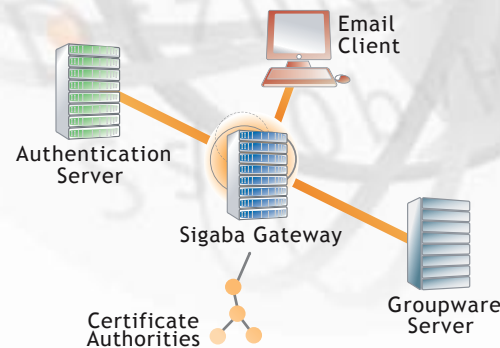


Figure 4. Leveraging Existing Technologies

Furthermore, Sigaba's Global Authentication technology enables companies to use their existing security technologies in conjunction with their Sigaba secure email solutions to leverage existing investments. Companies can hook into their smart cards, PKI, certificates, Secure ID, LDAP servers, Radius servers and other technologies with the Global Authentication technology and secure email products to roll out a comprehensive secure email solution.

### Auditing and Reporting

Sigaba's key exchange technology enables auditing and reporting of key access that can be used to determine when recipients have read email. Timestamps are recorded when keys are retrieved on a per-recipient basis. Message keys are associated with the sender's email address, subject of the message, timestamp when the message was sent and the list of all recipients to whom the message was sent. Details include the times when each recipient reads the message they received and the number of times they've requested the key for the message. These reports can be used to automatically send follow-up emails to people who do not open urgent messages, such as an email containing a margin

call. Another policy could inform a customer service representative if follow-up emails were unopened. The representative could then follow up with a phone call. This process could significantly reduce costs for many organizations.

### Sender control

This is an area in which Sigaba provides tremendous capabilities. The model of Sigaba is that the sender owns the email until the recipient reads it. For example, the sender can:

1. Set the expiration time, making the email unreadable past the expiration time.
2. Set the available time, making the email unreadable until a specific time.
3. Update the list of recipient, enforcing the rule of who can read the email. By deleting a user from this list, the sender can "shred" the mail for that specific recipient.
4. Determine whether and when a recipient has read the email.

### Attacks and Defenses

No system can guarantee 100% security. Here we explore possible attacks and describe how Sigaba's technology thwarts or mitigates these attacks.

### Guessing the Encryption Key

A popular form of breaking the security of a system is a brute-force attack. A brute force attack involves searching the entire key space to find the correct encryption key. Depending on the speed of the attacking computer, this can take days, months, years, or even centuries. For the sake of comparison, if it takes 1 day for a device to break a 40 bit DES key, it will take more than 7 years for the same device to break a 56 bit DES key, and more than several thousand billion years for the same device to break a 168 bit triple DES key.



Sigaba uses the publicly available and rigorously tested Advanced Encryption Standard (AES) algorithm with 128 bit keys [1]. Assuming that one could build a machine that could break a DES 56 bit key in one second, then it would take that machine approximately 149 thousand-billion (149 trillion) years to break a 128-bit AES key.

Additionally, Sigaba generates a unique key for every message. The use of per-message keys rather than per-user keys means that breaking of one key does not expose all of a sender's email messages, one of the critical shortcomings of PKI approaches.

### **Changing the Content of an Email**

Email messages and their attachments contain important information. An attacker may benefit from changing the content of an email message by replacing sensitive information such as shipping addresses, account numbers, and so forth. Sigaba protects the integrity of all email messages via a seal. Sigaba software verifies the message seal upon receipt and alerts the recipient if it discovers message tampering.

### **Untrusted Key Holder**

Sigaba uses a distributed-key-server architecture, which is a collection of key servers. These servers create, store, and deliver keys to authorized requesters. A system that uses another service for generation and distribution of encryption keys must trust that service. With Sigaba's approach, the key server never receives the actual email message. The issue of trust of the key server is simple: with keys but no messages, the key server is in no better position to decrypt an email message than a third party that steals the messages but does not know the encryption keys.

### **Man-in-the-Middle**

In the context of email, a man-in-the-middle attack involves a perpetrator who steals email messages, modifies email messages, or generates forged email messages. We consider each of these cases below.

### **Stealing Email Messages**

Because Sigaba is not involved in routing and delivering an email message, Sigaba does not make it any easier or more difficult for an attacker to steal an email message. In any case, the email message is encrypted, and the key does not travel with the email. In order to retrieve the encryption key the recipient must authenticate with the key server as a legitimate recipient. Because the authentic sender defines the recipients of a given email, there is no opportunity for a perpetrator to modify the recipient list.

### **Modifying Email Messages**

A perpetrator can modify a message before it gets to its destination but he or she faces two insurmountable problems. Firstly, the message is encrypted, so to achieve a useful change to the text of the message, the perpetrator would have to steal the message, steal the key, decrypt the message, modify it, re-encrypt the message, and insert it back into the email system. Secondly, Sigaba attaches a seal to the message, based on a message digest that cannot be modified. Any change to the content of the message will invalidate the seal. The Sigaba software notifies the recipient if it detects an invalid seal.

### **Generating Forged Email Messages**

To get an encryption key, a sender must authenticate and present a valid name assertion. As a result, generating a forged email message is as difficult as forging an authentication credential.

### **Random Number Generator**

A well-known target for attacking a security system is its random number generator. A security system frequently uses a random number generator for creating keys and performing cryptographic functions. A weak random number generator results in predictable patterns, which in turn enables an attacker to guess the encryption key.

Sigaba uses a random number generator that is compliant with Federal Information Processing Standard (FIPS) 140-1 [3].

### Intercepting the Key

An attacker can try to intercept the encryption key and decrypt the email message. Sigaba has the unique feature that the encryption key never travels with the email message in any form. Therefore, an attacker who intercepts an email can never distill from it any information about the encryption key.

### Forward and Backward Secrecy

A user should only be able to read messages for which he/she is an intended recipient. Having the right to read an email message from a particular sender does not automatically extend to all messages that were sent before or will be sent later by the same sender. This is the most significant problem in protecting email messages with passwords: the password cannot change frequently enough to preserve forward and backward secrecy.

With Sigaba each message has a unique key. A user who decrypts a message from a given sender cannot decrypt messages that were sent by the same sender before or after. When a message key expires, Sigaba deletes the key forever. Subsequently, no one can ever decrypt the message again.

### Security of the Database

All sensitive data in the key server's database is also protected. For example, the key server can use hardware-based encryption to protect all message encryption keys while in storage. This eliminates the risk of an attacker stealing the key server's database and discovering the encryption keys.

## SIGABA EMAIL SOLUTIONS

Sigaba developed its technology to solve a number of problems that current security technologies cannot solve. Sigaba then built a group of secure email products

to use the technology for the benefit of corporate and government communications.

### Secure Enterprise Email

Sigaba provides secure email solutions to large companies and government organizations that need to secure their email communications to partners, departments and individuals over open networks. The enterprise solution is shown in the diagram below.

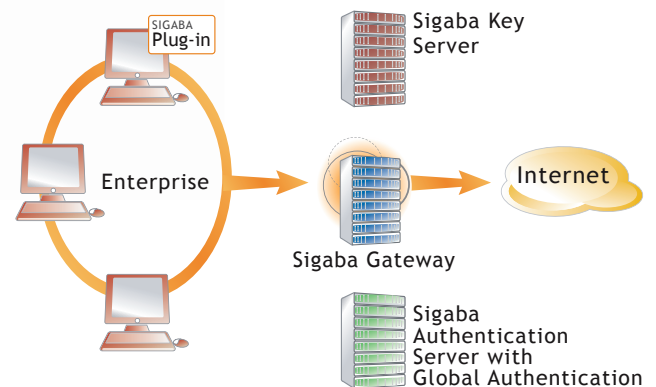


Figure 5. Secure Enterprise Email Solution

### Gateway

The Gateway component of the Sigaba Secure Email product is enterprise software that is installed and configured to run at the gateway to the corporate network. It encrypts outgoing email and decrypts incoming email based on corporate security policies.

Policies are based on the sender's or receiver's email address or a pattern match in any of the MIME headers. Combinations of patterns can be used to build more sophisticated policies. Separate policies are configured for encryption and decryption.

### Plug-ins

Plug-in are optional software components to Sigaba Secure Email that integrate with email client software, such as Outlook, Lotus Notes, GroupWise, Eudora and Outlook Express to manage the encryption and decryption of the email contents. The software

communicates with the Global Authentication and Key Server to authenticate and obtain keys, respectfully.

Plug-Ins enable email to be encrypted and decrypted at the desktop inside the organization. Executives with sensitive information that cannot be exposed to internal employees use Plug-Ins to keep their email secure inside the company as well as over open networks. In conjunction with the Gateway, email is protected internally based on end-user decisions and externally based on corporate policies.

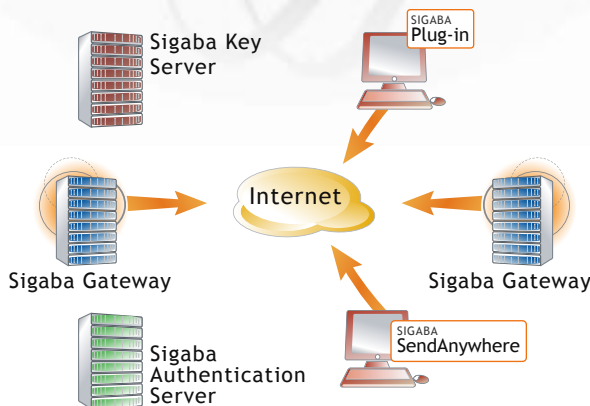


Figure 6. Recipients of Secure Email

Plug-ins are also available to recipients of secure email outside the organization. For secure ad-hoc communications with individuals, shareholders, partners, legal firms or consultants, Plug-Ins can be used. For longer term relationships, or to ensure policy compliance, companies can encourage their partners to install their own Affiliate Gateway.

### Secure Statements

Sigaba Secure Statements is designed for applications that involve secure transmission of sensitive information to very large numbers of users. Secure Statemetns sends such information in encrypted emails in an HTML attachment. The recipient opens the attachment and enters their credentials to decrypt the message.

### How does it work?

Sigaba takes an existing print stream data that has been converted to a standard electronic format (html, pdf, etc...). Once converted, the electronic data is sent to Sigaba’s statement delivery product. Sigaba manipulates the document in a number of ways:

The recipient receives the email. Typically, the email will contain minimal branding and instructions on how to decrypt the enclosed document. When the recipient opens the HTML attachment their experience will be dictated by their computing environment.

If ActiveX is supported, the recipient will be presented with a permissions box (first time only) asking them to allow the signed component. If they agree, they will then be presented with a credentials request. If their computing environment does not support ActiveX, the software will attempt to use a Java applet or Javascript to perform the decryption. In the worst case, if none of the above is permitted, Javascript in the page will automatically send the encrypted text to a web-based decryption server. This server will cache the ciphertext and prompt the user (using an ssl form) for their credentials.

Authentication credentials are sent to the proper Global Authentication server and then keys are retrieved from the appropriate Key Server.

In the case of the ActiveX component, the key server releases the key for the message and the ActiveX, Java script or Java applet component decrypts it. If the web decryption service is used, the key is passed to the decryption server. This server decrypts the message and sends it back to the recipient via SSL.

The document opens in its native application after it is decrypted. HTML documents open in the same browser window that the recipient opened to read the email.

The look and feel of the entire experience is not limited by Sigaba’s technology. Macromedia flash, complex

HTML, and innovative graphics can all be combined to provide a very rich experience.

### Secure Reply

The decrypted document, if it is an HTML page, can contain an HTML form with POST data sent securely back to the decryption server. In this fashion, Sigaba Secure Statement messages can empower secure replies or transactions or can initiate e-business sessions on the company's site. Since Secure Statement messages are sent securely, the HTML form can include hidden POST parameters that contain personally-identifiable information. Since the form can be posted back to the site over an HTTPS connection, the private information is secured for the entire round-trip. Used in such a manner, Sigaba is an excellent tool for company-initiated e-business sessions. The reply process is highly automated and replies are automatically tagged so that recipients can easily access additional information pertinent to the reply. This feature is normally used for customer support applications, bill payment, and other applications that require two-way secure communication.

### Common Components: Key Server

The Key Server is enterprise software that is installed and configured to run at the gateway to the corporate network inside the firewall. The Key Server handles requests for all of Sigaba's products. It generates random keys for encryption. It then returns keys to authenticated and authorized entities to use in both encryption and decryption.

### Owning a Key Server

The Key Server is deployed in-house and allows companies to integrate key storage with their corporate archival and retention policies.

Sigaba is configured to use the Key Server to obtain the keys it uses when sending secure email. All outgoing email is encrypted with keys from the in-house Key Server. Thus, a company owns the keys for all messages it

sends. All secure emails sent by Sigaba products include the location of the key server in the message headers.

In addition to the obvious positive security implications, there are many benefits to owning a Key Server. These benefits include:

- The owner can set security policies on the key, including when and how many times a key is released.
- The owner can modify the list of authorized recipients at any time, including after the content is encrypted.
- The owner can delete the key, thereby shredding the content.
- The owner can determine when and to whom a key is delivered.

### Global Authentication

Global Authentication is the technology that Sigaba uses to integrate existing authentication mechanisms with secure email. The technology is based on an XML standard for security [1] and produces a Name Assertion for each successful authentication.

The Global Authentication technology works with many different authentication mechanisms, including the following:

- Secure ID cards
- Digital Certificates
- Smart Cards
- Social Security Numbers and Personal Identification Numbers
- User names and passwords

Due to the complex and custom nature of authentication mechanisms, Sigaba makes integrating with these mechanisms possible by providing both off-the-shelf Authentication Adapters to popular authentication



mechanisms (such as LDAP and Active Directory). In addition, Sigaba Professional Services can help design and build the integration solution that is right for your company.

### **Global Authentication**

Companies can engage Sigaba Professional Services to design and implement a Global Authentication solution to use their internal authentication mechanism to authenticate senders and receivers of secure email. Senders and receivers are already part of their company's authentication database, and can use those credentials to send and receive secure email.

Global Authentication is the best solution for companies with employees, remote employees, customers, partners and shareholders that have already established authentication credentials with the company.

Financial services companies sending statements via the Sigaba Gateway with the Secure Statements product, for example, could deploy Global Authentication to enable customers receiving secure statements to use their Social Security Number and Personal Identification Number to authenticate and decrypt the statement.

### **Professional Services**

Sigaba employs a team of security experts that have many years of experience designing and building security solutions. In fact, it was from this experience that Sigaba's core technology was developed. Sigaba's security experts understand the issues with deploying security products and can help design solutions that leverage existing investments and achieve the security goals of the company.

Sigaba's Professional Services team can evaluate companies' secure email needs and design and help implement the perfect Sigaba solution to meet those needs.

Professional Services will develop custom Global Authentication solutions to leverage existing

investments in authentication mechanisms. Sigaba has extensive experience in PKI, smart cards, Radius, Secure ID, personal certificates, SSN/PIN and biometrics. They can help companies build the best secure email solution to seamlessly integrate with their security infrastructure.

### **CONCLUSIONS**

Federal regulations are commands. HIPAA and the Gramm-Leach-Bliley requirements are no exception. Yet the demands for secure communications that affect nearly every American company can be easily met with Sigaba's email software applications.

Sigaba makes secure email easy to implement by providing products that can be installed in under a day and services that can reduce implementation time drastically. Sigaba makes secure email easy to use by centralizing encryption policies to the gateway and integrating with existing email clients and groupware solutions.

Give Sigaba half a day. And get security that satisfies your customers, employees, business partners, IT staff, and the U.S. Government.

Call us today. Be compliant overnight. Contact Sigaba at [sales@sigaba.com](mailto:sales@sigaba.com) or 1-800-475-8226.

### **REFERENCES**

- [1] Security Services Markup Language (S2ML). (<http://www.s2ml.org>)
- [2] Federal Information Processing Standards Publication Draft for the Advanced Encryption Standard (AES). (<http://csrc.nist.gov/encryption/aes/>)
- [3] National Institute of Standards and Technology (NIST), FIPS 140-1, Security Requirements for Cryptographic Modules; January 11, 1994.